

Inventive - Demo Cybersecurity Analysis Report

September 5, 2025

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.

Please note, this report was prepared by Cynomi platform for the purpose of initial evaluation of your organization's cybersecurity posture. Cynomi does not take responsibility for or relating to the information included in this document or its accuracy and offers no warranty.

Powered by
cynomi

Business Goals

Understanding your company's business goals ensures that risk management efforts are aligned with strategic priorities, enabling a robust and resilient cybersecurity posture.

The following are your top-rated business goals:

Protect customer trust and reputation - Safeguard the organization's image by ensuring security and reliability, maintaining customer confidence.

Enable safe adoption of technology and digital transformation - Implement new technologies securely to enhance capabilities without introducing risks.

Foster a security-aware culture - Promote awareness and good practices among employees to enhance overall security.

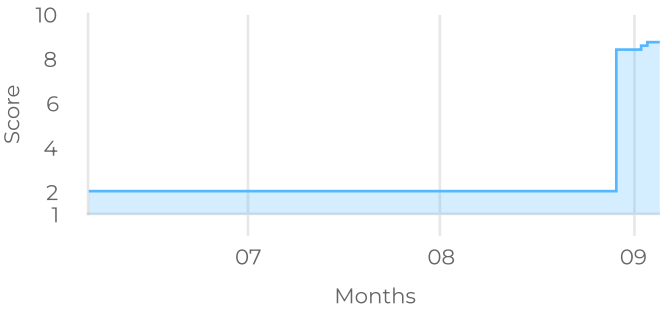
Optimize operational efficiency and reduce costs - Improve processes to work more efficiently and cut unnecessary expenses.

Achieve and maintain regulatory compliance - Follow all legal and regulatory requirements to avoid penalties and legal issues.

Posture Score

8.8 (Out of 10)

Major efforts have been taken. While there is never a 100% guarantee of blocking attacks, the organization is well protected.



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.



Fraud

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



Ransomware

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



Website Defacement

An unauthorized and malicious modification of web page content.



Cybersecurity Readiness Level

Security mapping has identified 30 critical domains requiring protection.

