

Stratton Oakmont Cybersecurity Analysis Report

February 8, 2023

Introduction

//

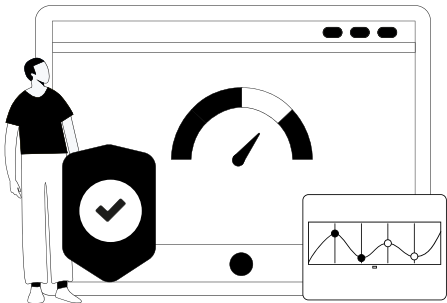
“The key to success is a well-constructed cybersecurity strategy with clear priorities. Spending must be balanced between people and technology with careful consideration for which risks should be addressed in which order. Decision-makers must be mindful of how their choices map against the NIST Cybersecurity framework to deliver a rounded set of defenses.” WSJ Cybersecurity

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 10027, the Center for Internet Security (CIS) controls, and SOC 2.

Posture score

3.2

Minor protection measures have been taken. The organization's risk level is high.



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.



Below average

3.1

Website Defacement

An unauthorized and malicious modification of web page content.



Below average

3.1

Ransomware

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



Below average

3.3

Fraud

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



Below average

3.1

Cybersecurity readiness level

31

Total Policies

0

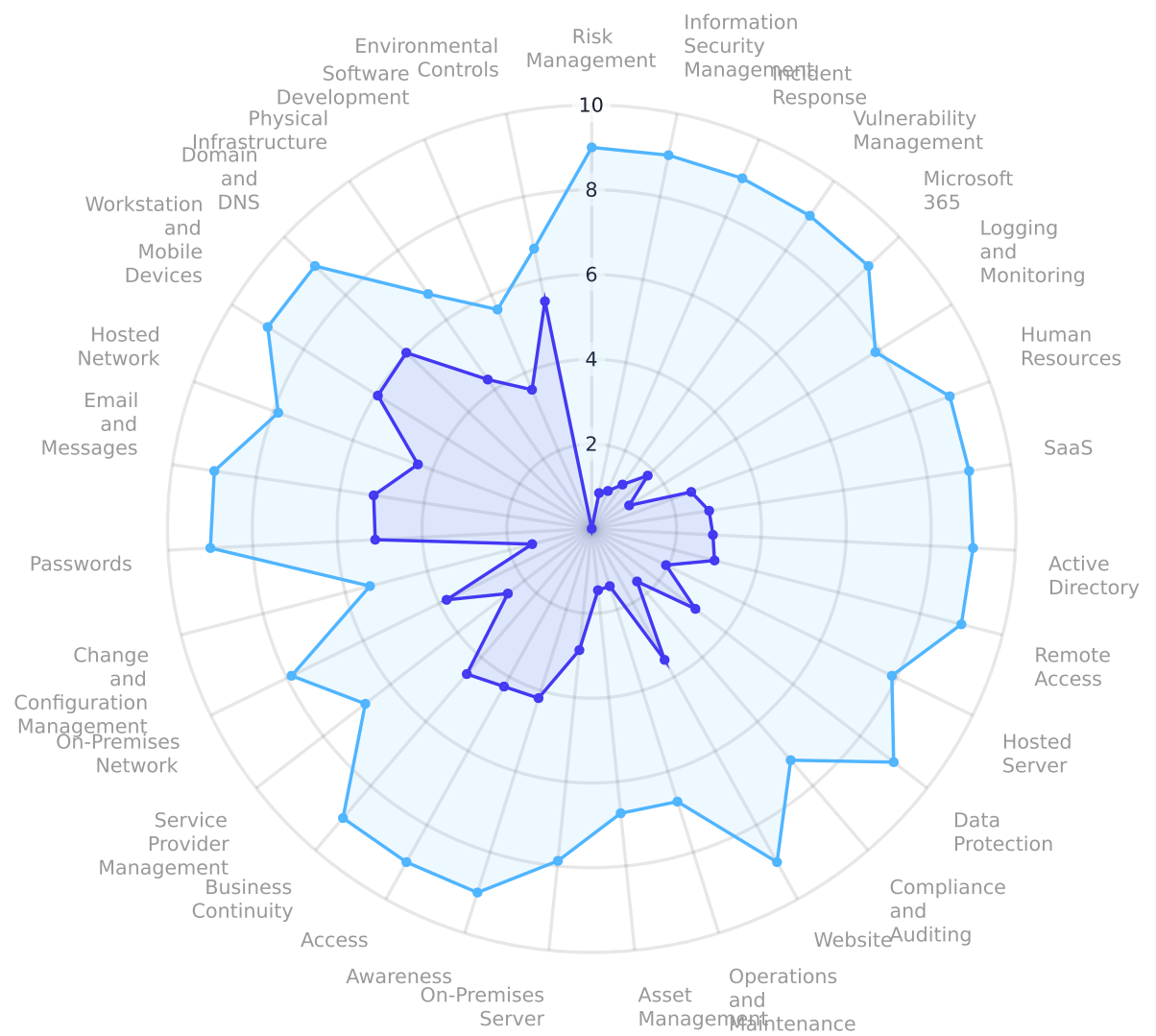
Meet target score

31

Under target score

A mapping process of your organization shows that 31 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

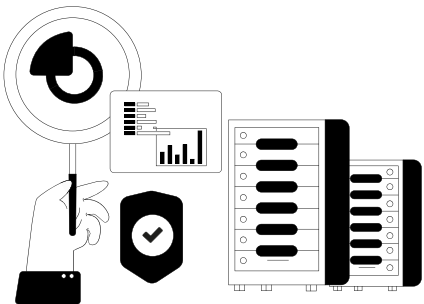
DOMAIN	SCORE
Access	4.3
Active Directory	2.9
Asset Management	1.5
Awareness	4.2
Business Continuity	4.5
Change and Configuration Management	1.5
Compliance and Auditing	1.6
Data Protection	3.1
Domain and DNS	6
Email and Messages	5.2
Environmental Controls	5.5
Hosted Network	4.4
Hosted Server	1.9
Human Resources	2.5
Incident Response	1
Information Security Management	0.9
Logging and Monitoring	1
Microsoft 365	1.8
On-Premises Network	3.8
On-Premises Server	2.9
Operations and Maintenance	1.4
Passwords	5.1
Physical Infrastructure	4.3
Remote Access	3
Risk Management	0
SaaS	2.8
Service Provider Management	2.5

Company readiness by security domain

DOMAIN	SCORE
Software Development	3.6
Vulnerability Management	1.3
Website	3.5
Workstation and Mobile Devices	5.9

Scan findings

- ✓ External scan
- ✓ Internal network scan
- ✓ Microsoft Secure Score



Scanning networks and applications exposes hidden infrastructure vulnerabilities. Addressing these vulnerabilities will reduce the chances of your organization being the subject of a cyberattack.

