Roger Insurance Cybersecurity Analysis Report

August 19, 2024

Powered by cynomi

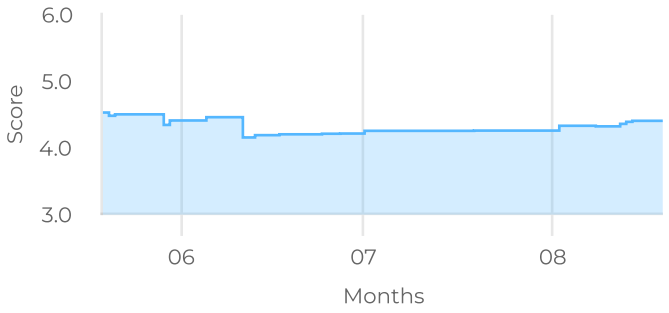
Introduction

This report details your organization's cybersecurity posture. It provides a high-level cyber risk assessment to indicate your organization's effectiveness at addressing cyber risks. It also provides a prioritized list of recommendations to improve your posture and mitigate those risks. The information in the report is compiled from publicly available information about your organization as well as information provided by you about your organization's environment. Recommendations in this report, adhere to multiple cybersecurity frameworks including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ISO 27001, the Center for Internet Security (CIS) controls, and SOC 2.

Posture score

4.4

Basic protection measures have been taken. Only the most basic attacks are blocked.



Attack vector score

Current cybersecurity threat readiness of four cyber attack categories.

Data Leak

An overlooked exposure in a data storage which might lead to data breach.

4.5

Average

Fraud

A crime in which someone gains inappropriate access to financial or sensitive business information, used to commit fraudulent crimes.

4.4

Average

Ransomware

A threat by a malicious software to either publish or block access to data by encryption, unless a ransom is paid.

4.5

Average

Website Defacement

An unauthorized and malicious modification of web page content.

4.3

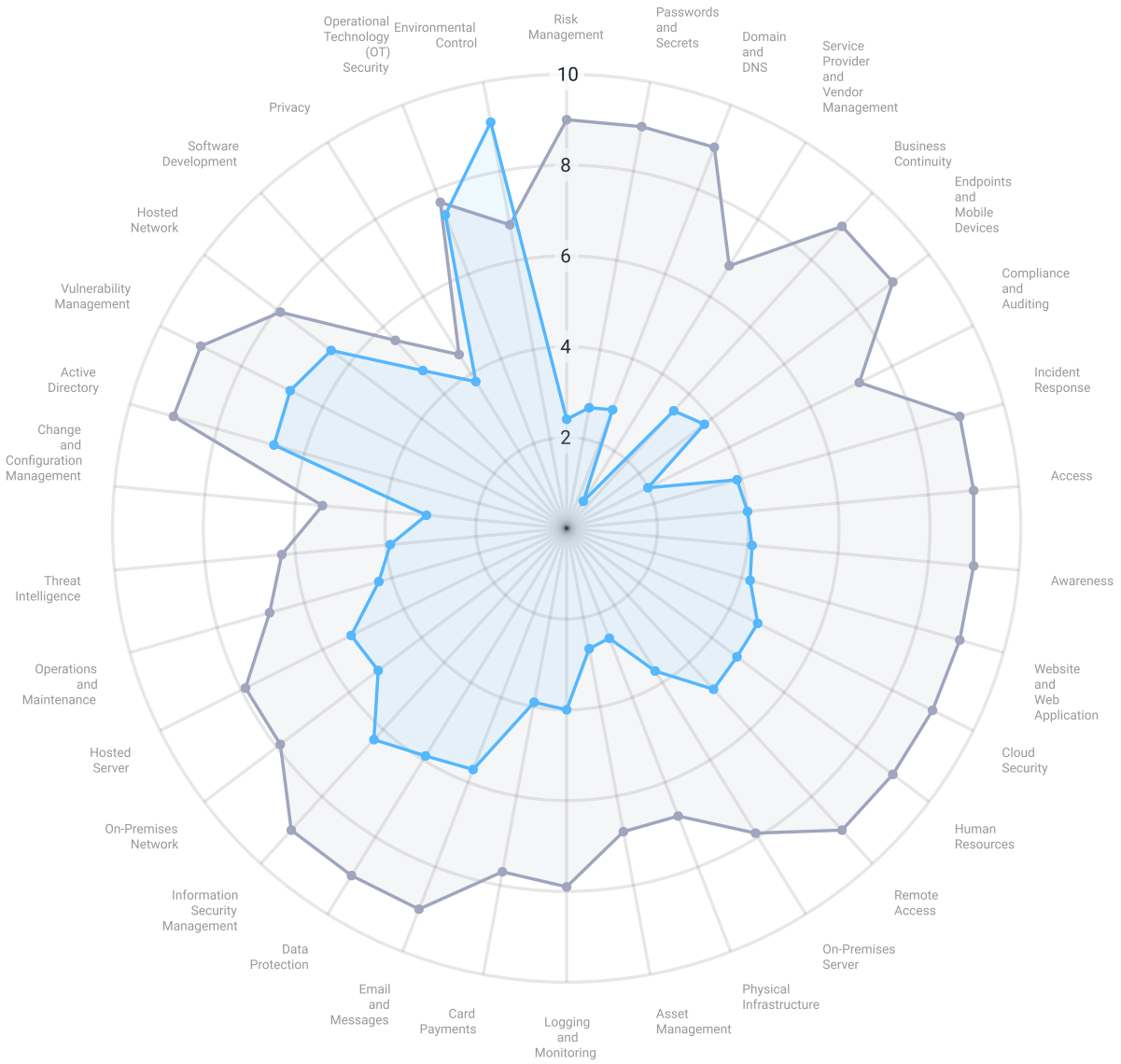
Average

Cybersecurity readiness level

34	1	33
Total Domains	Meet target score	Under target score

A mapping process of your organization shows that 34 security domains must be secured to safeguard the organization from cyberattacks.

To increase the organization's cybersecurity readiness, follow the custom-made policies of each security domain. For a good cyber hygiene, address first security domains with large gaps between current and target score.



Company readiness by security domain

DOMAIN	SCORE
Access	4
Active Directory	6.7
Asset Management	2.7
Awareness	4.1
Business Continuity	3.5
Card Payments	3.9
Change and Configuration Management	3.1
Cloud Security	4.7
Compliance and Auditing	2
Data Protection	5.9
Domain and DNS	2.8
Email and Messages	5.7
Endpoints and Mobile Devices	3.8
Environmental Control	9.1
Hosted Network	6.5
Hosted Server	5.3
Human Resources	4.7
Incident Response	3.9
Information Security Management	6.3
Logging and Monitoring	4
On-Premises Network	5.2
On-Premises Server	3.7
Operational Technology (OT) Security	7.4
Operations and Maintenance	4.3
Passwords and Secrets	2.7
Physical Infrastructure	2.6
Privacy	3.8

Company readiness by security domain

DOMAIN	SCORE
Remote Access	4.8
Risk Management	2.4
Service Provider and Vendor Management	0.7
Software Development	4.7
Threat Intelligence	3.9
Vulnerability Management	6.8
Website and Web Application	4.2

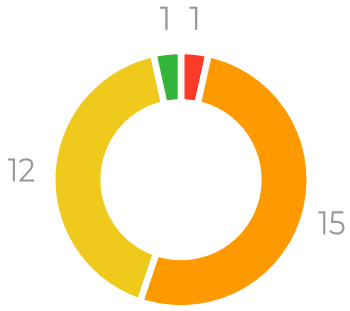
Scan Findings

Severity

64
Findings detected

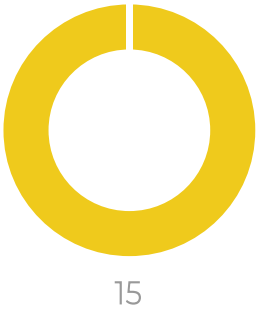
Critical	High	Medium	Low	Info
2	16	42	2	2

Internal Cynomi scan



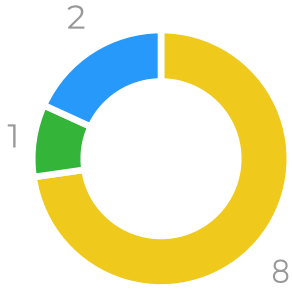
7 targets scanned — Total: 29

Microsoft Secure Score



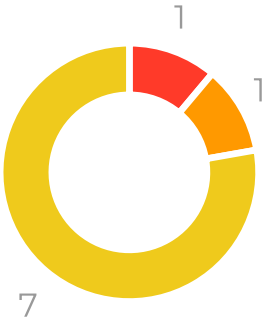
1 targets scanned — Total: 15

External Cynomi scan



2 targets scanned — Total: 11

External Nessus scan



1 targets scanned — Total: 9

Risk mitigation plan

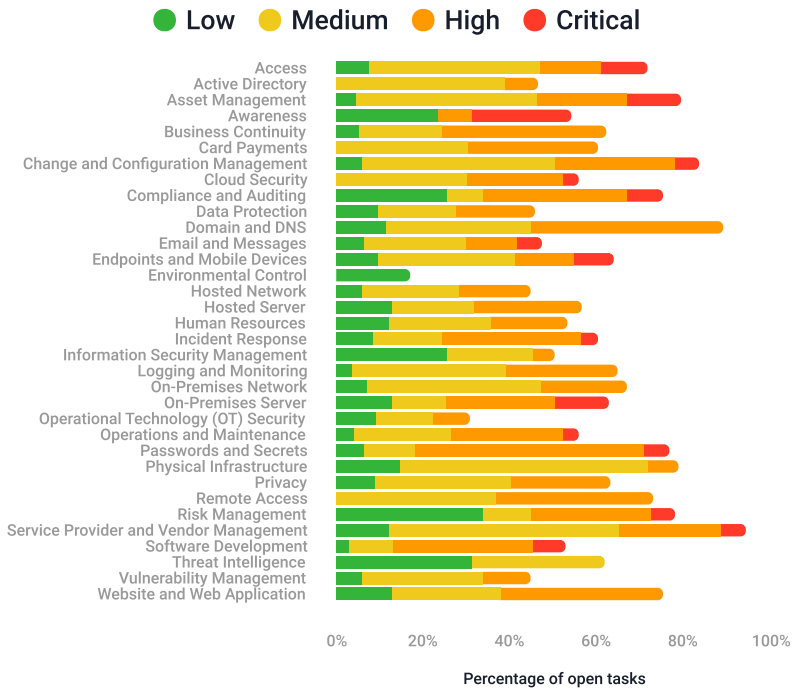
Completing critical and high severity tasks will impact organization cybersecurity the most, and increase posture score.