30

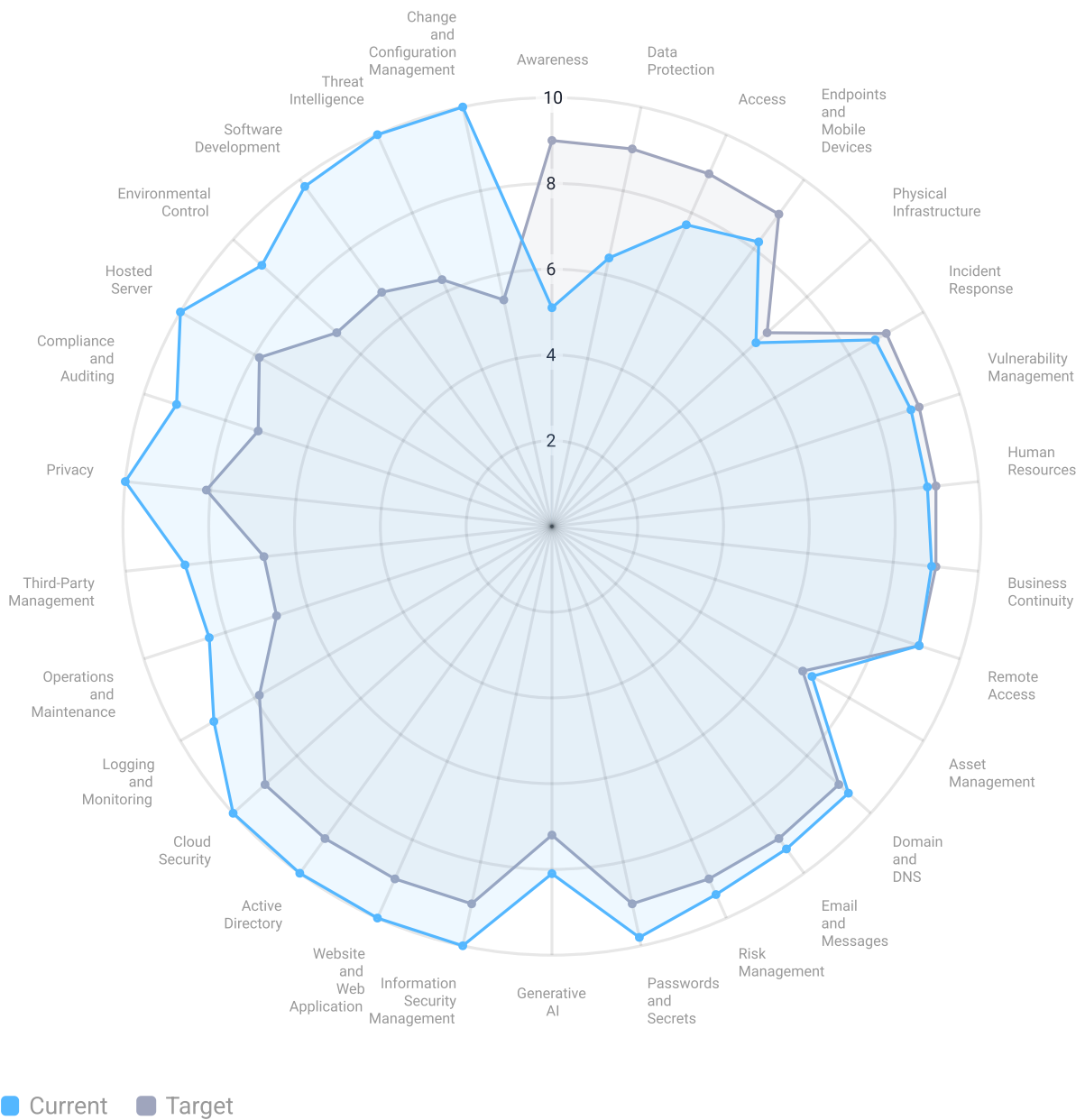
Total Domains

21

Meet target score

9

Under target score



Company Readiness by Security Domain

DOMAIN	SCORE
Access	7.7
Active Directory	10
Asset Management	7
Awareness	5.1
Business Continuity	8.9
Change and Configuration Management	10
Cloud Security	10
Compliance and Auditing	9.2
Data Protection	6.4
Domain and DNS	9.3
Email and Messages	9.3
Endpoints and Mobile Devices	8.2
Environmental Control	9.1
Generative AI	8.1
Hosted Server	10
Human Resources	8.8
Incident Response	8.7
Information Security Management	10
Logging and Monitoring	9.1
Operations and Maintenance	8.4
Passwords and Secrets	9.8
Physical Infrastructure	6.4
Privacy	10
Remote Access	9
Risk Management	9.4
Software Development	9.8

Company Readiness by Security Domain

DOMAIN	SCORE
Third-Party Management	8.6
Threat Intelligence	10
Vulnerability Management	8.8
Website and Web Application	10

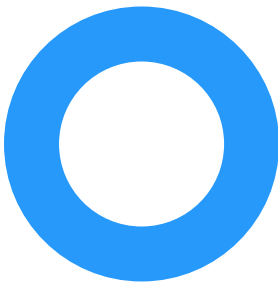
Scan Findings

Severity

23
Findings detected

0	0	0
Critical	High	Medium
0	23	
Low	Info	

External Cynomi scan



- Critical (0)
- High (0)
- Medium (0)
- Low (0)
- Info (23)