66

Total findings

15

Critical

19

High

22

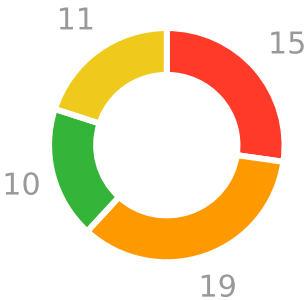
Medium

10

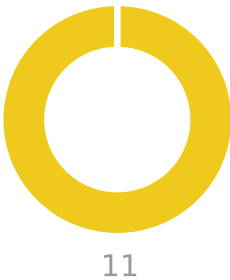
Low

External scan

Internal network scan



Microsoft Secure Score



Scan findings

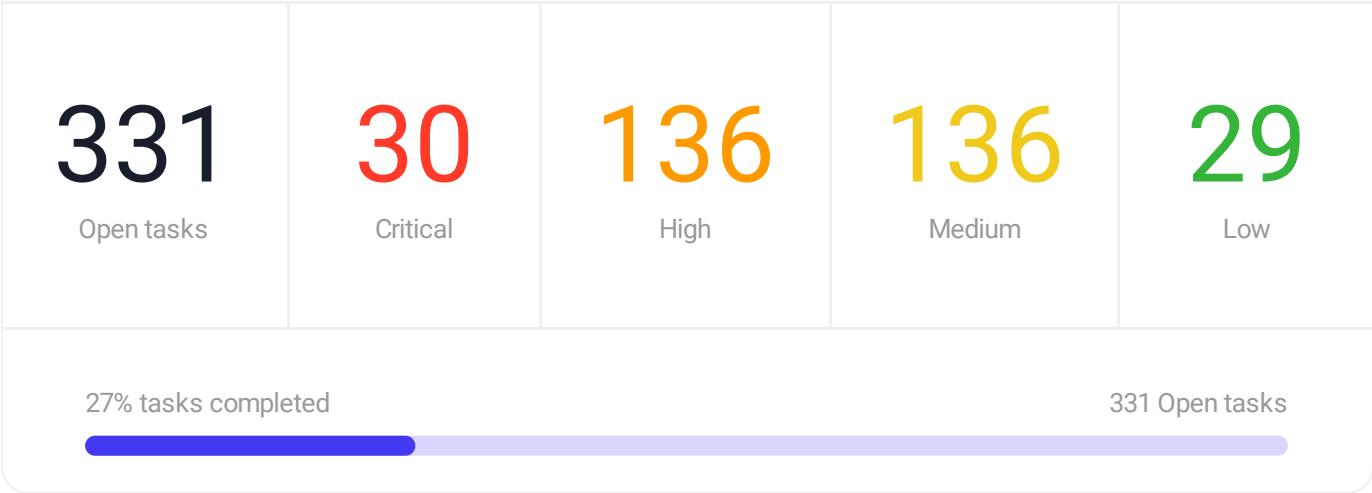
Sample findings

Each finding addresses a specific asset and details the specifics of its detected vulnerabilities. Using the Cynomi platform, you can review online or download the full list of findings.

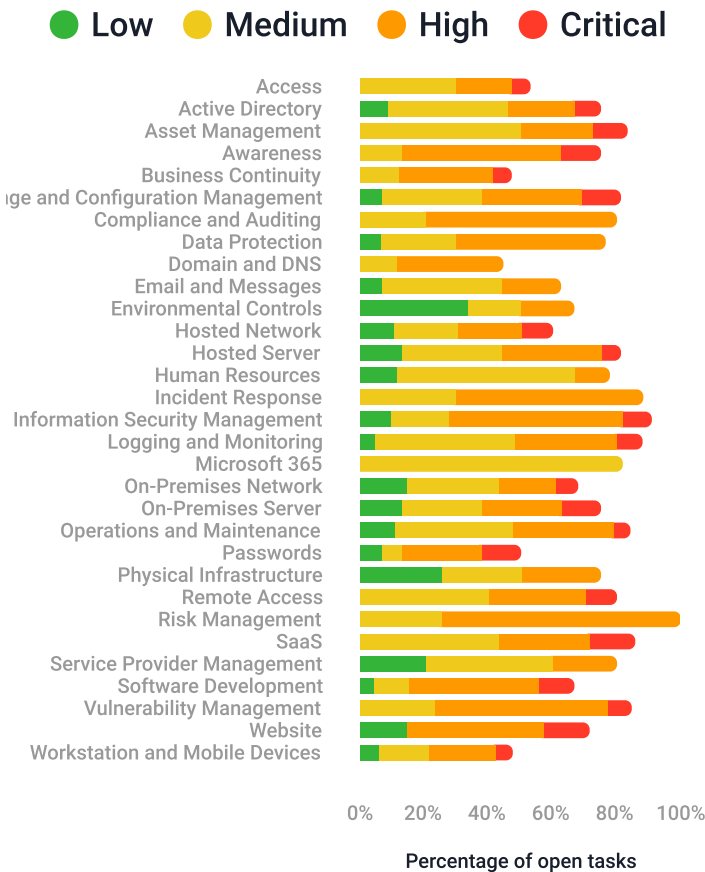
SOURCE	SEVERITY	FINDING	ASSET
Internal network scan	Critical	On-premises workstation antivirus is not detected	10.10.10.69
Internal network scan	Critical	Not all domain controllers are set with an updated and supported operating system	10.10.10.5
Internal network scan	Critical	Password length is not set to be at least 12 characters	10.10.10.5
Internal network scan	Critical	On-premises workstation password in not required for computer users	10.10.10.58
Internal network scan	High	On-premises workstation is missing security patches	10.10.10.55

Risk mitigation plan

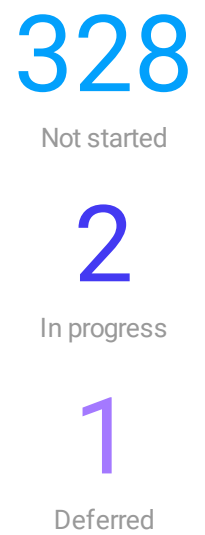
Completing critical and high severity tasks will impact organization cybersecurity the most, and increase posture score.



