Cybersecurity Health Assessment

SAMPLE

THRIVE℠

Assessment Scope & Approach

SCOPE

Sample Company, LLC has selected Thrive to assess their current security program and determine the state of organizational security posture. The deliverable is a document reviewing current areas of risk while outlining both tactical and strategic recommendations to address gaps and identify improvement opportunities in the following areas in alignment with the CIS framework:

01 Inventory & Control of Enterprise Assets	02 Inventory & Control of Software Assets	03 Data Protection
04 Secure Configuration of Enterprise Assets & Software	05 Account Management	06 Access Control Management
07 Continuous Vulnerability Management	08 Audit Log Management	09 Email & Web Browser Protections
10 Malware Defenses	11 Data Recovery	12 Network Infrastructure Management
13 Network Monitoring & Defense	14 Security Awareness & Skills Training	15 Service Provider Management
16 Applications Software Security	17 Incident Response Management	18 Penetration Testing

APPROACH

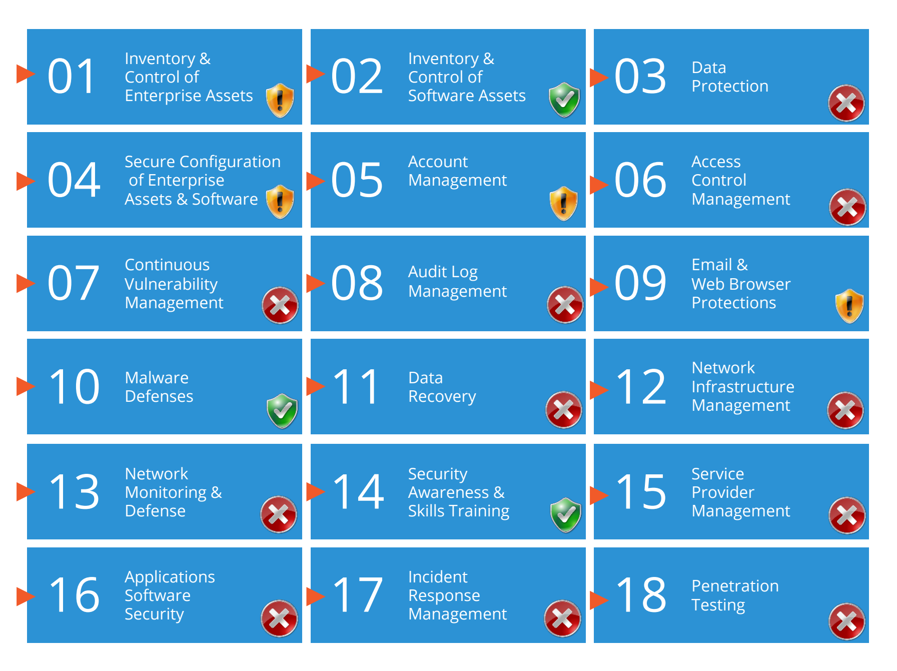
Thrive Consultants review technology infrastructure and security systems using a combination of automated and manual data collection methods. Thrive also utilizes existing technology and security management systems to assist with discovery and evaluation. This assessment has been conducted using automated tools, as well as screenshots and stakeholder interviews performed during the assessment period.

- Review the provided documentation
- Review the results of automated data collection tools
- Manual review of systems, infrastructure and critical devices
- Conduct staff interviews
- Compare findings to industry accepted best practices
- Conduct a Thrive peer review to recommend solutions

THRIVE™

Executive Summary

Security Program Overview



01 Inventory & Control of Enterprise Assets !	02 Inventory & Control of Software Assets ✓	03 Data Protection ✗
04 Secure Configuration of Enterprise Assets & Software !	05 Account Management !	06 Access Control Management ✗
07 Continuous Vulnerability Management ✗	08 Audit Log Management ✗	09 Email & Web Browser Protections !
10 Malware Defenses ✓	11 Data Recovery ✗	12 Network Infrastructure Management ✗
13 Network Monitoring & Defense ✗	14 Security Awareness & Skills Training ✓	15 Service Provider Management ✗
16 Applications Software Security ✗	17 Incident Response Management ✗	18 Penetration Testing ✗

✓	Meets Best Practices
!	Improvement Opportunity
✗	Risk Identified

Current State Executive Summary

01 Inventory & Control of Enterprise Assets	02 Inventory & Control of Software Assets	03 Data Protection
04 Secure Configuration of Enterprise Assets & Software	05 Account Management	06 Access Control Management
07 Continuous Vulnerability Management	08 Audit Log Management	09 Email & Web Browser Protections
10 Malware Defenses	11 Data Recovery	12 Network Infrastructure Management
13 Network Monitoring & Defense	14 Security Awareness & Skills Training	15 Service Provider Management
16 Applications Software Security	17 Incident Response Management	18 Penetration Testing

CURRENT STATE RISKS

- Patch management does not have formalized policy with scheduled patch deployment from the administration.
- Vulnerability management process is not a function of the organization. Vulnerability scanning and formalized scheduling within an administrative document are required to meet this security control.
- Established audit log management policy and procedures were not identified. This procedural document should define how the organization addresses the collection, review, and retention of audit logs.
- Detailed audit logging is not a function of the organization. A Security Information and Event Management (SIEM) tool is not in place throughout the organization which would create the necessary centralized audit logging.
- Ticketing systems internally do not exist for request and incident tracking.
- Technical controls are not configured to block unsupported browser and email clients. This is both necessary from a security update standard and a data loss prevention tactic.
- Spam filtering is provided through Microsoft ATP tools and is configured with default standards. Sandboxing and archiving is not a function of this tool and third-party spam filtering is recommended.
- Data recovery policy and procedures are not formalized administratively. There is no policy or document that addresses the scope of data recovery activities, recovery prioritization, and the security of backup data.
- Disaster recovery with dedicated real time replication for minimized Return Time Objective and Return Point Objectives are not a function of the organization.
- Disaster Recovery and Business Continuity plan were not provided during this assessment.