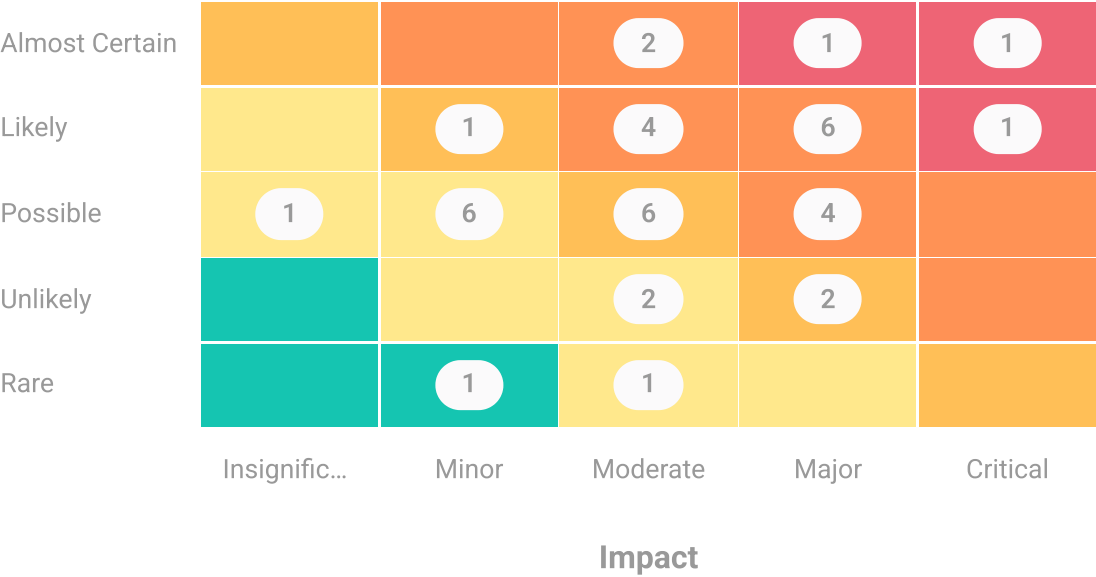
2 targets scanned

Total: 23

Risk Matrix

Understanding your risk matrix is key to producing the correct treatment plan for your company. Displayed here are the company's current risks.

Likelihood



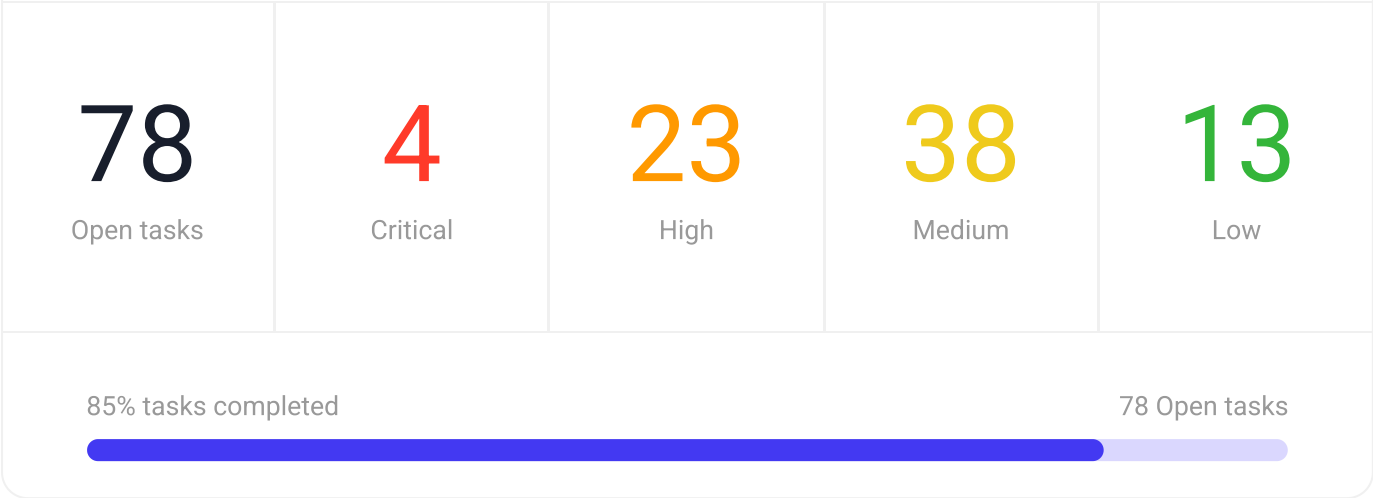
Key Risks

Identifying the key risks with the highest likelihood and greatest potential impact on your organization's objectives is crucial for effectively protecting your company from cybersecurity threats