Open tasks













Task status



Appendix A

Top 10 open tasks

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

ISSUE	RECOMMENDATION	ID
 New software vulnerabilities and security misconfigurations, which are inherent in any network or system, remain hidden and unmitigated.	Conduct external vulnerability assessments.	CYT-107803
 Your password policy does not require a minimum password length.	Enforce a minimum password length for all passwords.	CYT-999533
 No password management tools is used for secure, centralized management of passwords.	Deploy a password management tool.	CYT-233135
 There is no remote access policy.	Create a remote access policy and have company management approve it.	CYT-833140
 There is no strong and complex password enforcement.	Configure password policy to be secured.	CYT-384502
 Not all domain controllers run a supported operating system.	Set all domain controllers to run a supported and updated Operating System (OS).	CYT-095911
 There is no cybersecurity program.	Ensure that company management supports a cybersecurity program.	CYT-048630
 Applications running on the server are not regularly updated and patched.	Regularly update all applications running on company servers and verify patches.	CYT-371537
 A strong password policy is missing or not enforced.	Enforce a strong password policy for all connections to company servers, including connection through consoles, remote connections, or local logins.	CYT-979306
 A strong password policy is missing or not enforced.	Enforce a strong password policy for all connections to company servers, including connection through consoles, remote connections, or local logins.	CYT-498191

Appendix B

Open tasks by domain - Access

ISSUE	RECOMMENDATION	ID
 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-617212
 Inactive user accounts are not automatically flagged and removed.	Remove inactive user accounts, preferably automatically.	CYT-952139
 Access to information and application functions is not restricted in accordance with the access control policy.	Restrict access to information and application functions in accordance with the access-control policy.	CYT-127115
 Some service accounts might have unnecessary access privileges.	Establish a service account inventory containing service owner, review dates, and function.	CYT-174368
 Unauthorized or excessive access to company data is not detected.	Log and monitor queries of company sensitive data.	CYT-933655
 Idle remote sessions are not terminated.	Terminate idle remote sessions after a defined period of inactivity.	CYT-385532
 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-584712
 There is no defined process for removing unauthorized access rights and privileges to assets and systems.	Provide Single Sign-On capability to access company systems containing sensitive data.	CYT-688505
 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-883307





Appendix B

Open tasks by domain - Active Directory

ISSUE	RECOMMENDATION	ID
● There is no strong and complex password enforcement.	Configure password policy to be secured.	CYT-384502
● Not all domain controllers run a supported operating system.	Set all domain controllers to run a supported and updated Operating System (OS).	CYT-095911
● Different OS versions are found on the Domain Controllers servers	Set up all domain controllers with the same operating system configurations.	CYT-802555
● There are obsolete accounts that need to be deleted.	Delete inactive user accounts after a defined time period.	CYT-643598
● Unverified domains might be trusted.	Carefully check external domains for compliance with company Active Directory policy before configuring as trusted.	CYT-678223
● There are obsolete accounts that need to be deleted.	Delete disabled user accounts after a defined time period.	CYT-668032
● Some domain controller permissions and privileges are not restricted.	Prohibit default domain controller policy insecure configurations.	CYT-005337
● GPOs use weak password exchange protocol.	Prevent GPOs from using Network LAN Manager (NTLM)	CYT-047309
● GPO authentication is not secured.	Define GPOs to use Kerberos protocol with strong encryption algorithms.	CYT-112468
● Domain controller traffic is not secured.	Set Kerberos protocol to use strong encryption algorithms for all domain controllers.	CYT-234902
● Local administrator accounts are not secured.	Rename all local administrator account default names.	CYT-283637
● Admin accounts are not secured.	Define GPOs to restrict admins from using default login access to any asset.	CYT-949860
● Unauthorized users are granted the access rights and permissions of authorized users.	Deny anonymous user access to system information.	CYT-492591
● Non-administrative accounts might be able to set passwords via Group Policy.	Do not allow any Extensible Markup Language (XML) file with cpassword in System Volume (Sysvol).	CYT-841136

Appendix B

Open tasks by domain - Active Directory

ISSUE	RECOMMENDATION	ID
 There is no software update verification policy for DNS zones.	Use only secure updates from certified known sources in DNS zones.	CYT-226266
 Some domain controllers support old system versions.	Disable domain controller backward compatibility if not necessary.	CYT-538658
 Unauthorized users might have administrator permissions and privileges.	Clear all default administrative groups with access privileges and leave empty.	CYT-232519
 Some users with access privileges to sensitive assets might not be protected.	Include only sensitive users in the Protected Users security group.	CYT-219190



Appendix B

Open tasks by domain - Asset Management

ISSUE	RECOMMENDATION	ID
● 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-395293
● The company cannot validate whether or not software asset version is supported.	Only use vendor supported software versions.	CYT-575581
● The organization does not know what systems need to be protected.	Identify all assets and establish an asset inventory.	CYT-304608
● 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-183617
● Sensitive printed information is not shredded.	Shred hardcopy materials so that sensitive data cannot be reconstructed.	CYT-084294
● 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-488800
● 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-989255
● Asset owners are not identified.	Identify and document the owner of each asset.	CYT-824215
● Sensitive data is not removed from end-of-life or recycled media.	Require from assets' custodians to destroy media that cannot be sanitized.	CYT-939131
● Unauthorized hardware and software assets are not removed.	Remove any unauthorized hardware and software assets.	CYT-375233
● The organization cannot adequately plan for business continuity requirements.	Document the relationships between assets and business services.	CYT-592219
● 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-457288
● Asset inventories are not kept up to date.	Update asset inventory when a device or software is installed, removed, updated, or changed.	CYT-617887


Appendix B

Open tasks by domain - Asset Management

ISSUE	RECOMMENDATION	ID
 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-430657
 The organization has no process to automatically identify assets.	Ensure that assets are automatically identified and that, where possible, asset inventory is automatically updated.	CYT-285362

Appendix B

Open tasks by domain - Awareness

ISSUE	RECOMMENDATION	ID
 There is no security awareness program for employees.	Conduct cybersecurity awareness training for all employees.	CYT-720276
 There is no security awareness program for software developers.	Conduct role-based cybersecurity awareness and skills training for company software developers.	CYT-176684
 There is no security awareness program for IT administrators and DevOps staff.	Conduct cybersecurity awareness training for users with administrative access to company assets.	CYT-801509
 There is no process for ensuring employee commitment to company cybersecurity policy.	Ensure all employees are aware of and have signed company cybersecurity policy.	CYT-549414
 There is no improvement protocol for company security awareness programs.	Collect and store training data.	CYT-906502
 There is no employee security awareness program for detecting and reporting cyber incidents.	Conduct cybersecurity awareness training to employees about detecting and reporting potential signs of cyber incidents.	CYT-585743

Appendix B

Open tasks by domain - Business Continuity

ISSUE	RECOMMENDATION	ID
 Business-critical processes and related digital assets are not mapped.	Map and document critical processes and related assets.	CYT-926807
 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-879894
 Critical business data is not mapped or backed up.	Following mapping of critical processes and related assets, map and back up critical data.	CYT-162393
 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-898474
 Network storage is not backed up.	Back up critical data from company network storage.	CYT-113341
 Company server data and configurations are not backed up.	Back up the server data and configuration.	CYT-323818
 There is no process to ensure RTO and RPO targets can be met.	Verify that RTO and RPO targets can reliably be met.	CYT-192177
 There is no employee contingency plan training for the case of a disaster and the need for quick recovery.	Train employees for disaster recovery and emergency response.	CYT-556018


