CP

CYBERPOOLS.ORG

Cybersecurity Risk Assessment

Sample Organization

Assessment Date:	11/05/2025
Report Date:	11/05/2025
Conducted By:	Assessment Team
Member Contact:	Contact Person

Introduction

What is a Cyber Risk Assessment?

A cyber risk assessment is the process of identifying, evaluating, and prioritizing potential security threats to an organization's assets and infrastructure. This includes analyzing the likelihood and impact of these risks and determining the measures and controls to be put in place to mitigate them. The goal of a cyber risk assessment is to improve an organization's cybersecurity posture and prevent data breaches, unauthorized access, and other types of cyber-attacks.

Methodology

The following categories have been derived from previous version of the risk assessment which questions were influenced from previous cyber insurance claims, cybersecurity best practices, and common knowledge derived from the cybersecurity industry and as outlined by organizations such as NIST (National Institute of Standards and Technology), CISA (Cybersecurity and Infrastructure Security Agency) and CIS (Center for Internet Security).

It is recommended that organizations schedule a review meeting with appropriate district personnel to discuss identified risks and to define remediation actions.

Grading Methodology Update

As of September 2025, and in alignment with our continuous improvement practices across all Cyber Toolkit services, CyberPools has enhanced the grading formula used in this assessment. The updated methodology ensures that scores more accurately reflect implementation status across each control category and the overall assessment.

While the overall score provides a high-level benchmark, members should place greater emphasis on the control categories and the associated risk ratings (Low, Medium, High). These ratings highlight which areas carry greater weight in reducing organizational risk and therefore warrant more focused attention during remediation planning.

> **Questions or Feedback:** For any questions about our risk assessment or grading, please reach out to cyber@cyberpools.org

Executive Summary

[EXECUTIVE SUMMARY - CUSTOMIZED BY ACCOUNT MANAGER]

This section provides a high-level strategic overview of the assessment findings. The Account Manager reviews the detailed results and synthesizes key strengths and priority opportunities for improvement.

Sample Executive Summary:

"The organization demonstrates strong cybersecurity fundamentals with excellent performance in access management and incident response capabilities. A mature backup strategy and comprehensive security awareness program reflect the organization's commitment to operational resilience. Primary opportunity exists in implementing DNS filtering to strengthen malware defense posture. Overall, the assessment reveals a well-managed security program with focused areas for enhancement."

Note: This placeholder text will be replaced with custom content entered by the Account Manager in the CRM system. The executive summary should be 4-8 sentences highlighting strategic insights, key strengths, and priority recommendations.

Summary of Results

80%

OVERALL RISK SCORE

2

HIGH RISK

3

MODERATE RISK

45

LOW RISK

Section Scores

NO.	SECTION	SCORE
1.0	Inventory and Control of Assets	**96%**
2.0	Account Management	**67%**
3.0	Data Protection	**56%**
4.0	Secure Configuration of Enterprise Assets	**95%**
5.0	Malware Defense	**83%**
6.0	Data Recovery	**25%**
7.0	Security Awareness	**106%**
8.0	Vendor Management	**103%**
9.0	Incident Response Management	**73%**

Assessment Methodology

Rating Legend

CONTROL RATING	IMPACT RATING	RISK RATING
Fully Implemented Control(s) are fully implemented and effective at mitigating risk.	**Low (1)** Minimal disruption of operations and no sensitive data compromised or exfiltrated.	**Low (0-9)** Overall risk is low to organization
Partially Implemented Controls are partially implemented and somewhat effective in mitigating risk.	**Moderate (3)** Operational disruptions of operations but no sensitive data compromised or exfiltrated.	**Moderate (10-15)** Overall risk is moderate to organization
Not Implemented Control(s) are nonexistent.	**High (5)** Significant disruption of operations and sensitive data compromised or exfiltrated.	**High (16-25)** Overall risk is high to organization.
Not Applicable Control(s) are not necessary or applicable to the environment.	**Not Applicable (0)** No impact to your organization or environment as a result of the missing control.	**Not Applicable (0)** No risk posed as a result of the missing control.