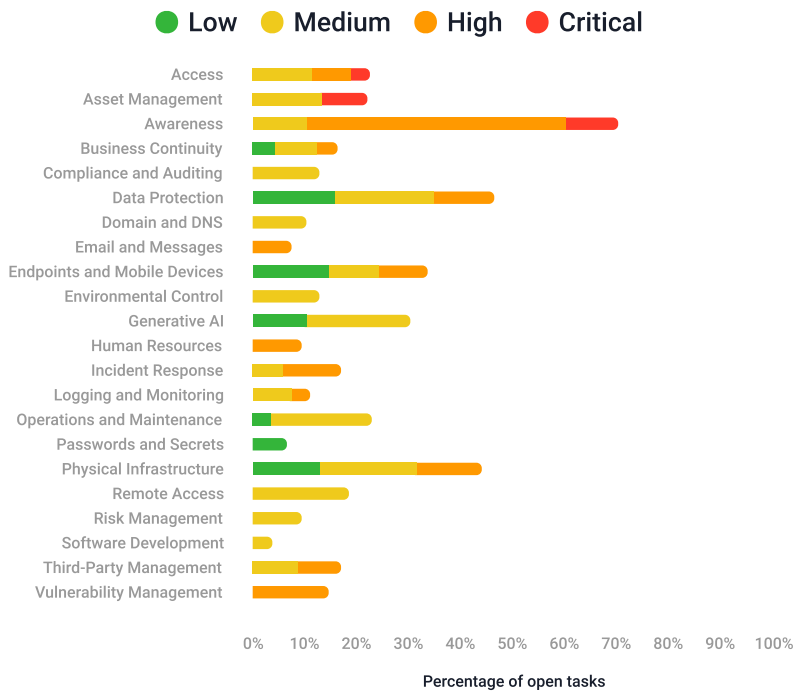
RISK	FUNCTION	RISK SEVERITY
System compromise	Protect, Detect, Respond, Recover	Extreme

Risk Mitigation Plan

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



Open tasks



Task status

78

Not started

Appendix A

Top 10 open tasks

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

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
 Administrators may use the same password for their "normal" activities and admin tasks which require a higher set of privileges.	Administrators are required to use separate passwords and accounts for their admin tasks, enhancing security and maintaining separation of duties.	CYT-00000845259
 The company cannot validate whether or not software asset version is supported.	Only vendor-supported software versions are used, ensuring system security and minimizing risks from unsupported software.	CYT-00000575581
 The company cannot validate whether hardware assets are end-of-life.	Hardware is evaluated on a monthly basis, ensuring continued performance, security, and compliance with company standards.	CYT-22656752867
 There are no cybersecurity exercises for employees.	Attack simulations are conducted for all employees, ensuring preparedness against potential threats.	CYT-00000555493
 Data stored on external storage devices is not consistently backed up, verified, or securely stored elsewhere, increasing the risk of data unavailability in the event of device loss, damage, or compromise.	Critical data stored on external storage devices, such as hard drives, is included in the regular backup routine, ensuring its availability for recovery in the event of loss, damage, or compromise.	CYT-00000166736
 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.	Formal agreements such as SLAs, confidentiality agreements, and data-sharing agreements with third-party contractors are created, ensuring data security during external interactions.	CYT-00000356369
 There is no limitation or management of access to shared resources.	Access to sensitive data stored in shared resources is restricted, ensuring it is only available to authorized individuals.	CYT-00000036602
 There is no mapping of data according to the regulations or contractual agreements it needs to comply with.	Data types subject to regulations or contractual obligations are mapped and protected according to compliance requirements, ensuring legal and contractual compliance.	CYT-00000604160
 The role-based access control is not used on privileged accounts.	Each privileged role is verified to ensure only the minimum access permissions needed are granted.	CYT-00000084849


Appendix A

Top 10 open tasks (Cont.)