Appendix B

Open tasks by domain - Change and Configuration Management

ISSUE	RECOMMENDATION	ID
 Systems are not hardened.	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs.	CYT-426565
 Basic technical security controls are not implemented.	Each system should have technical controls such as antivirus, monitoring, and logging as part of the baseline standard or template.	CYT-312995
 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-895743
 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-010966
 Configuration changes are not properly approved.	Deviations from the baseline configuration must be authorized following the change management processes before use.	CYT-472023
 Change is not tracked and/or appropriately documented through its life cycle.	All changes to configurations should be logged.	CYT-995938
 Unauthorized software can run on systems.	Only execution of authorized software, scripts and libraries should be allowed.	CYT-839061
 Configurations are not stored securely.	Master configurations or images should be stored securely.	CYT-418965
 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 prior to change implementation.	CYT-933706
 Change is not controlled in the environment.	The organization tests, validates, and documents change to systems before implementing the change.	CYT-366116
 Unauthorized changes are not detected.	Configuration monitoring should alert when unauthorized changes occur.	CYT-987655
 Authorized software is not defined.	A list of authorized software and version that is required for each platform should be documented.	CYT-772328

Appendix B

Open tasks by domain - Change and Configuration Management

ISSUE	RECOMMENDATION	ID
 Configurations are not backed up.	At least the last three (3) previous versions should be retained.	CYT-496034

Appendix B

Open tasks by domain - Compliance and Auditing

ISSUE	RECOMMENDATION	ID
● Not all company compliance requirements have been identified.	Identify all regulatory requirements and standards which apply to the company.	CYT-016508
● Not all regulatory requirements related to intellectual property rights have been identified.	Identify and comply with all legislative, regulatory and contractual requirements related to intellectual property rights.	CYT-036416
● There is no compliance and governance plan.	Establish a compliance and governance plan.	CYT-002079
● There is no external audit of cybersecurity policies and of protection processes.	Conduct periodic external audits of the company's cyber security policies and protection processes.	CYT-733894

Appendix B

Open tasks by domain - Data Protection

ISSUE	RECOMMENDATION	ID
● There is no limitation or managements of access to shared resources.	Restrict access to sensitive data stored in shared resources.	CYT-036602
● Outgoing and incoming transfers of sensitive information are not monitored or restricted.	Protect sensitive information transfers by restricting outgoing and incoming data.	CYT-603731
● There is no process for disposing of data once it is no longer needed.	Enforce retention and deletion of regulated data according to law or business agreements.	CYT-612835
● 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 the compliance requirements.	CYT-604160
●	Protect sensitive data flows by restricting outgoing and incoming data.	CYT-167544
● No use of data leak prevention tools.	Apply data leak prevention and detection tools.	CYT-826479
● Data saved on removable media is not encrypted.	Encrypt data that is saved on removable media.	CYT-061221
● There are no contractual restrictions on the use third-parties have of company data.	Create confidentiality or nondisclosure agreements with third-party contractors.	CYT-356369
● Sensitive data transactions are not logged and monitored.	Record sensitive data transactions; then produce and review event logging.	CYT-762613
● Sensitive data is not stored in a secure and seprate network segment.	Store and process sensitive data in a secure and separate network segment.	CYT-075850
● Logs containing sensitive data are not encrypted or do not have access limitations.	Protect logs containing sensitive data with access limitation and encryption.	CYT-527658
●	Develop and implement a cryptography controls policy.	CYT-056824
● There is no limitation on folder or file-sharing from employee workstations.	Prevent file-sharing of employee workstation folders.	CYT-422881











Appendix B

Open tasks by domain - Domain and DNS

ISSUE	RECOMMENDATION	ID
● Access to domain name registration and modification access is not enforced with multi-factor authentication.	Enable access to domain registration only through multi-factor Authentication.	CYT-057467
● 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-867450
● Your company does not log DNS server events.	Enable DNS query audit logging for detection and investigation of possible cyber-attacks and the targeting of company DNS server.	CYT-873292
● Company domains are not secured with DNSSEC.	Enable Domain Name System Security Extension (DNSSEC) for all registered domains.	CYT-374530





Appendix B

Open tasks by domain - Email and Messages

ISSUE	RECOMMENDATION	ID
 Sensitive data can be sent from your company's email to external emails without detection or prevention.	Apply Data Leak Protection (DLP) tools.	CYT-182882
 Electronic messaging applications are not secured.	Secure electronic messaging applications used by the company.	CYT-419773
 There is no advanced email protection tool implemented.	Implement an advanced email protection tool to handle advanced emails attacks.	CYT-578636
 Information transferred by electronic messaging is not being mapped and documented.	Ensure that information transferred by electronic messaging is mapped and documented.	CYT-008367
 No email awareness program is in place to raise awareness of malicious emails.	Conduct email awareness trainings, involving all company email account users.	CYT-285877
 Emails are transferred in cleartext between different email domains.	Apply Transport Layer Security (TLS) encryption.	CYT-984626
 There is no policy governing usage of company email accounts.	Issue an Email Usage Policy to be implemented by all company email account users.	CYT-428723
 A mechanism to prevent incoming email spoofing is missing or has not been configured.	Apply anti-spoofing tools.	CYT-756178
 Email content is transferred as cleartext.	Enforce encryption of emails containing sensitive materials.	CYT-312963
 Email forwarding rules are enabled.	Create and enforce email forwarding standards.	CYT-185743













Appendix B

Open tasks by domain - Environmental Controls

ISSUE	RECOMMENDATION	ID
 There is no fire suppression system installed.	Verify that a fire suppression system is installed and maintained.	CYT-574229
 There is no master shutoff or insulating valve installed.	Protect company assets from water leakage by installing an accessible master shutoff or insulating valve.	CYT-904091
 There is no temperature and humidity monitoring system.	Maintain acceptable temperature and humidity levels where company physical assets are stored.	CYT-934267
 Electrical Equipment and cables are not physically secured.	Protect electrical equipment and cables.	CYT-179538














Appendix B

Open tasks by domain - Hosted Network

ISSUE	RECOMMENDATION	ID
 Company network computers can directly access the internet.	Enforce the channeling of internet access from company networks through a web security solution.	CYT-105315
 Users may connect to the company's network using only a password.	Require Multi-Factor Authentication for remote access to hosted company networks.	CYT-642532
 There are no network traffic anomaly detection and prevention security controls.	Deploy network traffic anomaly detection and prevention security controls.	CYT-609986
 Firewalls have not been properly configured (hardened).	Harden company firewall configurations.	CYT-153686
 Firewall alerts are not configured.	Configure all company firewalls to automatically alert of high severity risks.	CYT-477889
 Network infrastructure is not managed securely.	Manage network infrastructure securely.	CYT-707030
 There is no restriction on connecting any device (i.e unknown computers, mobile devices, memory sticks etc.) directly to your network.	There is no restriction on connecting any device (i.e. unknown computers, mobile devices, memory sticks etc.) directly to your network.	CYT-060150
 Switches are not configured securely.	Harden switches configuration according to security best practices.	CYT-411407
 Firewall logs are not continuously monitored.	Regularly monitor all company firewall logs.	CYT-766626
 No measures are in place to mitigate a DDoS attack.	Protect network against Distributed Denial-of-Service (DDoS) attacks.	CYT-706879
 There are no dedicated computing resources for administrative management tasks.	Perform network administrative management tasks only by using dedicated computing resources.	CYT-738339
 Firewall logs are not stored in external storage.	Store firewall logs in a system that is external to the system running the firewalls.	CYT-055226