401	25	145	172	59
Open tasks	Critical	High	Medium	Low

39% tasks completed

401 Open tasks

Open tasks



Task status

361	13	17	10
Not started	In progress	Review	Deferred

Appendix A

Top 10 open tasks

The top 10 open tasks which impact your security posture the most.

ISSUE	RECOMMENDATION	ID
The company does not review and update policies, processes, and procedures.	The policy, processes, and procedures are reviewed and updated annually.	CYT-35205858003
Password complexity rules are not enforced.	Enforce password complexity rules on all assets.	CYT-00000784598
The company does not review and update policies, processes, and procedures.	The policy, processes, and procedures are reviewed and updated annually.	CYT-60895080478
Applications running on the server are not regularly updated and patched.	Regularly update all applications running on company servers and verify patches.	CYT-00000371537
A strong password policy is missing or not enforced.	Enforce a strong password policy for all connections to company servers, including connections through consoles, remote connections, or local logins.	CYT-00000979306
Anti-malware mechanisms are either missing or have not been configured.	Apply anti-malware tools.	CYT-00000756858
The company does not review and update policies, processes, and procedures.	The policy, processes, and procedures are reviewed and updated annually.	CYT-85446535983
Administrators may use the same password for their "normal" activities and admin tasks which require a higher set of privileges.	Require administrators to have different passwords and accounts for their admin user tasks.	CYT-00000845259
Inactive user accounts are not automatically flagged and removed.	Remove inactive user accounts, preferably automatically.	CYT-00000952139
The company does not review and update policies, processes, and procedures	The policy, processes, and procedures are reviewed and updated annually.	CYT-32016267896

Appendix B

Open tasks by domain - Access

	ISSUE	RECOMMENDATION	ID
🔴	The company does not review and update policies, processes, and procedures.	The policy, processes, and procedures are reviewed and updated annually.	CYT-85446535983
🔴	Administrators may use the same password for their "normal" activities and admin tasks which require a higher set of privileges.	Require administrators to have different passwords and accounts for their admin user tasks.	CYT-00000845259
🔴	Inactive user accounts are not automatically flagged and removed.	Remove inactive user accounts, preferably automatically.	CYT-00000952139
🟠	The organization lacks an efficient process to securely handle user account credential changes, raising the risk of unauthorized access and compromising data security.	Secure and manage user account changes.	CYT-50836925052
🟠	Failing to implement controls that trigger automated notices for changes in user access permissions may result in unauthorized access and lack of transparency in access management.	Automate notices to appropriate personnel for changes to user access permissions.	CYT-72084815841
🟠	Failure to implement controls that prevent unauthorized access to cryptographic keys can result in the compromise of critical security assets and encryption keys.	Implement controls that prevent unauthorized access to cryptographic keys.	CYT-87994462010
🟠	User access to sensitive assets and data is not secured.	Ensure that all account authentication is carried out using secure access protocols.	CYT-00000430577
🟡	Account identifiers may belong to more than one user at a time.	Ensure that account identifiers are not reused within a predetermined period.	CYT-00000184043
🟡	The company lacks a system for managing default accounts on its assets, which leaves potential vulnerabilities open. Default passwords might remain unaltered, and unnecessary accounts could remain active, providing accessible points for cyberattacks.	Ensure that Default accounts of company assets are managed.	CYT-28517273188
🟡	Multi-Factor Authentication is not enforced for privileged users.	Enforce Multi-Factor Authentication for all privileged accounts for all company assets.	CYT-00000282617
🟡	Not all applications are connected to a centralized Identity Provider (IdP).	Ensure all applications are connected to a centralized Identity Provider (IdP).	CYT-00000688505

Appendix B

Open tasks by domain - Access

	ISSUE	RECOMMENDATION	ID
🟡	Authentication information feedback is not blurred.	Blur feedback of authentication information.	CYT-00000460255
🟡	There is no Logging and monitoring of sensitive data queries.	Log and monitor queries of company sensitive data.	CYT-00000933655
🟡	There is no defined process for removing unauthorized access rights and privileges to assets and systems.	Establish a periodical audit of users' access rights and privileges.	CYT-00000584712
🟡	User accounts are not adjusted following changes to the role, access rights revocation, or position changes.	Adjust users' access rights and privileges upon role changes.	CYT-00000632658
🟡	There are no privacy and security notices for users when logging into organization systems.	Issue privacy and security notices to users upon logging into the organization system.	CYT-00000708103
🟡	Idle remote sessions are not terminated.	Terminate idle remote sessions after a defined period of inactivity.	CYT-00000385532
🟡	There is no restriction on the use of utility programs with system overriding and application control capabilities.	Restrict the use of utility programs with system-overriding and application-control capabilities.	CYT-00000883307
🟢	Some externally accessible company assets or services can be accessed without a two-factor authentication.	Enforce Multi-Factor Authentication for company assets and services that can be accessed from outside company network.	CYT-00000617212
🟢	There is no service account inventory.	Establish a service account inventory containing service owner, review dates, and function.	CYT-00000174368

Appendix B

Open tasks by domain - Active Directory

ISSUE	RECOMMENDATION	ID
Without proper management and restrictions, privileged Active Directory accounts could experience increased vulnerability to unauthorized access, data breaches, malicious activities, insider threats, compliance violations and operational disruptions, potentially resulting in loss of trust.	Enhance privileged account security by reducing risks associated with privileged access.	CYT-60822830738
The absence of MFA for regular accounts can lead to increased susceptibility to unauthorized access, credential theft, phishing attacks and compromise sensitive data, potentially leading to security breaches and data loss.	Select and implement multi-factor authentication (MFA) across regular accounts.	CYT-37680927168
The absence of a robust monitoring and alerting system for Active Directory audit logs can result in missed opportunities for early detection of security incidents, potentially leading to unaddressed vulnerabilities and compromised network security.	Set up a monitor, analyze and alert system for audit logs.	CYT-92421521300
A lack of thorough and regular review of Active Directory logs can result in gaps in security monitoring, potentially leading to prolonged exposure to threats, data breaches and other malicious activities going unnoticed and unaddressed.	Enable the auditing and analysis of Active Directory logs.	CYT-66874302438
Irregular synchronizing and updating of identity management configurations across all tenants can lead to inconsistent security policies, potential access control issues, and increased vulnerability to cyber threats across the organization's digital environment.	Create a centralized identity management system for both multi-tenanted Entra ID and traditional Active Directory environments.	CYT-83497999913
An absence of regular updates to the list of trusted applications and the associated consent rules can leave an organization vulnerable to new or evolving cybersecurity threats that exploit outdated permissions or unreviewed applications, resulting in unauthorized access to sensitive data and systems, undermining the company's security posture and compliance with data protection regulations.	Set up controls and implement application consent practices with Entra ID Protection.	CYT-96114274366

Appendix B

Open tasks by domain - Asset Management

	ISSUE	RECOMMENDATION	ID
🔴	The company cannot validate whether hardware assets are end-of-life.	Evaluate hardware on an ongoing, monthly basis.	CYT-22656752867
🔴	The organization cannot plan the adequate protection levels for assets that store, process, and transmit sensitive information.	Categorize hardware and system assets according to their level of sensitivity as defined in the data protection policy.	CYT-00000395293
🔴	The company cannot validate whether or not software asset version is supported.	Only use vendor supported software versions.	CYT-00000575581
🟠	Failing to conduct regular reviews of critical systems supported by legacy technologies may result in unidentified vulnerabilities and security gaps, increasing the risk of cyberattacks.	Review critical systems supported by legacy technologies to identify potential vulnerabilities, upgrade opportunities, or new defense layers.	CYT-14756261722
🟠	The organization does not prevent the use of company assets for private purposes.	Do not allow private use of company assets, except when authorized.	CYT-00000112153
🟠	Missing assets which require protection are unaccounted for.	Do not allow for company assets to be sold, given as gifts, loaned, exchanged, or disposed of unless specifically authorized by management.	CYT-00000488800
🟠	The network architecture and interconnectivity is not documented.	Create a network diagram with identified high-risk environments.	CYT-00000311307
🟠	The company does not understand the types of sensitive data records that are stored, transmitted, or processed by its systems.	Document data flow between assets that have statutory, regulatory, or contractual compliance requirements.	CYT-00000183617
🟡	The company lacks precise marking of authentication and authorization systems in the current asset inventory, potentially exposing unidentified vulnerabilities and weakening security controls.	Correctly tag authentication and authorization systems in your asset inventory.	CYT-70676302526
🟡	The organization cannot adequately plan for business continuity requirements.	Document the relationships between assets and business services.	CYT-00000592219
🟡	Asset inventories are not kept up to date.	Update asset inventory when a device or software is installed, removed, updated, or changed.	CYT-00000617887
🟡	Media is not marked with the necessary information markings or distribution limitations.	Mark media with necessary information markings and distribution limitation.	CYT-00000958127

Appendix B

Open tasks by domain - Asset Management

	ISSUE	RECOMMENDATION	ID
🟡	Sensitive data is not removed from end-of-life or recycled media.	Require from assets' custodians to destroy media that cannot be sanitized.	CYT-00000939131
🟡	Sensitive data is not removed from end-of-life or recycled equipment.	Render data on electronic media unrecoverable, so that data cannot be reconstructed.	CYT-00000430657
🟡	There is no formal approval process to control the removal of assets out of company premises.	Ensure that assets are never taken out of company premises without an authorized approval and protect assets which have been taken out.	CYT-00000457288
🟡	The organization does not handle assets according to the classification of information sensitivity.	Develop procedures to handle assets according to classification of information sensitivity.	CYT-00000989255
🟡	Unauthorized hardware and software assets are not removed.	Remove any unauthorized hardware and software assets.	CYT-00000375233
🟡	Removable media is not securely handled.	Develop procedures to securely handle removable media.	CYT-00000243600
🟢	Sensitive printed information is not shredded.	Shred hardcopy materials so that sensitive data cannot be reconstructed.	CYT-00000084294