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

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
-------	--------------	---------

 There is no enforcement of access rights and permission granting.	Access rights and permissions are granted based on role requirements, ensuring that users have appropriate levels of access aligned with their responsibilities.	CYT-00000090351
---	--	-----------------

Appendix B

Open tasks by domain - Access






 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
 Administrators may use the same password for their "normal" activities and admin tasks which require a higher set of privileges.	Administrators are required to use separate passwords and accounts for their admin tasks, enhancing security and maintaining separation of duties.	CYT-00000845259
 The role-based access control is not used on privileged accounts.	Each privileged role is verified to ensure only the minimum access permissions needed are granted.	CYT-0000084849
 There is no enforcement of access rights and permission granting.	Access rights and permissions are granted based on role requirements, ensuring that users have appropriate levels of access aligned with their responsibilities.	CYT-0000090351
 Authentication information feedback is not blurred.	Authentication feedback is blurred, preventing unauthorized users from gaining information during the login process.	CYT-00000460255
 With more active sessions, the risk of session hijacking increases.	The number of concurrent sessions per user is limited, ensuring secure access control and minimizing the risk of session-based attacks.	CYT-79273698792
 User accounts are not adjusted following changes to the role, access rights revocation, or position changes.	Users' access rights and privileges are adjusted upon role changes, ensuring alignment with their new responsibilities and minimizing unnecessary access.	CYT-00000632658

Appendix B

Open tasks by domain - Asset Management

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
 The company cannot validate whether or not software asset version is supported.	Only vendor-supported software versions are used, ensuring system security and minimizing risks from unsupported software.	CYT-00000575581
 The company cannot validate whether hardware assets are end-of-life.	Hardware is evaluated on a monthly basis, ensuring continued performance, security, and compliance with company standards.	CYT-22656752867
 Unauthorized hardware and software assets are not removed.	Unauthorized hardware and software assets are promptly removed, ensuring compliance and security within the network.	CYT-00000375233
 There is no formal approval process to control the removal of assets out of company premises.	Assets are not removed from company premises without authorization, and those taken out are protected to maintain security.	CYT-00000457288
 Removable media is not securely handled.	Procedures are developed to securely manage removable media, ensuring safe handling and protection against unauthorized access.	CYT-00000243600

Appendix B

Open tasks by domain - Awareness





 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
 There are no cybersecurity exercises for employees.	Attack simulations are conducted for all employees, ensuring preparedness against potential threats.	CYT-00000555493
 There is no process for ensuring employee commitment to company cybersecurity policy.	All employees are aware of and have signed the company cybersecurity policy, confirming their commitment to compliance.	CYT-00000549414
 There is no improvement protocol for company security awareness programs.	Training data is collected and stored, supporting continuous improvement and compliance tracking.	CYT-00000906502
 There is no security awareness program for software developers.	Role-based cybersecurity awareness and skills training is conducted for company software developers, ensuring they are equipped to address development-related risks.	CYT-00000176684
 There is no security awareness program for cybersecurity personnel, IT administrators and DevOps staff.	Cybersecurity awareness training is provided to users with administrative access, ensuring they understand the risks and their responsibilities in protecting company assets.	CYT-00000801509
 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.	Physical security personnel are provided with cybersecurity awareness training, ensuring alignment between physical and digital security practices.	CYT-69955260505
 There is no employee security awareness program for detecting and reporting cyber incidents.	Cybersecurity awareness training is conducted for employees, focusing on detecting and reporting potential cyber incidents.	CYT-00000585743

Appendix B

Open tasks by domain - Business Continuity

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
 Data stored on external storage devices is not consistently backed up, verified, or securely stored elsewhere, increasing the risk of data unavailability in the event of device loss, damage, or compromise.	Critical data stored on external storage devices, such as hard drives, is included in the regular backup routine, ensuring its availability for recovery in the event of loss, damage, or compromise.	CYT-00000166736
 The organization does not assess or monitor the expected failure timelines of critical system components, leading to unplanned outages due to predictable failures that could have been mitigated through proactive maintenance or timely replacement.	Mean Time To Failure (MTTF) is calculated for critical system components, informing maintenance, replacement and continuity strategies.	CYT-96616152001
 The organization lacks a predefined safe mode of operation, increasing the risk that systems will continue operating in an unstable or insecure state during a disruption, potentially worsening the impact.	A safe mode of system operation is established, ensuring critical systems can function securely and reliably during disruptions.	CYT-04554102925
 The organization lacks defined and tested alternate communication protocols, making it unprepared to maintain essential communications during disruptions.	An alternate communication protocols plan is established, ensuring continued communication during disruptions.	CYT-85809601276