THRIVE™

FUTURE STATE

- Vulnerability management administrative controls that define the scheduling of third-party vulnerability scans monthly, tooling for consistent internal vulnerability scanning, and patch management strategy and schedule. The vulnerability management document will include a mitigation strategy with stages that include Identification, Evaluation, Mitigation, and Reporting.
- Security Information and Event Management (SIEM) tool alongside a 24x7 Security Operations Center (SOC) to centralized audit logging throughout the environments management applications, security tools and network infrastructure. This will provide real time traffic monitoring and incident alert for proactive incident response and mitigation on a 24x7 basis.
- Internal ticketing system established for tracking and resolving requests, events, and incidents. Consistent review of tickets will be a form of remediation to proactively mitigate issues within the environment.
- Third party spam filtering tools deployed in front of the current email platform. Layering security tools with more in-depth functionality such as sandboxing will have a higher success rate in stopping malicious email attempts.
- Disaster recovery procedure and official runbook created for an administrative step by step detailed to restore the technology environment and business functionality. This will have qualified Return Time Objectives and Return Point Objectives for all data classifications.
- Disaster recovery specific tooling implemented to replicate data in real time to a secondary off-site SOC 2 complaint datacenter storage facility. This be accompanied by a yearly disaster recovery fail over test.

Ransomware Threat Mitigation

Formal Security Program	🟥	DNS Based Security Tools	🟩
Adopted Security Framework	🟥	Vulnerability Scanning	🟥
Next Generation Firewall	🟩	EDR Based Endpoint Protection	🟩
Mail Hygiene Services	🟨	Backup Strategy	🟨
Cyber Security Awareness Training	🟩	Disaster Recovery Strategy	🟥
Regular System Patching	🟨	Operating System Currency	🟩
Multi-Factor Authentication	🟩	SIEM/SOC	🟥

THRIVE

Project Planning & Recommendations

Project Planning & Recommendations

LEGEND

🟢 LOW 🟡 MEDIUM 🟠 HIGH ⚠ CRITICAL

Priority	Project Description	One-Time	Monthly OpEx
⚠	Backup Policy and Retention Update	**TBD**	**TBD**
⚠	Disaster Recovery Replication and Policy Runbook	**$0,000.00**	**$0,000.00**
🟠	Security Framework Implementation	**-**	**$0,000.00**
🟠	Security Information and Event Management w/ 24x7 SOC	**$0,000.00**	**$0,000.00**
🟠	Ticketing System Implementation	**$0,000.00**	**$0,000.00**
🟠	Server Cloud Migration and On-Premise Device Removal	**TBD**	**TBD**
🟡	M365 OneDrive/SharePoint and Full Suite Utilization	**TBD**	**TBD**
🟡	Network Segmentation Project	***$0,000.00**	**-**
🟡	SaaS Office 365 Third-Party Backup	**$000.00**	**$0,000.00**
🟢	Message Hygiene Third-Party Spam Filter	**$0,000.00**	**$0,000.00**
🟢	Vulnerability Scanning Monthly	**$000.00**	**$0,000.00**

*** Subject to change with further discovery**

THRIVE™

Security Control Analysis

Security Control Analysis

Data Protection

OBSERVATION	ASSESSMENT
🟩 Data access control lists are established within active directory security groups and group policy. These are standard controls for user permissions that meet best practice tooling. 🟩 Device encryption is standardized on end user machines with BitLocker deployed. 🟩 Removable media device blocking for data loss prevention is established as policy on end user devices. 🟩 Data loss prevention strategies are lacking on authorized controls for web email access, unauthorized file sharing applications, and local file saving that is allowed on end user devices. 🟥 Data management processes and policies were not defined or delivered during this assessment. Data retention is set within technical controls by third-party backup tools; however, this is not formalized within an administrative document. Retention limits, disposal requirements, sensitivity classifications and data inventory policy reviewal should all be standardized administratively. 🟥 File data hosting strategy is accessed with Windows NTFS shared drives locally stored on premise. Some of the data stored is hosted on Domain Controllers without a dedicated server machine. 🟥 Data retention is configured to 90 days with third party offsite backup systems established. Organizations within financial services are recommended to have backup retention set to seven years. 🟥 Data disposal requirements within formalized documentation at an administrative level is not in place today. 🟥 Centralized data access logging is not fully established across all applications within the environment.	Data management strategies clearly defined within an administrative policy is necessary to meet this security framework. This should include retention limits, disposal requirements, sensitivity classifications and data inventory reviewal. These definitions are recommended to meet compliance of the governing body within an organizations vertical. SEC compliance states data must be retained for seven years with the latest two years' worth of data easily accessible. Servers that host critical business data that is actively in use should be stand-alone in function. Domain controllers should not be the utilized for drive mapping and data hosting. Future state recommendations include migrating on premise servers into a cloud hosted data center and full M365 OneDrive/SharePoint utilization as the main critical data hosting and sharing platform.

Thank You

THRIVE℠

THRIVE™