Appendix B

Open tasks by domain - Awareness

	ISSUE	RECOMMENDATION	ID
🔴	The company does not review and update policies, processes, and procedures	The policy, processes, and procedures are reviewed and updated annually.	CYT-32016267896
🔴	There is no process for ensuring employee commitment to company cybersecurity policy.	Ensure that all employees are aware of and have signed the company cybersecurity policy.	CYT-00000549414
🔴	There is no improvement protocol for company security awareness programs.	Collect and store training data.	CYT-00000906502
🟠	The organization does not provide physical security personnel with the necessary training on cybersecurity matters. This absence of effective cybersecurity awareness training leaves physical security personnel ill-equipped to manage and address incidents.	Provide cybersecurity awareness training for physical security personnel.	CYT-69955260505
🟢	Not providing basic cybersecurity awareness materials to customers may result in customers falling victim to phishing attacks impersonating the company, potentially leading to reputational damage and financial losses.	Ensure customer awareness materials are readily available.	CYT-27473034528
🟢	Failing to provide security awareness training to customers annually may result in customers being less vigilant about cybersecurity threats and more susceptible to cyberattacks.	Provide retail customers and commercial clients with cybersecurity awareness training information, at least annually.	CYT-28855738172
🟢	Using generic, company-wide security awareness training may result in employees not fully understanding the specific risks associated with their business unit, leading to inadequate protection against targeted threats.	Provide business units with cybersecurity training relevant to their particular department's risks.	CYT-60480630535

Appendix B

Open tasks by domain - Business Continuity

	ISSUE	RECOMMENDATION	ID
🟠	Not all business application data is backed up.	Back up critical application data both On-Premises and in the cloud, Software as a service (SaaS).	CYT-00000898474
🟠	Your company's external storage devices are not backed up properly.	Make sure to include in the regular backup routine critical data stored in company external storage devices, such as hard drives.	CYT-00000166736
🟠	Lack of an ICT Business Continuity Policy can result in potential operational disruptions and extended recovery times during system failures, leading to financial losses, customer dissatisfaction, and regulatory non-compliance.	Develop and implement an ICT Business Continuity policy	CYT-72004228835
🟠	Recovery processes are not tested.	Test recovery processes for different scenarios.	CYT-00000863314
🟠	Critical business data is not mapped or backed up.	Following the mapping of critical processes and related assets, map up critical data.	CYT-00000162393
🟠	There is no contingency plan in the case that the company's main office will be unavailable.	Prepare a separate site for deploying contingency plans for data centers and employee workplaces.	CYT-00000644939
🟠	Backups are not separated from your company's network.	Store backups in a separate dedicated network, that is connected to the main company network only when backing up data.	CYT-00000417997
🟠	Information processing facilities are not implemented or are implemented without sufficient redundancy to meet availability requirements.	Implement information processing facilities with redundancy sufficient to meet availability requirements.	CYT-00000879894
🟡	The company does not review and update policies, processes, and procedures.	The policy, processes, and procedures are reviewed and updated annually.	CYT-82952923042
🟡	Data backups are not encrypted.	Encrypt backups to prevent data theft or loss.	CYT-00000960166
🟡	There is no process to ensure RTO and RPO targets can be met.	It is important to verify the reliability of meeting the targets for Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).	CYT-00000192177
🟡	The company has not defined its RTO and RPO.	Define with management the RTO and RPO for each critical business process.	CYT-00000799600
🟢	Company workstation data is not backed up.	Create a process to back up critical data from employee workstations.	CYT-00000497322

Appendix B

Open tasks by domain - Card Payments

ISSUE	RECOMMENDATION	ID
Assets are not secured properly.	Document and verify the scope of PCI environment.	CYT-33511609873
Unauthorized access to cardholder data.	MFA is required for access into the cardholder data environment.	CYT-59336085929
Cardholder data is not stored securely	Primary Account Number (PAN) is secured where stored.	CYT-08037515048
Systems are not adequately protected	Perform risk analysis and management on the cardholder data environment.	CYT-84530105504
Cardholder data is not properly masked.	Primary Account Number (PAN) is secured wherever displayed.	CYT-95969140320
The company's payment page can introduce malicious code.	Implement anti-tampering measures within web pages.	CYT-01139383805

Appendix B

Open tasks by domain - Change and Configuration Management

ISSUE	RECOMMENDATION	ID
The company does not review and update policies, processes, and procedures.	The policy, processes, and procedures are reviewed and updated annually.	CYT-80535481384
Configurations are not standardized in the environment.	Baseline security requirements shall be established for all organization-owned or managed assets and should be based on industry-recognized practices.	CYT-00000895743
Change is not tracked and/or appropriately documented through its life cycle.	All changes to configurations should be logged.	CYT-00000995938
Unauthorized software can run on systems.	Only execution of authorized software, scripts, and libraries should be allowed.	CYT-00000839061
Changes to critical systems are not controlled.	The organization determines the types of changes that are configuration controlled.	CYT-00000614353
Changes that can cause a high-risk event or affect a critical business system are not monitored and controlled.	The organization approves configuration-controlled changes with explicit consideration for the security impact.	CYT-00000010966
Unauthorized changes are not detected.	Configuration monitoring should alert when unauthorized changes occur.	CYT-00000987655
Authorized software is not defined.	A list of authorized software and versions that are required for each platform should be documented.	CYT-00000772328
Configurations are not stored securely.	Master configurations or images should be stored securely.	CYT-00000418965
Changes that have affected the security and availability of the system cannot be tracked to understand the root cause of a failure.	Configuration-controlled changes are documented, reviewed, and audited.	CYT-00000507341
Physical and logical access restrictions associated with changes to organizational systems are not managed.	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	CYT-00000589102
Change is not controlled in the environment.	The organization tests, validates, and documents change to systems before implementing the change.	CYT-00000366116
The security risk to the organization is not understood before a change occurs.	The organization analyzes changes to information systems to determine potential security impacts before change implementation.	CYT-00000933706

Appendix B

Open tasks by domain - Change and Configuration Management

ISSUE	RECOMMENDATION	ID
Changes cannot be rolled back in the event of failure.	Any system whose changes cannot be tested must have the configuration backed up or a viable back-out plan in place before a change occurs.	CYT-00000701435
Configurations are not backed up.	At least the last three (3) previous versions should be retained.	CYT-00000496034

Appendix B

Open tasks by domain - Cloud Security

	ISSUE	RECOMMENDATION	ID
🔴	Failing to implement MFA can increase the likelihood of account compromise and unauthorized access to sensitive data.	Implement Multi-Factor Authentication (MFA) for all cloud services that support it, to enhance the security of user authentication.	CYT-00000530496
🟠	If minimum security requirements are not defined, the company may adopt cloud services that do not adequately protect sensitive data, leading to potential legal and regulatory penalties.	Define minimum security requirements for cloud services based on the company's risk tolerance and regulatory requirements.	CYT-63275835276
🟠	Lack of monitoring and alert systems may result in undetected unauthorized cloud services usage, increasing security risks and compliance issues.	Implement monitoring and alert systems to detect unauthorized cloud services usage.	CYT-99323166643
🟠	Failing to develop a data classification framework may result in data breaches, regulatory penalties, and damage to the company's reputation.	Develop a data classification framework that aligns with the company's risk tolerance and regulatory requirements.	CYT-14827350637
🟠	If appropriate access controls and security measures are not implemented, the company can face legal penalties, loss of intellectual property, and damage to its reputation.	Implement appropriate access controls and security measures based on data classification levels.	CYT-53043334952
🟠	No verification of security best practices and recommended controls are in place for your SaaS service providers.	Require security best practices for all SaaS services.	CYT-00000873052
🟠	Cloud services are not configured according to security best practices.	Configure all cloud services according to security best practices.	CYT-00000541183
🟡	If the chosen provider does not meet the company's technical and functional requirements, it can negatively impact productivity, collaboration, and overall business operations.	Identify and evaluate the required cloud service providers.	CYT-71803158031
🟡	Inadequate incident management can lead to long-term damage to the company's reputation, loss of customer trust, and increased operational costs.	Assess cloud service providers' history of security incidents and their resolutions.	CYT-27436051830
🟡	Choosing a provider without proper comparison can hinder the company's ability to adapt and compete in the market, limiting growth and innovation.	Compare the cloud service provider's offerings against established industry benchmarks and best practices.	CYT-91724803583

Appendix B

Open tasks by domain - Cloud Security

ISSUE	RECOMMENDATION	ID
If stakeholder responsibilities are not well-defined and documented, the company may experience security lapses, data breaches, and reduced accountability.	Define and document the specific responsibilities of each stakeholder in the cloud security ecosystem.	CYT-06167781007
Lack of training and guidance on secure cloud service usage can lead to security incidents, loss of sensitive data, and potential damage to the company's reputation.	Provide guidance and training to employees, contractors, and third-party users on the secure usage of cloud services.	CYT-08544870527
Lack of visibility into cloud service usage can hinder the company's ability to manage and secure its cloud assets.	Include relevant information in the inventory, such as service provider, type of service, and responsible department.	CYT-60820521350
Failing to implement SSO can lead to decreased user efficiency and increased risk of password-related security incidents.	Implement Single Sign-On (SSO) for cloud services that support it, to simplify and centralize user authentication.	CYT-00000001328
Not deploying CASB or SASE solutions can result in ineffective security policies and increased vulnerability to threats.	Deploy Cloud Access Security Broker (CASB) or Secure Access Service Edge (SASE) solutions to protect cloud services and applications by enforcing consistent security policies and monitoring user activities.	CYT-00000529472

Appendix B

Open tasks by domain - Compliance and Auditing

	ISSUE	RECOMMENDATION	ID
🔴	The company does not review and update policies, processes, and procedures.	The policy, processes, and procedures are reviewed and updated annually.	CYT-38081941330
🟠	Not attending to critical audit findings may increase vulnerability to cyber threats due to unaddressed critical issues, potentially leading to data breaches, system downtimes, and compromised integrity and confidentiality of information systems.	Establish a process for the verification and remediation of audit findings.	CYT-69433846093
🟠	Cybersecurity controls may need to be updated to ensure effectiveness.	Conduct cybersecurity control functional reviews.	CYT-00000969080
🟠	Not all company compliance requirements have been identified.	Identify all regulatory requirements and standards which apply to the company.	CYT-00000016508
🟠	There is no compliance and governance plan.	Establish a compliance and governance plan.	CYT-00000002079
🟡	There is no external audit of cybersecurity policies and protection processes.	Conduct periodic external audits of the company's cyber security policies and protection processes.	CYT-00000733894
🟢	Failing to ensure that threat intelligence aligns with the organization's risk posture and size may result in ineffective threat assessments and misalignment with the company's risk management strategy.	Ensure the internal audit validates that the threat intelligence received matches the organization's risk posture and size.	CYT-38720857610
🟢	Not updating the processes and procedures for internal audit evaluations in line with changes to the company's risk profile may result in misalignment between audit activities and risk management strategy.	Implement a process to update the internal audit function based on risk profile changes to the company.	CYT-11984182620
🟢	Failure to regularly review the organization's cybersecurity risk appetite statement may result in outdated risk tolerance guidelines and ineffective alignment with the company's risk management strategy.	Ensure the internal audit regularly reviews the cyber risk appetite statement.	CYT-45480328816