Appendix B

Open tasks by domain - Compliance and Auditing

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<div><div></div><div>There is no external audit of cybersecurity policies and protection processes.</div></div>	Periodic external audits of the company's cybersecurity policies and protection processes are undertaken, ensuring adherence to industry standards.	CYT-00000733894

Appendix B

Open tasks by domain - Data Protection

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<p>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.</p>	<p>Formal agreements such as SLAs, confidentiality agreements, and data-sharing agreements with third-party contractors are created, ensuring data security during external interactions.</p>	<p>CYT-00000356369</p>
<p>There is no limitation or management of access to shared resources.</p>	<p>Access to sensitive data stored in shared resources is restricted, ensuring it is only available to authorized individuals.</p>	<p>CYT-00000036602</p>
<p>There is no mapping of data according to the regulations or contractual agreements it needs to comply with.</p>	<p>Data types subject to regulations or contractual obligations are mapped and protected according to compliance requirements, ensuring legal and contractual compliance.</p>	<p>CYT-00000604160</p>
<p>Neglecting proper labeling introduces a security weakness by causing unclear data management processes and increasing the likelihood of mishandling sensitive information, which includes unauthorized access or unintended exposure.</p>	<p>Accurate information labeling protocols are developed, ensuring consistent classification and security of data.</p>	<p>CYT-19415479561</p>
<p>The use of removable storage devices in external systems is not limited.</p>	<p>The use of removable storage devices in external systems is limited, ensuring reduced exposure to potential risks.</p>	<p>CYT-00000364879</p>
<p>Data lifecycle is not governed</p>	<p>A Data Governance Body is established, ensuring proper oversight and management of data security practices.</p>	<p>CYT-42972026705</p>
<p>Data integrity between agencies is not managed.</p>	<p>A Data Integrity Board is established, ensuring the protection of data accuracy and consistency.</p>	<p>CYT-73466071797</p>
<p>Matching programs are not approved.</p>	<p>The processing of data in a matching program is controlled, ensuring compliance and data integrity.</p>	<p>CYT-13720863380</p>
<p>Data cannot be processed in a systems failure</p>	<p>Data diversity is ensured, reducing redundancy and strengthening data protection.</p>	<p>CYT-51370895894</p>

Appendix B

Open tasks by domain - Data Protection

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
 There is no limitation on folder or file-sharing from employee workstations.	File-sharing of employee workstation folders is prevented, ensuring data security in the workplace.	CYT-00000422881
 The information posted on public systems is not carefully monitored.	Any information posted or processed on publicly accessible information systems is monitored and controlled, ensuring it meets security standards.	CYT-00000456589
 System of Record Notices are not published	System of Record Notices are generated, ensuring accurate documentation of data processing activities.	CYT-46910822503

Appendix B

Open tasks by domain - Domain and DNS

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<div><div></div><div>Your company does not limit internet access to its internal DNS server.</div></div>	Company DNS server connectivity to the internet is enforced through an approved DNS resolver, ensuring secure and monitored DNS access.	CYT-00000880006

Appendix B

Open tasks by domain - Email and Messages








 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<div><div></div><div>There is no advanced email protection tool implemented.</div></div>	An advanced email protection tool is implemented to detect and mitigate sophisticated email-based threats.	CYT-00000578636