Appendix B

Open tasks by domain - Hosted Server

ISSUE	RECOMMENDATION	ID
 A strong password policy is missing or not enforced.	Enforce a strong password policy for all connections to company servers, including connection through consoles, remote connections, or local logins.	CYT-498191
 Outdated servers or vulnerable operating systems are not separated from the rest of the network.	Verify that all unsupported servers are installed on a different network segment.	CYT-594537
 Unused and unnecessary services/ports are open.	Uninstall or disable all unused or unnecessary services from company servers.	CYT-017744
 Users are not locked out following several unsuccessful login attempts.	Following multiple unsuccessful attempts to sign in, enforce user lockout.	CYT-712527
 The default-account credentials of one or more servers and applications were not modified.	Modify server default-account credentials.	CYT-066449
 There is no approved software list for company servers.	Install only approved software on servers.	CYT-382705
 There is no removable media anti-malware scan enforced.	For all removable media connected to company servers, configure anti-malware scan.	CYT-644151
 System or security event logging is not performed.	Log and monitor attempts to access unsupported servers.	CYT-919226
 Applications running on the server are not regularly updated and patched.	Regularly update all applications running on company servers and verify patches.	CYT-901447
 Server communication is not encrypted or secured.	Verify all communication flow from and to company servers is protected, encrypted, and monitored.	CYT-053661
 Advanced endpoint protection is not applied for company servers.	Apply an advanced endpoint protection to safeguard endpoints against advanced attacks.	CYT-689740
 Autorun and autoplay are not automatically disabled when connecting removable media.	For all removable media connected to company servers, disable autorun and autoplay.	CYT-070578
 Not all company servers have a host-based firewall enabled.	On all company hosted servers, implement a host-based firewall.	CYT-374914

Appendix B

Open tasks by domain - Human Resources

ISSUE	RECOMMENDATION	ID
 There is no process for revoking an employee's access credentials when their employment is terminated.	Ensure that upon termination of individual employment, all access credentials and authenticators are revoked.	CYT-688701
 Company data is not protected against misuse by employees or third-party contractors.	Ensure that HR incorporate 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-610545
 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-513886
 Company data is not protected against misuse by former employees or third-party contractors.	Ensure that all post-employment requirements for protecting sensitive company information are legally binding and incorporated into employee and third-party contracts.	CYT-067664
 Employment contract does not support 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-112516
 There are no rules and procedures of 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-669280
 Employees and third-party contractors might not be aware of sanctions for violating company cyber policy.	Ensure that the company has an approved sanction process for cyber policy breaches.	CYT-687979

Appendix B

Open tasks by domain - Incident Response

ISSUE	RECOMMENDATION	ID
● No third party Incident Response (IR) support.	Engage a third-party incident response vendor for fast response and post-incidents reviews	CYT-373508
● 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-791067
● There is no plan on place to handle a cyber incident.	Prepare an incident response plan outlining potential actions to the most likely and highest impact cyberattacks.	CYT-338667
● Incidents are not thoroughly analyzed as they occur.	To ensure an effective response, thoroughly analyze an incident as it occurs.	CYT-093213
● Response procedures might not be executed according to incident response plan.	Execute response procedures according to the incident response plan.	CYT-789550
● No logs of network and system events are collected.	Define and apply controls for logging and storage of the identification, collection, acquisition, and preservation of incident information, which can serve as evidence in criminal or civil proceedings.	CYT-004652
● No measures are taken towards preventing expansions of incidents.	Prevent an expansion of an incident and contain it.	CYT-606697
● Individuals involved in 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-097791
● Roles and responsibilities are not clearly defined in case of an incident.	Designate key roles and responsibilities to manage and handle cyberattacks.	CYT-410441
● 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-487586
● There is no process for communicating cybersecurity incidents to stakeholders, affected third-parties, or relevant employees.	Report information security events both internally and externally; for instance, third-party vendors, law enforcement, cyber insurance providers, and relevant government agencies.	CYT-143196

Appendix B

Open tasks by domain - Incident Response

ISSUE	RECOMMENDATION	ID
● There is no procedure for improving the company's incident response plan by reviewing past incidents.	To improve the company's incident response plan and develop future incident responses, analyze and resolve cybersecurity incidents and gather insight into adversary tactics, techniques, and procedures by conducting post-incident reviews.	CYT-936557
● Incident Response (IR) tabletop exercises are not conducted.	To contribute to company incident response readiness and understanding, conduct incident response practice sessions.	CYT-581352
● There is no defined incident alert threshold that helps differentiating between events and incidents.	Establish a threshold for alerts when an incident is detected and classified.	CYT-024763
● There is no employee awareness covering cyber incidents and employee's role in them.	Ensure employees are aware of their respective roles in main incident scenarios.	CYT-776300

Appendix B

Open tasks by domain - Information Security Management

ISSUE	RECOMMENDATION	ID
● There is no cybersecurity program.	Ensure that company management supports a cybersecurity program.	CYT-048630
● The company does not have a full set of cybersecurity policies and guidelines.	Create cybersecurity policies consistent with company business goals, assessed risks, threats, and relevant regulatory requirements.	CYT-635874
● There is no operational or organizational structure of management stakeholders and board of directors.	Set an operational and organizational structure for management stakeholders and an independent board of directors.	CYT-385236
● The cybersecurity framework does not fully support business objectives and has no defined roles and responsibilities for company management.	Make sure that management aligns information security guidelines, roles and responsibilities, and threat landscape with the company's business objectives.	CYT-509230
● There is no cybersecurity program which is consistent with business objectives, assessed risks, and regulatory requirements.	Create a cybersecurity program consistent with company business objectives, assessed risks, and the regulatory landscape.	CYT-193093
● The company's business sector is not identified and a business model cannot be defined.	Define the company's business model and relevant guidelines in relation to its business sector.	CYT-546709
● There are no guidelines for an internal control system of management and board of directors.	Set guidelines for an internal control system of the different management levels and the board of directors.	CYT-559627
● There is no identification of internal and external issues affecting company cybersecurity policies.	Identify all internal and external issues affecting company cybersecurity policies.	CYT-820950
● 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-203001
● There is no understanding of what the needs are of information security stakeholders.	Understand who are the interested parties in company information security and what are their needs and expectations in terms of compliance obligations.	CYT-756954