Appendix B

Open tasks by domain - Data Protection

	ISSUE	RECOMMENDATION	ID
🟠	Sensitive or private data is not encrypted at rest.	Encrypt sensitive data at rest.	CYT-00000791029
🟠	There are no formal agreements such as Service Level Agreements (SLAs), confidentiality or Non-Disclosure Agreements (NDAs), and data sharing agreements on the use third parties have of company data.	Create formal agreements such as Service Level Agreements (SLAs), confidentiality or Non-Disclosure Agreements (NDAs), and data-sharing agreements with third-party contractors.	CYT-00000356369
🟠	Data saved on removable media is not encrypted.	Encrypt data that is saved on removable media.	CYT-00000061221
🟠	There is no mapping of data according to the regulations or contractual agreements it needs to comply with.	Map all data types that are subject to regulations or contractual obligations and make sure they are protected according to compliance requirements.	CYT-00000604160
🟡	The organization's lack of strong, tailored security measures for sensitive data may expose integrity and confidentiality vulnerabilities, posing substantial risks to the organization and individuals involved.	Ensure the integrity of sensitive data.	CYT-87402626314
🟡	Access to sensitive data is not restricted and managed.	Manage sensitive data access and allow access strictly by necessity.	CYT-00000326735
🟡	Sensitive data transactions are not logged and monitored.	Record sensitive data transactions; then produce and review event logging.	CYT-00000762613
🟡	The use of removable storage devices in external systems is not limited.	Limit the use of removable storage devices in external systems.	CYT-00000364879
🟢	The information posted on public systems is not carefully monitored.	Monitor and control any information posted or processed on publicly accessible information systems.	CYT-00000456589
🟢	Outgoing and incoming transfers of sensitive information are not monitored or restricted.	Protect sensitive data flows by restricting outgoing and incoming data.	CYT-00000167544

Appendix B

Open tasks by domain - Domain and DNS

	ISSUE	RECOMMENDATION	ID
🟠	Access to a domain name registration and modification access is not enforced with Multi-Factor Authentication.	Enable access to domain registration only through multi-factor Authentication.	CYT-00000057467
🟠	The company domain name is not locked.	Lock all company-registered domain names to prevent unauthorized and unwanted transfers.	CYT-00000993630
🟠	Your company does not use established, secure public DNS servers.	Configure all DNS requests to go through a DNS filtering service or a gateway.	CYT-00000867450
🟠	A lack of comprehensive DNS logging means potentially overlooking early signs of security breaches or malware communication attempts.	Enable DNS query audit logging for detection and investigation of possible cyber-attacks and the targeting of the company DNS servers.	CYT-00000873292
🟡	Domain name renewal dates may be unmonitored.	Manage domain records renewal dates and renew prior to expiry.	CYT-00000092216
🟡	Company domains are not secured with DNSSEC.	Enable Domain Name System Security Extension (DNSSEC) for all registered domains.	CYT-00000374530
🟡	Your company does not limit internet access to its internal DNS server.	Enforce that company DNS server connectivity to the internet is always through an approved DNS resolver.	CYT-00000880006
🟢	Domain name backup details may be incorrect or incomplete.	Verify that domain registration records contain secondary contact details and payment methods.	CYT-00000972178

Appendix B

Open tasks by domain - Email and Messages

	ISSUE	RECOMMENDATION	ID
🔴	Anti-malware mechanisms are either missing or have not been configured.	Apply anti-malware tools.	CYT-00000756858
🟠	There is no advanced email protection tool implemented.	Implement an advanced email protection tool to handle advanced email attacks.	CYT-00000578636
🟠	Electronic messaging applications are not secured.	Secure electronic messaging applications used by the company.	CYT-00000419773
🟡	The organization lacks a cohesive strategy for managing and securing on-premise VoIP devices and SaaS VoIP applications, introducing the risk of mismanagement and security vulnerabilities.	Control and monitor Voice over Internet Protocol (VoIP) applications and devices.	CYT-58148355965
🟡	Email admin accounts are not separated from regular user accounts.	Admin account holders should have a separate user account for non-admin work.	CYT-00000169742
🟡	Company email can be accessed with only a password.	Require Multi-Factor Authentication on all company email accounts.	CYT-00000579275
🟡	The email content is transferred as cleartext.	Enforce encryption of emails containing sensitive materials.	CYT-00000312963
🟢	A mechanism to prevent outgoing email spoofing is missing or has not been configured.	Implement email authentication protocols for outgoing mail.	CYT-00000073202

Appendix B

Open tasks by domain - Endpoints and Mobile Devices

ISSUE	RECOMMENDATION	ID
The operating system of company workstations should be regularly updated.	Apply updates to the operating system regularly.	CYT-00000516172
Workstations are not locked following several failed login attempts.	Lock out after several failed login attempts.	CYT-00000115823
Workstations do not comply with your company's password policy.	Enforce strong password requirements.	CYT-00000823650
Not all company workstations employ an internal firewall.	Use an internal firewall for all company workstations.	CYT-00000677248
The company does not maintain an updated and comprehensive inventory of authorized software applications. Internet-connected software and extensions are not prioritized or appropriately documented. Unauthorized software may not be appropriately removed or documented.	Prevent unauthorized software installation on workstations	CYT-00000053930
The organization needs a unified strategy for mobile device management, as inconsistent practices are increasing vulnerabilities.	Create policies and procedures for mobile device usage.	CYT-41438173222
Failing to validate software versions and patches on mobile devices used for remote access may result in security gaps and non-compliance with security standards.	Validate software versions and patches for any mobile devices connecting to the corporate network for storing and accessing company information.	CYT-43536648264
Workstations are not centrally managed and controlled.	Ensure that all operating systems and hardware configurations are centrally managed.	CYT-00000309102
There are no requirements for local admin passwords.	Local admins should have a different and strong password for each admin account.	CYT-00000110981
Unmanaged personal workstations and devices can access company resources.	Restrict the connection of personal unmanaged workstations to company assets.	CYT-00000855803
There is no secure workspace for work-related applications on mobile devices.	Create a secure workspace for work-related applications on mobile devices.	CYT-00000012382
Collaborative computing devices may not give any indication when being activated.	Ensure that collaborative computing devices indicate activity to users when activated.	CYT-00000154301

Appendix B

Open tasks by domain - Endpoints and Mobile Devices

ISSUE	RECOMMENDATION	ID
There are no restrictions on the number of local admins per workstation.	Use only a minimal amount of local admin accounts, and make sure they are securely managed.	CYT-00000136241
Security patches are not regularly updated and applied to applications running on company workstations.	Apply application security patches on a regular basis to prevent attackers from exploiting known software vulnerabilities.	CYT-00000389462

Appendix B

Open tasks by domain - Environmental Control

ISSUE	RECOMMENDATION	ID
There is no temperature and humidity monitoring system.	Maintain acceptable temperature and humidity levels where company physical assets are stored.	CYT-00000934267

Appendix B

Open tasks by domain - Hosted Network

ISSUE	RECOMMENDATION	ID
Failing to adopt ZTNA principles and technologies can result in increased vulnerability to threats and diminished security effectiveness.	Adopt Zero Trust Network Access (ZTNA) principles and technologies to limit access to resources based on user identities, device context, and least privilege.	CYT-73833228857
There are no network traffic anomaly detection and prevention security controls.	Deploy network traffic anomaly detection and prevention security controls.	CYT-00000609986
Firewalls and network devices are not physically secured.	Maintain the safety of facilities containing network devices and equipment.	CYT-00000035613
Some network devices have not been patched.	Regularly update and patch company network infrastructure, e.g. firewalls and switches.	CYT-00000363506
Firewall logs are not continuously monitored.	Regularly monitor all company firewall logs.	CYT-00000766626
IP assets are using their real addresses when communicating to the internet.	Mask the IP addresses of network components and devices engaged in outgoing communication.	CYT-00000203293
There is no restriction on connecting any device (i.e unknown computers, mobile devices, memory sticks etc.) directly to your network.	Enforce company network device attestation.	CYT-00000060150
Firewall logs are not stored in external storage.	Store firewall logs in a system that is external to the system running the firewalls.	CYT-00000055226

Appendix B

Open tasks by domain - Hosted Server

	ISSUE	RECOMMENDATION	ID
🟠	Users are not locked out following several unsuccessful login accounts.	User lock-out following multiple unsuccessful attempts should be enforced on servers.	CYT-00000712527
🟠	Unused and unnecessary services or ports are open and ready for communication.	Uninstall or disable all unused or unnecessary services from company servers.	CYT-00000017744
🟠	Too many user accounts have administrative access to company servers.	Restrict administrative access to company servers to a limited number of authorized users.	CYT-00000866417
🟠	There is no approved software list for company servers.	Install only approved software on servers.	CYT-00000382705
🟡	Applications running on the server are not regularly updated and patched.	Regularly update all applications running on company servers and verify patches.	CYT-00000901447
🟡	There is no removable media anti-malware scan enforced.	For all removable media connected to company servers, configure an anti-malware scan.	CYT-00000644151
🟡	System or security event logging is not performed.	Log and monitor attempts to access unsupported servers.	CYT-00000919226
🟢	Not all company servers have a host-based firewall enabled.	On all company-hosted servers, implement a host-based firewall.	CYT-00000374914
🟢	Autorun and autoplay are not automatically disabled when connecting removable media.	For all removable media connected to company servers, disable autorun and autoplay.	CYT-00000070578