Appendix B

Open tasks by domain - Endpoints and Mobile Devices

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
 Company workstations are not hardened.	External media connections are disabled to prevent unauthorized data transfers and security risks.	CYT-00000550972
 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.	Unauthorized software installation on workstations is prevented to maintain system integrity.	CYT-00000053930
 Workstations have too many functions	Kiosks and thin clients are utilized where applicable, improving security and reducing system complexity.	CYT-89422704790
 Workstations are not centrally managed and controlled.	Operating systems and hardware configurations are centrally managed, ensuring consistency and streamlined security management.	CYT-00000309102
 Systems are not refreshed to a known good state regularly	Non-persistent security controls are implemented to enhance system security and minimize vulnerabilities.	CYT-44587121760
 The organization relies on applications which cannot be reconstituted on any platform in the event of a failure or attack.	Platform-independent applications are used when possible, ensuring compatibility and reducing risks.	CYT-81444088910
 There are no restrictions on the number of local admins per workstation.	Local admin accounts are minimized and securely managed, reducing the risk of unauthorized access.	CYT-00000136241

Appendix B

Open tasks by domain - Environmental Control

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<div><div></div><div>Environmental hazards are not considered when selecting a facility location</div></div>	Facility location planning is conducted to minimize risks from physical and environmental hazards, ensuring asset protection.	CYT-09958734532

Appendix B

Open tasks by domain - Generative AI

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<div><div></div><div>Employees could use services in a way that can violate laws or regulations.</div></div>	AI-generated content that could facilitate fraud, crime, impersonation, or harm is strictly prohibited.	CYT-73198496450
<div><div></div><div>Dissemination of biased content can perpetuate stereotypes, alienate certain groups, and harm the company's reputation.</div></div>	AI-generated content is reviewed for biases to ensure fairness and objectivity.	CYT-95173210116
<div><div></div><div>Failure to label data origins can lead to a lack of transparency, making it difficult to trace the source of information.</div></div>	AI-generated content is labeled to indicate its origin, ensuring transparency in its creation.	CYT-84991301956

Appendix B

Open tasks by domain - Human Resources




 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<div><div></div><div>Appropriate background checks are not carried out for employees ahead of issuing them access to company systems and data.</div></div>	Candidate background checks are performed before employment and before issuing access to company systems or data, ensuring secure hiring practices.	CYT-00000876235

Appendix B

Open tasks by domain - Incident Response

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
 No third-party Incident Response (IR) support.	A third-party incident response vendor is engaged to ensure fast response and post-incident reviews.	CYT-00000373508
 Critical information gathering is missing from your incident response preparation phase.	An updated company asset inventory is maintained, including network topology and sensitive data locations, ensuring proper tracking and protection.	CYT-00000791067
 Incident Response (IR) tabletop exercises are not conducted.	Incident response practice sessions are conducted to improve company readiness and understanding.	CYT-00000581352

Appendix B

Open tasks by domain - Logging and Monitoring

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<div><div></div><div>Unreliable event detection processes may result in missed security events and delayed responses to incidents.</div></div>	Event detection processes are validated for reliability, ensuring accurate detection of security incidents.	CYT-84895482286
<div><div></div><div>Log records are not backed up on a separate system than the system creating the logs.</div></div>	Log records are periodically backed up and stored in a system separate to the one conducting the monitoring, ensuring data protection.	CYT-00000798631
<div><div></div><div>It is not possible to delete only one single log from log storage.</div></div>	Log storage is configured to enable secure deletion, ensuring compliance with retention policies.	CYT-00000763838

Appendix B

Open tasks by domain - Operations and Maintenance

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
 Systems are not tracked to origin	System provenance is tracked, ensuring accountability and traceability of operational systems.	CYT-95244422867
 Security is not aligned with enterprise IT architecture.	Enterprise IT architecture aligns with industry-recognized practices, ensuring standardized and secure design.	CYT-00000887704
 Systems stay in an unchanged state for long periods of time	Concealment and misdirection techniques are implemented to confuse attackers and protect critical assets.	CYT-56247190759
 Systems are not redundant	Systems are designed for redundancy with distributed processing and storage, ensuring continuity and fault tolerance.	CYT-19615771764
 Using single vendor technologies makes vulnerabilities and exploits more impactful to the organization	A diverse set of technologies is used when selecting system components to enhance security and reduce risk.	CYT-62119420731
 There is no separation of duties between development, and production environments.	A separation of duties is maintained between development and production environments to ensure accountability and reduce security risks.	CYT-00000738316
 Critical systems environments cannot be fully protected from tampering	Systems are deployed using read-only storage, ensuring data integrity and preventing unauthorized modifications.	CYT-74462421480