Appendix B

Open tasks by domain - Logging and Monitoring

ISSUE	RECOMMENDATION	ID
● Audit logs are not being collected.	Collect audit logs.	CYT-895962
● The monitoring system does not operate an abnormal activity detection and alert mechanism.	To identify suspected cyber-incidents, apply automated detection mechanisms to all company monitoring platforms.	CYT-959963
● Monitoring of sensitive activities within sensitive and critical systems is difficult.	Verify that monitoring of sensitive activities within sensitive and critical system can be done without difficulty.	CYT-881228
● Actions of high-privilege users are not logged.	Define actions of high-privilege users as an event type.	CYT-543844
● Endpoint device security-related events are not logged.	Define endpoint device security-related event logs as an event type.	CYT-001346
● 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-301571
● There is no log-file breach identification alert system.	Implement a central log file monitoring and alert system.	CYT-395545
● There is no audit-log management process.	Establish and maintain an audit-log management process.	CYT-094210
● Active Directory events are not logged.	Define Active Directory events as an event type.	CYT-500806
● Indicators of Compromise (IoCs) are not logged.	Define Indicators of Compromised (IoC) data as an event type.	CYT-987925
● It is not possible to retrieve only one single log out of log storage.	Configure log storage to allow secure log retrieval.	CYT-048095
● 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-017161
● It is not possible to delete only one single log from log storage.	Configure log storage to allow secure log deletion.	CYT-763838

Appendix B

Open tasks by domain - Logging and Monitoring

ISSUE	RECOMMENDATION	ID
● There is no logging failure identification alert mechanism.	Create an alert mechanism for the case of logging failure.	CYT-673314
● 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-322620
● 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-798631
● Network traffic is not logged.	Define network traffic as an event type.	CYT-831279
● 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-869040
● There is no sensitive-role control record analysis.	Periodically review and analyze control records of users with sensitive roles or any account with access privileges.	CYT-405010
● DNS queries are not logged.	Define DNS queries as an event type.	CYT-231378
● Third-party and service provider actions within company systems are not logged.	Define access and actions of third-party service providers to company systems as an event type.	CYT-522696
● Endpoint URL browsing is not logged.	Define endpoint URL browsing as an event type.	CYT-895397

Appendix B

Open tasks by domain - Microsoft 365

ISSUE	RECOMMENDATION	ID
● The policy for inbound phishing messages is not well defined.	For read or unread messages that are identified as phishing after delivery, assigned Anti-phishing inbound policy with both 'Enable zero-hour auto purge (ZAP).	CYT-225146
● Users can access your digital assets or services with only a username and password. Accounts can be easily breach.	Ensure all users can complete multifactor authentication for secure access.	CYT-297649
● Customer lockbox feature is turned off.	Turn on customer lockbox feature.	CYT-689126
● Safe Links policies for email messages is missing	Create Safe Links policies for email messages.	CYT-067205
● Suspicious login are not handle properly and protected with MFA.	Turn on sign-in risk policy.	CYT-037104
● Safe attachment is turned off	Turn on Safe Attachments in Block mode.	CYT-445377
● Office 365 or Azure Active Directory admin can't identify user account that has been compromised.	Turn on User and Sign-in Risk policy.	CYT-410870
● Weaker protocols and cipher such as TLS 1.0/1.1 and 3DES dependencies are used.	Remove TLS 1.0/1.1 and 3DES dependencies.	CYT-837198
● Users can grant access permissions for 3rd party apps that can be a malicious application.	Do not allow users to grant consent to unmanaged applications.	CYT-145731
● The option for 'Enable zero-hour auto purge for malware' is not enabled for all users. Users can release quarantined messages that contain malware.	Create Zero-hour Auto Purge policies for malware.	CYT-271404
● The policy for inbound spam messages is not well defined.	Create Zero-hour Auto Purge policies for spam messages.	CYT-526526
● Legacy authentication is enabled and does not support multi-factor authentication (MFA).	Enable policy to block legacy authentication.	CYT-195903
● Microsoft Defender is not set to scan endpoints.	Turn on Safe Documents for office clients.	CYT-620125
● Periodic password resets are enforced.	Do not configure passwords to expire.	CYT-516566
● Users can set easily guessable passwords for their accounts when using the helpdesk service for password reset.	Enable self-service password reset.	CYT-409954

Appendix B

Open tasks by domain - Microsoft 365

ISSUE	RECOMMENDATION	ID
<ul style="list-style-type: none">● Only one global administrator for the organization. In case this account is breached or corrupted , the administrator cannot fulfill the needs or obligations of your organization.	Designate more than one global admin	CYT-649177
<ul style="list-style-type: none">● Users can edit Anti-spam lists and add allowed domains.	Sender domains allowed for Anti-spam policies.	CYT-749546
<ul style="list-style-type: none">● Sharing information could help attacker to better plan attacks on the organization and to lead to data leak.	Exchange Online calendar sharing.	CYT-655870

Appendix B

Open tasks by domain - On-Premises Network

ISSUE	RECOMMENDATION	ID
 Company network computers can directly access the internet.	Enforce the channeling of internet access from company networks through a web security solution.	CYT-203509
 Users can connect to the company's network with only a password.	Require Two-Factor Authentication for remote access to on-premises company networks.	CYT-319996
 There are no network traffic anomaly detection and prevention security controls.	Deploy network traffic anomaly detection and prevention security controls.	CYT-101697
 Unapproved ports are potentially open.	Block all incoming communication from ports that are either unapproved or unrequired by closing them; all approved or required ports should be left open.	CYT-317549
 Company employees and guests share a single network for Wi-Fi access.	Provide Wi-Fi access for guests through a segmented guest network.	CYT-084608
 Firewalls have not been properly configured (hardened).	Harden company firewall configurations.	CYT-850508
 Network infrastructure is not managed securely.	Manage network infrastructure securely.	CYT-442955
 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-197910
 No measures are in place to mitigate a DDoS attack.	Protect network against Distributed Denial-of-Service (DDoS) attacks.	CYT-290733
 Switches are not configured securely.	Harden switches configuration according to security best practices.	CYT-989947
 The company's Wi-Fi router uses its default login and password.	Change Wi-Fi routers default login details and password and create new ones.	CYT-214199
 Your company's Wi-Fi routers' firmware is not regularly updated.	Regularly update Wi-Fi firmware.	CYT-635957
 Your company's Wi-Fi routers' firewall is not activated.	Set Wi-Fi routers internal firewall to be activated.	CYT-496486
 Firewall alerts are not configured.	Configure all company firewalls to automatically alert of high severity risks.	CYT-660263
 Firewall logs are not continuously monitored.	Regularly monitor all company firewall logs.	CYT-479472