Appendix B

Open tasks by domain - Human Resources

	ISSUE	RECOMMENDATION	ID
🟠	Not addressing the concerns and grievances of unhappy employees in a timely and respectful manner may escalate the situation, potentially harming employee morale and organizational security.	Monitor and address unhappy or frustrated employees.	CYT-18445192848
🟠	Failure to promptly and appropriately address and resolve issues with risky or non-compliant employees can intensify the situation, negatively impacting both individual and organizational well-being and security.	Develop a procedure to address employees exhibiting risky behaviors	CYT-19052327169
🟠	There is no process for revoking an employee's access credentials when their employment is terminated.	Revoke all access credentials upon termination of employment.	CYT-00000688701
🟡	There is no process for updating employee access credentials upon employee role change.	Ensure that when employees are reassigned or their role changes, their access credentials, and authentications are reviewed and adjusted.	CYT-00000513886
🟡	Company data is not protected against misuse by employees or third-party contractors.	Ensure that HR incorporates a Non-Disclosure Agreement (NDA) or a similar confidentiality agreement that reflect the demands for protecting data and operational details, for both employee and third-party contracts.	CYT-00000610545
🟡	Employment contracts do not support the legal investigation of suspected misconduct.	Verify that all employment contracts allow the company the ability to investigate employee misconduct when there is reasonable evidence of policy violation or any information security breach.	CYT-00000112516
🟡	There are no rules and procedures for a clean desk and unattended user-equipment protection in employee and third-party contracts.	Ensure that HR incorporates the rules and procedures of a clean desk and unattended user-equipment protection in employee and third-party contracts.	CYT-00000669280
🟢	Failing to have an ongoing HR program for recruiting, retaining, and developing cybersecurity staff may lead to a shortage of qualified personnel, compromising the effectiveness of the organization's security programs.	Implement a program for talent recruitment, retention, and succession planning for the cybersecurity and resilience staff.	CYT-95771075299
🟢	Failing to establish a cybersecurity-related mindset and culture may result in employees making decisions that do not prioritize cybersecurity, potentially leading to security vulnerabilities.	Promote a risk culture requiring formal consideration of cybersecurity risks in all business decisions.	CYT-39716472902

Appendix B

Open tasks by domain - Incident Response

	ISSUE	RECOMMENDATION	ID
	The company does not review and update policies, processes, and procedures.	The policy, processes, and procedures are reviewed and updated annually.	CYT-35205858003
	Implementing changes to systems or access rights for incident management without formal approval may introduce security risks and vulnerabilities.	Ensure that any changes pertaining to incident management are approved by management prior to implementation.	CYT-74194826294
	Having no plans to re-route or substitute critical functions and services affected by a successful attack on internet-facing systems may result in disruptions to operations and services.	Provide plans to re-route or substitute critical functions and services that may be affected by a successful cyber attack.	CYT-07524877459
	Critical information gathering is missing from your incident response preparation phase.	Maintain an updated company asset inventory, including network topology and sensitive data locations.	CYT-00000791067
	Roles and responsibilities are not clearly defined in case of an incident.	Designate key roles and responsibilities to manage and handle cyberattacks.	CYT-00000410441
	No third-party Incident Response (IR) support.	Engage a third-party incident response vendor for fast response and post-incident reviews.	CYT-00000373508
	No measures are taken towards preventing the expansion of incidents.	Prevent an expansion of an incident and contain it.	CYT-00000606697
	Individuals involved in the unauthorized use or disclosure of personal information, which caused a security incident, are not sanctioned.	Sanction individuals involved in unauthorized use or disclosure of personal information.	CYT-00000097791
	Detection and prevention tools and techniques are not improved after a cyber incident had occurred.	Improve detection and prevention tools and techniques after a cyber incident had occurred.	CYT-00000487586
	Failing to conduct resilience testing aligned with realistic and emerging threats may leave the institution unprepared to respond effectively to actual cyber incidents.	Perform resilience testing based on analysis and identification of realistic and highly likely threats.	CYT-09489481954
	Failing to reconfigure and thoroughly test restored assets before putting them back into operation may result in security weaknesses and vulnerabilities.	Establish processes that ensure restored assets are appropriately reconfigured and thoroughly tested prior to operating.	CYT-50676351900

Appendix B

Open tasks by domain - Incident Response

	ISSUE	RECOMMENDATION	ID
🟡	Not quarantining, removing, disposing of, or replacing assets affected by a security incident may result in ongoing security vulnerabilities and potential re-infections.	Implement processes for assets affected by a security incidents.	CYT-96324412294
🟡	There is no employee awareness covering cyber incidents and employees' roles in them.	Ensure employees are aware of their respective roles in main incident scenarios.	CYT-00000776300
🟢	Not preparing an annual report of security incidents may result in a lack of transparency and awareness of security issues among the board and relevant stakeholders.	Produce an annual board report consisting of security incidents or violations.	CYT-28771812576
🟢	Not actively participating in sector-specific cyber exercises or scenarios may result in insufficient incident response capabilities and preparedness.	Ensure the company engages in sector-specific cyber exercises or scenarios.	CYT-68368038235

Appendix B

Open tasks by domain - Information Security Management

	ISSUE	RECOMMENDATION	ID
●	The company does not have a full set of cybersecurity policies and guidelines.	Create cybersecurity policies consistent with company business goals, and assessed risks, threats, and relevant regulatory requirements.	CYT-00000635874
●	Ineffective internal and external communication of vital cybersecurity information within the company creates the potential for misunderstandings, misalignment, and inadequate response to cyber threats.	Implement effective internal and external information communication processes.	CYT-30435099779
●	The absence of an information management system for cybersecurity controls could deprive the organization of high-quality information required to sustain effective cybersecurity measures, potentially resulting in delayed identification and response to cybersecurity incidents.	Establish procedures and protocols to reliably identify, capture, and categorize high-quality cybersecurity control information.	CYT-58525657230
●	Information-security authorities and special interest groups are not identified and cannot be appropriately contacted.	Identify the relevant information-security authorities and special interest groups, and maintain appropriate contact.	CYT-00000203001
●	There is no identification of internal and external issues affecting company cybersecurity policies.	Identify all internal and external issues affecting company cybersecurity policies.	CYT-00000820950
●	Failing to assess the risks posed by external critical infrastructure could leave the company unprepared for disruptions, potentially leading to operational failures.	Ensure any critical infrastructure risks that could affect the institution are considered.	CYT-82672974730
●	Without an annual report, the board may lack crucial insight into the state of information security and business continuity programs, potentially leading to uninformed decision-making.	Provide a management report to the board detailing the overall status of information security and business continuity programs.	CYT-20983795950
●	The absence of threat intelligence and security posture metrics from a board meeting may result in the board lacking critical insights into emerging cyber threats and the company's security readiness.	Address threat intelligence trends and the organization's security posture, in order to enhance the board meeting package.	CYT-19661001886
●	Without a board approved cyber risk appetite statement, the company may lack a clear framework for managing cyber risks, potentially leading to inconsistent risk management practices.	Produce a cyber risk appetite statement for the organization and gain board approval.	CYT-56064130724

Appendix B

Open tasks by domain - Information Security Management

ISSUE	RECOMMENDATION	ID
Cybersecurity policies are not communicated.	Communicate cybersecurity policies and ensure that they are acknowledged within the company and relevant stakeholders.	CYT-00000646586

Appendix B

Open tasks by domain - Logging and Monitoring

ISSUE	RECOMMENDATION	ID
Failure to check trade reports for completeness could lead to inaccurate financial reporting and decision-making, resulting in compliance issues and financial losses. It may also undermine the credibility and reliability of data used for critical business operations.	Implement routine system checks on trade reports	CYT-34394501163
Failing to implement tools to detect unauthorized data mining may result in insider threats and data breaches.	Implement the use of tools to detect unauthorized data mining.	CYT-53354755912
Unreliable event detection processes may result in missed security events and delayed responses to incidents.	Ensure that event detection processes are proven reliable.	CYT-84895482286
Log record is not configured to include enough details to allow proper cyber-incident or attack investigations.	Configure log recording to include, at least, event timestamp, event data, source and target of activity, user account identifier, process identifier, file name, and success or failure.	CYT-00000301571
Actions of high-privilege users are not logged.	Define actions of high-privilege users as an event type.	CYT-00000543844
Critical events in sensitive and business assets are not logged.	Define critical events in sensitive and business assets as event types.	CYT-00000454915
Indicators of Compromise (IoCs) are not logged.	Define Indicators of Compromised (IoC) data as an event type.	CYT-00000987925
Endpoint device security-related events are not logged.	Define endpoint device security-related event logs as an event type.	CYT-00000001346
The organization lacks a structured approach for communicating detected alerts and potential incidents, hindering swift and effective cybersecurity threat responses.	Establish communication protocols for detected alerts and potential incidents.	CYT-78901531554
The organization lacks consistent testing and enhancement of monitoring and detection procedures, which may overlook emerging threats or anomalies, posing a security breach risk.	Regularly test and enhance monitoring and alert systems.	CYT-80263638058

Appendix B

Open tasks by domain - Logging and Monitoring

	ISSUE	RECOMMENDATION	ID
🟡	The company lacks confirmation of detection activity compliance, potentially leading to inadvertent breaches of pertinent legal, regulatory, and contractual obligations, encompassing data protection, privacy, and industry-specific norms.	Verify that detection activities are compliant with legal requirements.	CYT-69549661424
🟡	Log file security-access controls are not configured to prevent unauthorized accounts from making alterations.	Configure security-access controls for log files, including modification and deletion privileges.	CYT-00000869040
🟡	There is not enough log-file storage space.	Allocate enough logging and monitoring storage space to comply with company logging and monitoring retention requirements.	CYT-00000017161
🟡	Log records are not backed up on a separate system than the system creating the logs.	Periodically back up log records and store those records in a system separated from the system conducting the monitoring.	CYT-00000798631
🟡	Network traffic is not logged.	Define network traffic as an event type.	CYT-00000831279
🟡	The company does not have a mechanism for setting thresholds for incident alerts, which may result in overlooking potential attacks or significant security events.	Apply alert thresholds and identify potential attacks	CYT-00000959963
🟡	The company does not monitor personnel activities, leaving it exposed to potential internal threats and making it difficult to detect and prevent insider incidents or unauthorized behavior.	Implement personal activity monitoring	CYT-00000405010
🟡	Log storage does not process for deleting logs that are not needed for operational purposes.	Do not keep logs containing private information for longer than required by regulation or for incident investigation.	CYT-00000322620
🟡	External security information is not reviewed and analyzed.	Periodically review and analyze external security information.	CYT-00000605647
🟢	Configuration changes to firewalls and network devices are not logged.	Define changes to firewalls and network device rules and configurations as an event type.	CYT-00000360783