Appendix B

Open tasks by domain - Passwords and Secrets








 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<div><div></div><div>Password minimum age is not enforced.</div></div>	A minimum age for passwords is enforced, ensuring users cannot frequently reset passwords to reuse the same credentials.	CYT-00000840846

Appendix B

Open tasks by domain - Physical Infrastructure

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
 No up-to-date list of authorized personnel to access your physical facilities.	A list of authorized personnel with access to the company's physical facilities is defined and maintained to enhance physical security.	CYT-00000971513
 Undetected surveillance devices or technical vulnerabilities compromise sensitive information	Technical surveillance countermeasures surveys are performed to detect and mitigate potential surveillance risks in company facilities.	CYT-69592865130
 Systems communications can be intercepted remotely through RF leakage	Systems are protected from electromagnetic signal leakage to prevent unauthorized data access and leakage.	CYT-08385473561
 The company lacks a standardized process for escorting and monitoring visitors, introducing inconsistencies and potential security vulnerabilities.	Visitors are escorted, and their activity is monitored within the company premises to ensure security and compliance.	CYT-00000787888
 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.	Visitors and external technicians are required to deposit personal devices, ensuring secure access to company facilities.	CYT-29634626747
 Infrastructure is not protected from electromagnetic pulses	Infrastructure is protected from electromagnetic pulses (EMPs) to maintain operational continuity and data security.	CYT-82850167780
 Delivery and loading areas are not appropriately protected.	Delivery and loading areas are protected to prevent unauthorized access and potential threats to company assets.	CYT-00000381161

Appendix B

Open tasks by domain - Remote Access

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<ul style="list-style-type: none">There is no defined termination time or process of remote access sessions after idle period.	Remote access connections are terminated based on predefined conditions, ensuring secure and controlled disconnection procedures.	CYT-00000135462
<ul style="list-style-type: none">Company users can use public Wi-Fi networks to access company assets.	Public Wi-Fi is not used for remote access except under exceptional circumstances and with necessary precautions, ensuring secure remote connections.	CYT-00000321483

Appendix B

Open tasks by domain - Risk Management

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<div><div></div><div>The company is not covered by a cybersecurity insurance.</div></div>	Cybersecurity insurance is acquired to protect company assets against potential losses from cybercrime incidents.	CYT-00000115481

Appendix B

Open tasks by domain - Software Development

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<div><div></div><div>There is no process for identifying and communicating software component security requirements to third-party providers.</div></div>	Software component security requirements are identified and communicated to third-party providers to ensure compliance.	CYT-00000983608

Appendix B

Open tasks by domain - Third-Party Management

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<div><div></div><div>Counterfeit or tampered assets can come into the organization through the supply chain</div></div>	The authenticity of all components is verified, ensuring that no counterfeit or compromised parts enter the supply chain.	CYT-65075576751
<div><div></div><div>Failing to review due diligence results and management's recommendations regarding third-parties may result in insufficient oversight of external partners and potential risks.</div></div>	The board, board committee, or appointed professional reviews due diligence results, including management's recommendations, ensuring informed decisions regarding third-party usage.	CYT-08119651130

Appendix B

Open tasks by domain - Vulnerability Management

 Repeat task  Repeat task - overdue

ISSUE	REQUIREMENTS	TASK ID
<div><div></div><div>A Bug Bounty program is not used for discovering web application vulnerabilities.</div></div>	A Bug Bounty program is implemented, incentivizing external researchers to report vulnerabilities, enhancing the organization's security posture.	CYT-00000341227
<div><div></div><div>Undiscovered and unknown web application vulnerabilities.</div></div>	Penetration testing is conducted for business-critical web applications, ensuring they are resilient against sophisticated attacks.	CYT-00000788907