Appendix B

Open tasks by domain - On-Premises Network

ISSUE	RECOMMENDATION	ID
● The company's Wi-Fi routers are not located at a secure location.	Secure physical and environmental location of Wi-Fi routers.	CYT-685794
● The company's Wi-Fi routers use their default network name (SSID).	Discard Wi-Fi networks default name and create a new one.	CYT-732581
● Your company's Wi-Fi routers allow WPS and DHCP services.	Disable company routers Dynamic Host Configuration Protocol (DHCP) and Wi-Fi Protected Setup (WPS) services.	CYT-964786
● Firewall logs are not stored in external storage.	Store firewall logs in a system that is external to the system running the firewalls.	CYT-397534

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-371537
 A strong password policy is missing or not enforced.	Enforce a strong password policy for all connections to company servers, including connection through consoles, remote connections, or local logins.	CYT-979306
 Outdated servers or vulnerable operating systems are not separated from the rest of the network.	Verify that all unsupported servers are installed on a different network segment.	CYT-046789
 There is no approved software list for company servers.	Install only approved software on servers.	CYT-366830
 Users are not locked out following several unsuccessful login accounts.	Following multiple unsuccessful attempts to sign in, enforce user lockout.	CYT-327236
 The default-account credentials of one or more servers and applications were not modified.	Modify server default-account credentials.	CYT-783251
 There is no removable media anti-malware scan enforced.	For all removable media connected to company servers, configure anti-malware scan.	CYT-179618
 Unused and unnecessary services or ports are open and ready for communication.	Uninstall or disable all unused or unnecessary services from company servers.	CYT-104481
 Server communication is not encrypted or secured.	Verify all communication flow from and to company servers is protected, encrypted, and monitored.	CYT-043215
 Advanced endpoint protection is not applied for company servers.	Apply an advanced endpoint protection to safeguard endpoints against advanced attacks.	CYT-425233
 Autorun and autoplay are not automatically disabled when connecting removable media.	For all removable media connected to company servers, disable autorun and autoplay.	CYT-815208
 Not all company servers have a host-based firewall enabled.	On all company on-premises servers, implement a host-based firewall.	CYT-487742





Appendix B

Open tasks by domain - Operations and Maintenance

ISSUE	RECOMMENDATION	ID
● Software installation is not restricted.	The installation of software on all operational systems shall be restricted.	CYT-572956
● Security operations are Ad-hoc.	The organization uses defined operational security controls to protect key information to ensure the correct and secure operations of data processing facilities.	CYT-088262
● Security is planned into projects.	Information security shall be addressed in project management, regardless of the type of project.	CYT-187562
● Equipment should be correctly maintained to ensure its continued availability and integrity.	Maintenance is scheduled and documented in accordance with manufacturer specifications.	CYT-651276
● New systems are not verified for functionality.	New systems and applications must be tested for functionality before being put into production.	CYT-448596
● Critical and remotely exploitable vulnerabilities are not patched.	All systems and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.	CYT-926000
● Protections are not designed for defense-in-depth.	Systems have layered protections.	CYT-293320
● The company does not manage infrastructure spending and availability requirements.	Resources are planned, deployed, and measured to provide the required systems performance for legal, statutory, and other compliance obligations.	CYT-441014
● Off-site maintenance is not controlled.	Maintenance activities are controlled whether being performed on-site or remotely.	CYT-132709
● Protections are not planned.	Processes are developed to implement security resource planning and the associated planning controls.	CYT-955563
● Protections are not throughout the asset's lifecycle.	Utilize separate environments for development and production.	CYT-391233
● Testing is performed in production environments.	Utilize separate environments for development and production.	CYT-778853









Appendix B

Open tasks by domain - Operations and Maintenance

ISSUE	RECOMMENDATION	ID
 There are no maintenance records.	Maintenance records are kept and include at least the date, the name of the individual performing the maintenance, a description of the work performed, and a list of assets or parts of assets replaced or removed.	CYT-503016
 Due diligence is not performed for acquisitions.	The enterprise IT architecture is used in all development and acquisitions.	CYT-939328
 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-706414
 There are documented operating procedures. Procedures are not available to the users who need them.	All facility and system operating procedures shall be documented and made available to all users who need them.	CYT-345591







Appendix B

Open tasks by domain - Passwords

ISSUE	RECOMMENDATION	ID
 Your password policy does not require a minimum password length.	Enforce a minimum password length for all passwords.	CYT-999533
 No password management tools is used for secure, centralized management of passwords.	Deploy a password management tool.	CYT-233135
 Users may be using the same password for numerous accounts and services.	Do not use the same password for different user accounts.	CYT-678163
 Users may store passwords in locally saved, unencrypted files.	Prohibit storing passwords in clear text on local files.	CYT-618272
 Some of your company's assets or devices may not comply with your company's password policy.	Enforce company password policy on all assets and devices.	CYT-769629
 Users may be using a relatively simple or easy to hack password.	Educate employees on the value of strong passwords, and how to create them.	CYT-106274
 Your password policy does not require password rotation.	Enforce password rotation for all passwords.	CYT-479013
 Password age has no minimum limit.	Enforce a password Minimum age for all passwords.	CYT-840846

Appendix B

Open tasks by domain - Physical Infrastructure

ISSUE	RECOMMENDATION	ID
 No up-to-date list of authorized personnel to access your physical facilities.	Define and maintain a list of authorized personnel to access company physical facilities.	CYT-971513
 No physical access control at the entrance and exit points to your company's physical facilities.	Enforce physical access control to all company physical-facility entrance and exit points.	CYT-010800
 Removable media assets are not physically protected.	Physically protect removable storage devices, such as portable hard drives and laptops.	CYT-905568
 Secure areas are not appropriately protected.	Implement procedural measures to protect secure areas.	CYT-487257
 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-431987
 Delivery and loading areas are not appropriately protected.	Protect delivery and loading areas.	CYT-381161

Appendix B

Open tasks by domain - Remote Access

ISSUE	RECOMMENDATION	ID
● There is no remote access policy.	Create a remote access policy and have company management approve it.	CYT-833140
● 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-522580
● The company does not conduct remote access awareness activities for employees.	Provide access awareness and security guidelines to all employees.	CYT-938834
● Virtual desktop infrastructure is not enforced for accessing sensitive assets from privately-owned computers.	When using company-owned workstations is not possible, use virtual desktop infrastructure for remote access.	CYT-840436
● Unauthorized or overuse of remote access to company data will not be detected.	Log and monitor remote access to company data and assets	CYT-464605
● 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-321483
● 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-777915
● There is no defined termination time or process of remote access sessions after idle period.	Terminate remote access connection according to predefined conditions.	CYT-135462