Appendix B

Open tasks by domain - On-Premises Network

ISSUE	RECOMMENDATION	ID
Failing to adopt ZTNA principles and technologies can result in increased vulnerability to threats and diminished security effectiveness.	Adopt Zero Trust Network Access (ZTNA) principles and technologies to limit access to resources based on user identities, device context, and least privilege.	CYT-74127491848
Firewalls and network devices are not physically secured.	Maintain the safety of facilities containing network devices and equipment.	CYT-00000465756
IP assets are using their real addresses when communicating to the internet.	Mask the IP addresses of network components and devices engaged in outgoing communication.	CYT-00000049464
There are no network traffic anomaly detection and prevention security controls.	Deploy network traffic anomaly detection and prevention security controls.	CYT-00000101697
Firewalls have not been properly configured (hardened).	Harden company firewall configurations.	CYT-00000850508
Potentially insecure communication between different company sites.	Secure and encrypt communications between two or more company sites.	CYT-00000713966
Failing to configure perimeter firewalls for wireless network environments to restrict unauthorized traffic may result in unauthorized access to wireless networks and potential security breaches.	Implement and configure any wireless network environments with perimeter firewalls to restrict unauthorized traffic.	CYT-35444853947
Failing to extend monitoring controls to cover all internal network-to-network connections may result in undetected unauthorized activities and potential security breaches within the company's internal network.	Establish monitoring controls for the coverage of all internal, network-to-network connections.	CYT-47442597480
The absence of posture checking tools to automatically block access from unpatched devices may result in security vulnerabilities and potential breaches.	Use tools to automatically block attempted access from unpatched employee and third-party devices.	CYT-79701691554
Allowing the broadcast range of wireless network(s) to extend beyond company-controlled boundaries may expose the network to unauthorized access from outside secure areas, increasing the risk of security breaches.	Confine broadcast range of the wireless network(s) to company-controlled boundaries.	CYT-60843423896
Switches are not configured securely.	Harden switches configuration according to security best practices.	CYT-00000989947

Appendix B

Open tasks by domain - On-Premises Network

	ISSUE	RECOMMENDATION	ID
🟡	There is no restriction on connecting any device (i.e. unknown computers, mobile devices, memory sticks, etc.) directly to your network.	Enforce company network device attestation.	CYT-00000197910
🟡	Some network devices have not been patched.	Regularly update and patch company network infrastructure, e.g. firewalls and switches.	CYT-00000085421
🟡	Firewall logs are not continuously monitored.	Regularly monitor all company firewall logs.	CYT-00000479472
🟡	The company's Wi-Fi router does not require users to authenticate themselves.	Protect wireless access using authentication.	CYT-00000017905
🟡	Your company's Wi-Fi routers' firmware is not regularly updated.	Regularly update Wi-Fi firmware.	CYT-00000635957
🟡	Your company's Wi-Fi routers' firewall is not activated.	Set the Wi-Fi router's internal firewall to be activated.	CYT-00000496486
🟡	There are no dedicated computing resources for administrative management tasks.	Perform network administrative management tasks only by using dedicated computing resources.	CYT-00000565897
🟢	Firewall logs are not stored in external storage.	Store firewall logs in a system that is external to the system running the firewalls.	CYT-00000397534
🟢	The company's Wi-Fi routers use their default network name (SSID).	Discard the Wi-Fi network's default name and create a new one.	CYT-00000732581

Appendix B

Open tasks by domain - On-Premises Server

	ISSUE	RECOMMENDATION	ID
🔴	Applications running on the server are not regularly updated and patched.	Regularly update all applications running on company servers and verify patches.	CYT-00000371537
🔴	A strong password policy is missing or not enforced.	Enforce a strong password policy for all connections to company servers, including connections through consoles, remote connections, or local logins.	CYT-00000979306
🟠	Users are not locked out following several unsuccessful login accounts.	User lock-out following multiple unsuccessful attempts should be enforced on servers.	CYT-00000327236
🟠	Antivirus or Anti-Malware solutions are not installed or are not up to date.	Implement anti-malware and anti-virus mechanisms on all servers.	CYT-00000829911
🟠	There is no approved software list for company servers.	Install only approved software on servers.	CYT-00000366830
🟠	The default-account credentials of one or more servers and applications were not modified.	Modify server default account credentials.	CYT-00000783251
🟡	Unused and unnecessary services or ports are open and ready for communication.	Uninstall or disable all unused or unnecessary services from company servers.	CYT-00000104481
🟡	Server communication is not encrypted or secured.	Verify all communication flow from and to company servers is protected, encrypted, and monitored.	CYT-00000043215
🟢	Not all company servers have a host-based firewall enabled.	On all on-premises company servers, implement a host-based firewall.	CYT-00000487742
🟢	Autorun and autoplay are not automatically disabled when connecting removable media.	For all removable media connected to company servers, disable autorun and autoplay.	CYT-00000815208

Appendix B

Open tasks by domain - Operational Technology (OT) Security

	ISSUE	RECOMMENDATION	ID
●	If unidirectional outgoing connections are not securely managed, the risk of unauthorized access and data compromise escalates, emphasizing the critical need for implementing and maintaining secure and approved solutions for unidirectional information transmissions.	Implement unidirectional outgoing connections for OT networks.	CYT-24738948415
●	The absence of measures to securely disable remote modification and shutdown functionalities can expose environmental networks and sensors to potential unauthorized access, alterations, and disruptions, compromising the effectiveness of environmental monitoring systems.	Secure remote access to environmental network and sensors.	CYT-98268104453
●	The absence of unique, robust passwords, aligning with organizational password policies, for each OT component can significantly escalate the systems' susceptibility to unauthorized access and subsequent security breaches.	Implementing unique strong passwords for OT components.	CYT-62338250698
●	If secure access protocols for mobile devices to OT components are not diligently implemented and monitored, there's a heightened risk of breaches due to insecure or unauthorized access.	Secure mobile access to OT components.	CYT-04027125317
●	A lack of stringent measures and regular checks to secure OT components against unauthorized remote control can expose operational systems to significant risks, including system manipulation and data breaches.	Prohibit unauthorized remote control of OT components.	CYT-07877114190
●	The lack of secure configuration locking mechanisms can result in vulnerabilities, making environmental sensors and devices susceptible to unauthorized access and modifications, compromising the integrity of the environmental data collected.	Secure the configurations of environmental sensors and devices.	CYT-50127092758
●	The lack of secure and authenticated instruction delivery protocols and compliance enforcement can expose OT components to operational and security risks due to unauthorized or incorrect instructions being followed.	Provide secured operational and maintenance instructions for OT components.	CYT-77592286302

Appendix B

Open tasks by domain - Operations and Maintenance

	ISSUE	RECOMMENDATION	ID
🔴	The company does not review and update policies, processes, and procedures.	The policy, processes, and procedures are reviewed and updated annually.	CYT-62344036033
🟠	Protections are not designed for defense-in-depth.	Systems have layered protections.	CYT-00000293320
🟠	Security is not included in enterprise planning.	The enterprise architecture includes security requirements.	CYT-00000934256
🟠	Security is planned into projects.	Information security shall be addressed in project management, regardless of the type of the project.	CYT-00000187562
🟠	New systems are not verified for functionality.	New systems and applications must be tested for functionality before being put into production.	CYT-00000448596
🟠	Equipment should be correctly maintained to ensure its continued availability and integrity.	Infrastructure and hardware maintenance is scheduled and documented in accordance with manufacture specifications.	CYT-00000651276
🟠	Multi-Factor Authentication is not required for remote maintenance sessions.	Ensure that Multi-Factor Authentication is used to establish secure, remote maintenance sessions through external network connections.	CYT-00000287973
🟠	Maintenance personnel's activities are not supervised.	Supervise the maintenance activities of the maintenance personnel.	CYT-00000819155
🟡	There is no separation of duties between development, and production environments.	Utilize a separation of duties between development, and production environments.	CYT-00000738316
🟡	The organization lacks strong integrity-checking mechanisms for in-house and third-party software, firmware, hardware, and data, leaving vulnerabilities due to compromised or altered elements. This exposes the organization to risks like security breaches, data loss, and regulatory non-compliance.	Implement integrity-checking mechanisms for in-house and third-party software, firmware, hardware, and information.	CYT-77388167141
🟡	A lack of a well-organized process for obtaining, utilizing, and sharing pertinent, high-quality information on operational systems and processes within the company may lead to inefficiencies, miscommunications, and subpar decision-making.	Generate, use, and communicate quality information for operational systems and processes. Establishing Information Management and Communication Procedures for Operational Systems and Processes	CYT-18611045161

Appendix B

Open tasks by domain - Operations and Maintenance

	ISSUE	RECOMMENDATION	ID
🟡	The company lacks effective procedures to verify system inputs, processing, and outputs. This absence of verification controls jeopardizes data accuracy, system performance, and data security, posing potential breaches.	Establish verification protocols for system inputs, processing, and outputs.	CYT-22513964399
🟡	Due diligence is not performed for acquisitions.	The enterprise IT architecture is used in all development and acquisitions.	CYT-00000939328
🟡	Off-site maintenance is not controlled.	Infrastructure and hardware maintenance activities are controlled where being performed on-site or remotely.	CYT-00000132709
🟢	The company does not measure capacity and plan for future demand.	Projections are made to plan for future growth and capacity requirements to reduce the risk of system overload	CYT-00000706414

Appendix B

Open tasks by domain - Passwords and Secrets

	ISSUE	RECOMMENDATION	ID
🔴	Password complexity rules are not enforced.	Enforce password complexity rules on all assets.	CYT-00000784598
🟠	The absence of a dedicated policy and process for passwords and secret authentication leaves the organization without a structured approach to credential management, leading to inconsistent practices, mishandling, and increased susceptibility to cybersecurity risks.	Create a policy and management process for passwords and secret authentication information.	CYT-69380916206
🟠	Users may email their password to colleagues, or as a reminder to themselves.	Prohibit sharing passwords in plain text via email.	CYT-00000577073
🟠	Employees may be using the same password for numerous accounts and services.	Make sure that employees are not using the same password for different user accounts, including their personal accounts.	CYT-00000678163
🟠	Employees are not aware of the value of strong passwords and how to create them.	Educate employees on the value of strong passwords, and how to create them.	CYT-00000106274
🟠	Employees may share passwords between them.	Prohibit password sharing.	CYT-00000895649
🟠	Users may store passwords in locally saved, unencrypted files.	Prohibit storing passwords in clear text on local files.	CYT-00000618272
🟠	Users are not required to change an initial default password.	All users should change their passwords on their first login.	CYT-00000173037
🟠	Passwords or secrets may be delivered to employees in an insecure manner.	Deliver or give over passwords to employees in a secure manner.	CYT-00000038083
🟠	Password history limit is not enforced or is set too low.	Enforce a password history limit for all passwords.	CYT-00000694130
🟡	The company lacks appropriate procedures for storing and transmitting cryptographically-protected passwords and secrets, creating potential security weaknesses and non-compliance with industry standards and regulations.	Use cryptology algorithms and techniques to store and transmit passwords and secrets.	CYT-46806411020
🟡	Users may write passwords on post-it notes.	Do not write passwords on any visible medium, such as Post-it Notes.	CYT-00000484886
🟢	Password minimum age is not enforced.	Enforce a password Minimum age for all passwords.	CYT-00000840846

Appendix B

Open tasks by domain - Physical Infrastructure

ISSUE	RECOMMENDATION	ID
No physical access control of dedicated communication and computing areas.	Control, record, secure and enforce physical access authorization to company communication and computing areas, such as server rooms and communication cabinets.	CYT-00000996872
Undetected intrusion or security incidents, resulting in potential theft, vandalism, or damage to company assets.	Install and maintain alarm systems in critical areas of company facilities, such as server rooms, communication cabinets, and entry and exit points.	CYT-85191665143
The organization inadequately safeguards IT equipment against potential environmental hazards, leaving essential infrastructure vulnerable. This absence of protective measures heightens exposure to environmental threats and amplifies the risk of unauthorized access, potentially causing severe disruptions and financial setbacks.	Implement physical security measures for IT equipment.	CYT-86108571158
Without adequate physical protection and network segregation, security cameras and surveillance systems remain vulnerable to unauthorized access, tampering, and malicious interference, posing significant security risks to the organization.	Implement physical protection and network segregation for security cameras and surveillance systems.	CYT-79755677295
Lack of a secure deposit system and clear, enforceable policies may result in non-compliance, allowing unauthorized devices in sensitive areas and exposing the organization to potential security threats.	Implement mandatory deposit of personal devices for visitors and external technicians.	CYT-29634626747
The company lacks a standardized process for escorting and monitoring visitors, introducing inconsistencies and potential security vulnerabilities.	Escort visitors and monitor visitor activity within the company premise.	CYT-00000787888
Secure areas are not appropriately protected.	Implement procedural measures to protect secure areas.	CYT-00000487257
Sensitive assets such as removable media are not physically protected.	Physically protect sensitive assets and removable storage devices, such as portable hard drives and laptops.	CYT-00000905568
Physical access devices are not properly managed.	Create a physical access device inventory and track devices' activity.	CYT-00000933945

Appendix B

Open tasks by domain - Physical Infrastructure

	ISSUE	RECOMMENDATION	ID
●	Delivery and loading areas are not appropriately protected.	Protect delivery and loading areas.	CYT-00000381161
●	No physical controls are in place to protect devices with sensitive outputs.	Control physical access to output devices such as printers and copiers connected to systems containing sensitive information.	CYT-00000431987

Appendix B

Open tasks by domain - Privacy

	ISSUE	RECOMMENDATION	ID
	Not being compliant with data privacy regulations.	Assign qualified individuals, roles, and responsibilities for managing the privacy program.	CYT-75842959380
	Inaccurate inventory makes it difficult to assess risks and identify the necessary controls to protect personal data.	Make an inventory of personal data and make sure it is documented.	CYT-15253220286
	Processing personal data without the knowledge or consent of the data subject.	Provide individuals with clear options to either allow or prohibit (opt out) the processing of personal data.	CYT-74926913707
	Possession of personal data without consent.	Prohibit the processing of personal data prior to receiving consent to do so.	CYT-54460387784
	Users cannot withdraw consent for the use of their data.	Provide individuals with a way to revoke consent to process their personal data.	CYT-03897561271
	Personal data is used for purposes that the individual has not authorized.	Provide individuals with the option to consent or opt out of selling or monetizing their personal data.	CYT-36193616786
	Without the comprehension of how personal data flows within their systems, the organization may be unable to recognize potential vulnerabilities and may not implement sufficient safeguards to protect the security of the personal data.	Include personal data processing activities in a data flow diagram.	CYT-42288144897
	Data is not adequately protected.	Identify and document personal data custodians.	CYT-44303142065
	Failure to remove personal data when no longer necessary.	Retain personal data for only the authorized period of time.	CYT-05290073085
	Data is stored outside an authorized region.	Ensure compliance with any geographic data location restrictions.	CYT-75131986422
	There is unauthorized access to personal data.	Where possible, make personal data exportable.	CYT-33963005251
	Disclosures of personal data are not documented.	Manage and document internal and external disclosures of personal data.	CYT-76041786907
	The organization is not proactive in maintaining personal data accuracy.	Correct flaws in personal data upon identification.	CYT-73801660248
	The organization fails to allow individuals access to their personal data.	Provide individuals with access to their personal data.	CYT-93659411212

Appendix B

Open tasks by domain - Privacy

	ISSUE	RECOMMENDATION	ID
🟠	The organization holds outdated or incorrect data.	Provided individuals with a way to correct or amend their personal data.	CYT-96949817036
🟡	Ignoring grievances from individuals can lead to increased scrutiny from regulators, resulting in a loss of reputation.	Provide a grievance process for individuals that challenge company adherence to policy.	CYT-57760822953
🟡	Service providers do not properly handle the company's consumer personal data.	Implement a process for the handling of personal data by service providers.	CYT-45186167661
🟡	Customers are not informed of the financial incentives of sharing personal information.	Notify consumers of any financial incentives associated with the exchange of personal information.	CYT-35147419568
🟡	The company does not verify the requestor of personal information.	Establish a verification process for consumer information requests.	CYT-78288903464
🟢	The company does not have required documentation of privacy data requests.	Ensure all privacy data requests are logged and kept.	CYT-00520247525
🟠	Non-compliance with the handling of fraudulent requests to limit the use and disclosure of sensitive personal information could expose an organization to legal penalties, financial losses, and reputational damage.	Establish a process for handling fraudulent requests to limit data use.	CYT-57900272341
🟡	The company does not verify adequately a consumer opt-it after an opt-out.	Establish a two-step opt-in process for data monetization after opting out.	CYT-38943078734

Appendix B

Open tasks by domain - Remote Access

ISSUE	RECOMMENDATION	ID
Remote users are not locked out following several failed login attempts.	Lock out remote user accounts after several failed login attempts.	CYT-00000489625
Users' remote access to company assets does not require two factor authentication.	Require Multi-Factor Authentication for account users to remotely access company assets.	CYT-00000522580
Remote access sessions are not controlled and managed.	Manage and control remote access sessions using access control points.	CYT-00000488629
Remote access to security-sensitive data and information is not restricted.	Restrict remote access to security-sensitive data and information.	CYT-00000521864
Unauthorized or overuse of remote access to company data will not be detected.	Log and monitor remote access to company data and assets	CYT-00000464605
Data can not be remotely wiped from mobile devices.	Make sure that the company can remotely wipe or delete its proprietary data from stolen or lost devices or in cases of employee termination.	CYT-00000777915
There is no defined termination time or process of remote access sessions after idle period.	Terminate remote access connection according to predefined conditions.	CYT-00000135462
Company users can use public Wi-Fi networks to access company assets.	Do not use public Wi-Fi except under exceptional circumstances and with the needed precaution and protection controls.	CYT-00000321483

Appendix B

Open tasks by domain - Risk Management

	ISSUE	RECOMMENDATION	ID
🔴	The company does not review and update policies, processes, and procedures.	The policy, processes, and procedures are reviewed and updated annually.	CYT-60895080478
🟠	Failure to ensure the independent testing for ICT systems includes potential exposure to unresolved security vulnerabilities and biases in system evaluations, which can lead to severe security incidents and regulatory non-compliance, ultimately affecting the organization's operational stability and trustworthiness.	Establish measures to ensure independent testing.	CYT-46455034225
🟠	Failing to report lessons learned could leave management uninformed about potential vulnerabilities and areas needing improvement, hindering proactive risk management and strategic planning.	Establish a process for compiling and presenting a report on lessons learned to management.	CYT-24658866057
🟠	Failing to identify and enhance authentication controls for internet-based systems and high-risk transactions may result in increased vulnerability to cyberattacks targeting critical assets.	Ensure the risk assessment identifies internet-based systems and high-risk transactions that require additional authentication controls.	CYT-80251144685
🟠	There is no cybersecurity risk remediation plan.	Establish a cybersecurity risk remediation plan.	CYT-00000558447
🟠	Cybersecurity risks cannot be identified since there is no risk assessment.	Conduct risk assessment to identify, rank, mitigate, and monitor cybersecurity risks.	CYT-00000795670
🟡	There is no monitoring and tracking of cybersecurity risks.	Monitor and track cybersecurity risks.	CYT-00000994005
🟡	The company is not covered by a cybersecurity insurance.	Acquire cybersecurity insurance to protect company assets against potential cybercrime destruction.	CYT-00000115481
🟢	Cybersecurity improvements are not aligned with business strategy	Establish a process to identify, evaluate and implement strategic opportunities	CYT-56853659998
🟢	Neglecting to address non-technological risks (e.g.: financial, strategic, regulatory, and compliance risks) in the risk management program may lead to unanticipated consequences and losses.	Include non-technological cyber risks in the company's risk management program.	CYT-44502389556

Appendix B

Open tasks by domain - Risk Management

ISSUE	RECOMMENDATION	ID
Failing to calculate and understand the impact of cybersecurity incident losses per business unit or department may result in misallocation of resources and an inadequate response to incidents.	Implement a process to analyze and assign potential losses and expenses related to cybersecurity incidents, per business unit.	CYT-86567805363
Neglecting to adjust the risk assessment process to consider widely known risks and best practices may lead to inadequate risk management and failure to address known threats effectively.	Adjust the risk assessment for widely known risks or common risk management practices.	CYT-44451984968
Not monitoring and remediating high residual risks from risk assessments may result in unaddressed vulnerabilities and potential security incidents.	Monitor moderate and high residual risk issues from the cybersecurity risk assessment until items are addressed.	CYT-23838603045
Not presenting and discussing cybersecurity at independent risk management meetings may result in a lack of focus on cyber risks and inadequate risk management.	Present and discuss cyber risk reports at independent risk management meetings.	CYT-45992244421