Appendix B

Open tasks by domain - Risk Management

ISSUE	RECOMMENDATION	ID
● Lack of risk management practice will lead to gaps in the understanding of the potential risk and overall impact that can be driven upon materialization of a risk.	The company will facilitate the implementation of risk management controls.	CYT-630500
● Critical assets and processes are not identified and cannot be analyzed for their business impact.	The company will identify critical assets and processes, and perform a business impact analysis.	CYT-438968
● Cybersecurity risks cannot be identified since there is no risk assessment.	Conduct risk assessment to identify, rank, mitigate, and monitor cybersecurity risks.	CYT-795670
● There is no risk register.	Establish a cybersecurity risk register.	CYT-811070
● There is no cybersecurity risk remediation plan.	Establish a cybersecurity risk remediation plan.	CYT-558447
● There is no KRI plan.	Establish a Key Risk Indicator (KRI) plan.	CYT-208111
● There is no monitoring and tracking of cybersecurity risks.	Monitor and track cybersecurity risks.	CYT-994005
● The company is not covered by a cybersecurity insurance.	Acquire cybersecurity insurance to protect company assets against potential cybercrime destruction.	CYT-115481


Appendix B

Open tasks by domain - SaaS

ISSUE	RECOMMENDATION	ID
 Your SaaS service providers may not be meeting the required data security regulations and standards.	Verify that all SaaS applications holding company sensitive data comply with the relevant data protection regulation.	CYT-929692
 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-873052
 No measures are in place to mitigate a DDoS attack on your SaaS applications.	Protect SaaS applications from a Distributed Denial-Of-Service attacks (DDoS).	CYT-191226
 Users can access your SaaS applications without detection of risky or suspicious behavior.	Enforce Cloud Access Security Broker (CASB) for all user accounts with access to company SaaS applications.	CYT-529472
 Users log into company SaaS applications using different credentials with no central management.	Enforce a Single Sign-On (SSO) for all user accounts with access to company SaaS applications.	CYT-001328
 No protection mechanism is in place to negate web attacks.	Apply an advanced security tool to negate various website attacks.	CYT-828839

Appendix B

Open tasks by domain - Service Provider Management

ISSUE	RECOMMENDATION	ID
 There is no periodical service-provider security-assessment process.	Conduct periodical service-provider security assessments.	CYT-373569
 There is no guarantee that service-provider contracts define security requirements.	Ensure service-provider contracts define security requirements.	CYT-482316
 Service providers could expose the company to security threats.	Ensure service-provider contracts define security requirements and legally require notifying within a reasonable time of any security weakness which can influence the company.	CYT-201093
 There is no secure service-provider decommission process.	Securely decommission service providers.	CYT-399299





Appendix B

Open tasks by domain - Software Development

ISSUE	RECOMMENDATION	ID
 Not all secure development environments are well protected.	Ensure that all secure development environments are protected from internal and external threats.	CYT-210738
 No tools are used to improve software development process security.	Adopt supporting tools to improve software development security.	CYT-684484
 Access to software code is not restricted.	Protect all forms of code against unauthorized access and tampering.	CYT-826793
 Not all development endpoints are protected against internal and external threats.	Ensure that all development endpoints are protected from internal and external threats.	CYT-572954
 Live data is not carefully managed throughout the software development lifecycle.	Carefully manage live and test data throughout the software development lifecycle.	CYT-958311
 Secure design principles are not applied in software architecture.	Apply secure design principles in software architecture and follow code best practices.	CYT-008125
 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-818205
 Software vulnerabilities are not assessed, prioritized and remediated.	Assess, prioritize, and remediate software vulnerabilities.	CYT-075315
 There is no process for identifying software vulnerabilities.	Regularly search for and identify software vulnerabilities.	CYT-266846
 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-938163
 Software release integrity is not verified.	Verify the integrity of software releases.	CYT-948779
 Management is not fully aware, committed and supportive of the required efforts and practices for secure software development.	Make sure that company management is committed to a secure software development process.	CYT-203170
 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-770717
 Software production environment is not separated from other environments.	Maintain separate development, testing, and operational environments.	CYT-730066












Appendix B

Open tasks by domain - Software Development

ISSUE	RECOMMENDATION	ID
 There is no policy which addresses software vulnerability disclosure and remediation.	Create a software vulnerability disclosure and remediation policy.	CYT-941015
 Vetted security modules and services are not being used.	When possible, use vetted security modules and services, instead of developing new ones.	CYT-543751
 There is no role-based software developments security training program.	Provide software development role-based security training.	CYT-053199
 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-106430

Appendix B

Open tasks by domain - Vulnerability Management

ISSUE	RECOMMENDATION	ID
 New software vulnerabilities and security misconfigurations, which are inherent in any network or system, remain hidden and unmitigated.	Conduct external vulnerability assessments.	CYT-107803
 No vulnerability management plan in place.	Establish and use a vulnerability management policy and plan.	CYT-933946
 Unknown vulnerabilities in your company's web applications and APIs.	Conduct web application vulnerability assessments.	CYT-809488
 Penetration testing is not conducted for externally exposed assets.	Conduct penetration testing for externally exposed assets.	CYT-313367
 Undiscovered and unknown web application vulnerabilities.	Conduct penetration testing for business-critical web applications	CYT-788907
 A Bug Bounty program is not used for discovering web application vulnerabilities.	Use a Bug Bounty program.	CYT-341227
 Found vulnerabilities are not remediated.	Remediate vulnerabilities found during penetration testing.	CYT-072154
 Security tools are not validated following penetration testing.	Validate security tools following penetration testing.	CYT-632199
 There is no penetration testing program.	Establish and maintain a penetration testing program.	CYT-604116
 Penetration testing is not conducted for internal assets and network.	Conduct penetration testing for internal assets and network.	CYT-553099
 Undiscovered and unknown security control vulnerabilities and miss configuration.	Conduct penetration testing for company security systems	CYT-823036










Appendix B

Open tasks by domain - Website

ISSUE	RECOMMENDATION	ID
 No verification relating to the security best practices of your website's or web app's hosting provider.	Maintain security best practices for hosted web servers.	CYT-593957
 No protection mechanism to negate attacks targeting web applications.	Apply a web application firewall (WAF) to negate various attacks targeting web applications.	CYT-845412
 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-153592
 There is no web application penetration testing program for identifying threats.	Conduct penetration testing on all company websites and web applications.	CYT-228974
 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-487386

Appendix B

Open tasks by domain - Workstation and Mobile Devices

ISSUE	RECOMMENDATION	ID
 Workstations are not locked following several failed login attempts.	Lock out after several failed login attempts.	CYT-115823
 Laptops hard drives are not encrypted.	Encrypt laptop hard drives to protect locally stored data.	CYT-110978
 Company workstations are not hardened.	Disable connections to external media.	CYT-550972
 Not all company workstations employ an internal firewall.	Use an internal firewall for all company workstations.	CYT-677248
 Company workstations do not lock out users following a period of inactivity.	Lock out user accounts after a period of inactivity.	CYT-650598
 There are no security measures applied on mobile devices.	Apply security measures on mobile devices.	CYT-569103
 There is no secure workspace for work-related applications on mobile devices.	Create a secure workspace for work-related applications on mobile devices.	CYT-012382
 Not all unapproved services are disabled or uninstalled from company workstations.	Uninstall or disable unnecessary or unapproved services.	CYT-305127
 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-136241