Appendix B

Open tasks by domain - Service Provider and Vendor Management

	ISSUE	RECOMMENDATION	ID
🔴	The company does not review and update policies, processes, and procedures.	The policy, processes, and procedures are reviewed and updated annually.	CYT-71517517562
🟠	The risk gap of not undertaking third-party subcontractor risk assessments is increased vulnerability to security breaches and compliance failures, due to insufficient oversight of extended service chains.	Ensure that third-party subcontractor risk is evaluated.	CYT-96600402296
🟠	The absence of a designated role for monitoring third-party service providers could lead to inadequate oversight and unmitigated risks in external service delivery.	Implement monitoring of third-party service providers.	CYT-54933582121
🟠	Failing to establish procedures for monitoring and testing third-party connections may result in unmanaged security risks and vulnerabilities in external connections.	Monitor and test controls for primary and backup third-party connections on a regular basis.	CYT-80481403917
🟠	There is no process for following changes to service-provider services, regulations, and security policies.	Keep a detailed inventory of each service provider and vendor.	CYT-00000418529
🟡	The company lacks a well-defined Service Provider Management Policy or neglects regular reviews and updates, potentially leading to inconsistencies and heightened vulnerabilities in service provider management.	Establish and maintain a Service Provider Management Policy.	CYT-60004961072
🟡	Failing to review due diligence results and management's recommendations regarding third-parties may result in insufficient oversight of external partners and potential risks.	Ensure the board, board committee or appointed professional reviews a summary of due diligence results including management's recommendations regarding the use of third-parties.	CYT-08119651130
🟡	Not conducting pre-contract physical site visits of high-risk vendors may lead to the inadequate assessment of vendor security and reliability.	Arrange physical, pre-contract site visits of high-risk vendors by the company or a qualified third-party.	CYT-89925731888
🟡	Failing to implement automated reminders for third-party information collection may result in outdated or incomplete information, hindering effective risk management.	Implement automated reminders to identify when required third-party information needs to be obtained or analyzed.	CYT-87709970352

Appendix B

Open tasks by domain - Service Provider and Vendor Management

	ISSUE	RECOMMENDATION	ID
●	Failing to design and verify security controls for detecting and preventing intrusions from third-party connections may expose the company's systems to unauthorized access and security breaches.	Ensure security controls are designed and verified to detect and prevent intrusions from third-party connections.	CYT-10205531696
●	Not scaling the monitoring of third-parties based on risk may result in misallocation of resources and attention, leaving high-risk third-parties inadequately monitored.	Align the monitoring of third-parties in accordance with the associated risk they pose.	CYT-67261660292
●	The absence of monitoring controls covering all external connections may result in limited visibility into potential threats and security incidents involving third-party service providers, business partners, and customers.	Establish the use of monitoring controls to cover all external connections (e.g.: third-party service providers, business partners, customers).	CYT-28368252719
●	If the organization doesn't focus on cybersecurity requirements with vendors and service providers or doesn't differentiate based on influence, there might be a risk of misalignment and unexpected threats from third-party relationships.	Ensure service provider and vendor contracts define security requirements.	CYT-00000482316
●	Service providers and vendors could expose the company to security threats.	Ensure service provider and vendor contracts define security requirements and legally require notifying within a reasonable time of any security weakness that can influence the company.	CYT-00000201093
●	Failing to implement a process to identify new third-party relationships, including those established without formal approval, may result in a lack of visibility into potential security risks.	Establish a process to identify new third-party relationships, including those that were established without formal approval.	CYT-93026290521
●	There is no secure service provider or vendor decommission process.	Securely decommissioned service providers a vendors.	CYT-00000399299

Appendix B

Open tasks by domain - Software Development

ISSUE	RECOMMENDATION	ID
The company does not review and update policies, processes, and procedures.	The policy, processes, and procedures are reviewed and updated annually.	CYT-23916341383
No tools are used to improve software development process security.	Adopt supporting tools to improve software development security.	CYT-00000684484
There is no defined process for reviewing code.	Perform code review and apply code analysis tools to identify vulnerabilities and verify compliance with security requirements.	CYT-00000065333
Secure design principles are not applied in software architecture.	Apply secure design principles in software architecture and follow code best practices.	CYT-00000008125
There is no process for verifying that third-party software components are trusted or up-to-date.	Use only up-to-date and trusted third-party software components.	CYT-00000012091
Software releases are not archived.	Archive and protect software releases.	CYT-00000942651
Software development infrastructure security requirements are not identified and cannot be properly maintained.	Establish and review software development policies and practices based on security requirements.	CYT-00000709156
Some roles and responsibilities related to software development are not defined.	Define roles and responsibilities to ensure that every aspect of software development is managed and controlled.	CYT-00000938163
There is no process for identifying software vulnerabilities.	Regularly search for and identify software vulnerabilities.	CYT-00000266846
Compiler or build tools are not configured to improve executable security.	Configure your compiler and build tools to improve executable security.	CYT-00000565919
There is no requirement to use an existing secure software rather than duplicating functionality.	When feasible, use an existing well-secured software rather than duplicating functionality.	CYT-00000770717
Software design is not reviewed with reference to security requirements and identified risks.	Review software design for compliance with security requirements and for identified risks.	CYT-00000818205
Software default settings are not configured to provide maximum security.	Configure software default settings to provide maximum security.	CYT-00000076800
Software security risks are not identified and therefore cannot be mitigated at the design stage.	Identify your software security risks and mitigate at the design stage.	CYT-00000144634

Appendix B

Open tasks by domain - Software Development

	ISSUE	RECOMMENDATION	ID
●	Live data is not carefully managed throughout the software development lifecycle.	Carefully manage live and test data throughout the software development lifecycle.	CYT-00000958311
●	Not all development endpoints are protected against internal and external threats.	Ensure that all development endpoints are protected from internal and external threats.	CYT-00000572954
●	There is no process for identifying and communicating software component security requirements to third-party providers.	Identify and communicate software component security requirements to third-party providers.	CYT-00000983608
●	The company may experience increased security incidents, intellectual property theft, or reputational damage due to an insecure outsourcing vendor.	Assess and select outsourcing vendors based on their security capabilities, track record, and compliance with relevant industry standards.	CYT-54502886618
●	Software development QA plan does not include security testing.	Include security testing in the software development QA plan.	CYT-00000822486
●	Vetted security modules and services are not being used.	When possible, use vetted security modules and services, instead of developing new ones.	CYT-00000543751
●	Changes to systems and platforms within the development lifecycle are not controlled.	Enforce control procedures for changes to systems and platforms within the development lifecycle.	CYT-00000106430

Appendix B

Open tasks by domain - Threat Intelligence

	ISSUE	RECOMMENDATION	ID
🟡	The organization may fail to detect or respond to threats in a timely manner, resulting in increased security incidents and damage.	Assign roles and responsibilities for threat intelligence operations.	CYT-17157679730
🟡	The organization may experience increased security incidents due to a lack of actionable threat information.	Collect threat intelligence from multiple sources, both internal and external.	CYT-85569152424
🟡	Failing to maintain threat intelligence in a read-only repository may lead to the unintentional modification of indicators, potentially resulting in inaccurate threat data when referenced.	Store and maintain a read-only, central repository of cyber threat intelligence.	CYT-13307166974
🟡	Failing to establish and maintain an efficient SOC or equivalent may result in delayed or inadequate responses to security incidents, increasing the company's exposure to cyber risks.	Establish and maintain a Security Operations Center (SOC) or equivalent, for centralized and coordinated security processes and technology.	CYT-94394584660
🟢	The organization may become more vulnerable to security incidents due to an outdated understanding of the threat landscape and ineffective threat intelligence practices.	Regularly review and update threat intelligence processes, tools, and techniques.	CYT-64930444107
🟢	Not establishing information-sharing agreements may hinder the company's ability to collaborate with other organizations and share threat information, reducing collective cybersecurity efforts.	Use information-sharing agreements to facilitate sharing threat information with other financial sector organizations or third-parties.	CYT-44412597262
🟢	Failing to proactively share threat information with industry peers, law enforcement, regulators and information-sharing forums may result in a lack of collective awareness and cooperation in addressing cyber threats.	Share threat information proactively with the industry, law enforcement, regulators, and information-sharing forums.	CYT-96028906492
🟢	Not communicating and collaborating with the public sector regarding cyber threats may limit the company's access to government resources and support during cybersecurity incidents.	Communicate and collaborate with the public sector regarding cyber threats.	CYT-89570424490

Appendix B

Open tasks by domain - Vulnerability Management

	ISSUE	RECOMMENDATION	ID
●	Failing to test and apply patches for high-risk vulnerabilities promptly may expose the company's systems to exploitation by cyber adversaries, leading to security breaches and data compromise.	Ensure that patches are tested and applied upon release for high-risk vulnerabilities.	CYT-04263220318
●	No vulnerability management plan in place.	Establish and use a vulnerability management policy and plan.	CYT-00000933946
●	Undiscovered and unknown security control vulnerabilities and miss configuration.	Conduct penetration testing for company security systems.	CYT-00000823036
●	Not conducting thorough security investigations and forensic analysis of incidents may result in inadequate understanding of security breaches and their root causes.	Assign qualified staff or third-parties to perform security investigations, forensic analysis, and undertake remediation.	CYT-89792929071
●	Failing to adhere to generally accepted forensic procedures may compromise the integrity of evidence, affecting the company's ability to support legal actions against cyber adversaries.	Use accepted and appropriate forensic procedures, including chain of custody, to gather and present evidence to support potential legal action.	CYT-20391475226
●	New software vulnerabilities and security misconfigurations, which are inherent in any network or system, remain hidden and unmitigated.	Perform internal system scans.	CYT-00000462312
●	There is no penetration testing program.	Establish and maintain a penetration testing program.	CYT-00000604116
●	The absence of thorough reviews of penetration testing activities may result in ineffective testing and missed vulnerabilities.	Review the penetration testing scope and results to help determine the need for rotating companies based on the quality of work.	CYT-64345490643

Appendix B

Open tasks by domain - Website and Web Application

	ISSUE	RECOMMENDATION	ID
🟠	No measures are in place to mitigate a DDoS attack on your web servers.	Protect web servers from traffic overloads caused by Denial-of-Service Attacks (DDoS).	CYT-00000153592
🟠	No protection mechanism to negate attacks targeting web applications.	Apply a web application firewall (WAF) to negate various attacks targeting web applications.	CYT-00000845412
🟠	There is no web application penetration testing program for identifying threats.	Conduct penetration testing on all company websites and web applications.	CYT-00000228974
🟡	A lack of proactive monitoring to detect and respond to anomalous behavior in real time may result in missed security incidents and increased risk.	Monitor online customer transactions for anomalous behavior.	CYT-24481639948
🟡	Periodic vulnerability scanning is not performed.	Routinely scan company web servers for vulnerabilities and missing software updates.	CYT-00000998623
🟢	Your company's website uses cookies without appropriate safeguards. Cookies can be observed by unauthorized parties as they are transmitted in clear text.	Transfer cookies only in an encrypted manner.	CYT-00000487386