Scoring Methodology

Raw Score Calculation

Each control is evaluated using a two-factor calculation that multiplies the implementation status by the potential impact to the organization.

Formula: Control Rating × Impact Rating

Control Rating: Indicates control implementation status.

- 1 = Fully Implemented
- 3 = Partially Implemented
- 5 = Not Implemented

Impact Rating: Reflects the level of organizational disruption if the control fails.

- 1 = Low impact (minimal disruption, no data compromise)
- 3 = Moderate impact (operational disruption, no sensitive data compromise)
- 5 = High impact (significant disruption and/or data compromise)

Score Normalization

Raw scores are normalized to a 0–100 scale to produce comparable category and overall scores across assessments.

- Ensures organizations can be measured consistently year over year.

- Maintains alignment with industry benchmarks and CyberPools grading standards.
- Keeps the model sensitive to partially implemented controls versus complete gaps.

Risk Calculation Example

> **Control:** Multi-factor Authentication
>
> **Control Rating:** Partially Implemented (3)
>
> **Impact Rating:** High (5)
>
> **Raw Risk Score:** 3 x 5 = 15
>
> **Result:** 15 scores as moderate risk based on risk rating legend above.

How to Read This Report

This assessment provides a comprehensive evaluation of your organization's cybersecurity posture. Each section is designed to give you actionable insights with full context for decision-making.

> ### Report Structure
>
> **Control Categories:** Nine security focus areas covering the full spectrum of cybersecurity controls
>
> **Category Scoring:** Each category receives an overall percentage score (higher is better)
>
> **Individual Questions:** Detailed assessment of specific controls within each category

Understanding Category Pages

Each category section includes:

1 **Category Header**

Category number, name, and overall score percentage with visual grade badge

2 **Category Overview**

Brief description of what this category covers and why it matters

3

Why It Matters

Business impact and real-world risks if controls in this area fail

4

Control Assessment Questions

Detailed evaluation of individual controls (see breakdown below)

Understanding Question Blocks

Each control question provides comprehensive context:

Question Number & Text	e.g., 1.1 Does the organization inventory all devices?
Control Description	Explains what the control does and best practices
Control Status	FULLY IMPLEMENTED (1) PARTIALLY IMPLEMENTED (3) NOT IMPLEMENTED (5)
Impact	LOW (1) MODERATE (3) HIGH (5)
Risk Score	Calculated as Control Status × Impact. Higher scores indicate greater risk.
Assessment Notes	Field observations, evidence, and context from the assessment team

Using This Report

- Review the **Key Findings** section first for immediate priorities
- Use category scores to identify focus areas for improvement
- Reference Assessment Notes for specific remediation guidance
- Track progress over time by comparing scores between assessments

⚠ KEY FINDINGS

The following controls were highlighted based on their risk scores and should be reviewed with the stakeholder team.

High Risk Findings (2)

Risk Score 16-25 – requires immediate attention.

0.0 Unknown Question (ID: ddc56966...)

Category: Account Management

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 25 - HIGH

> They have a separate login for the vpn, then another login for the network. No MFA currently

0.0 Unknown Question (ID: e95173e9...)

Category: Data Recovery

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 25 - HIGH

> Can't say we do it often.

Moderate Risk Findings (3)

Risk Score 11-15 – schedule remediation activities.

0.0 Unknown Question (ID: ee21191d...)

Category: Data Protection

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 15 - MODERATE

> No separation of accounts.

0.0 Unknown Question (ID: cd72f5cf...)

Category: Data Recovery

Control Status: PARTIALLY IMPLEMENTED (3) Impact: MODERATE (3) Risk Score: 15 - MODERATE

> tabled for a response

0.0 Unknown Question (ID: 66fb305d...)

Category: Incident Response Management

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 15 - MODERATE

> No testing yet.

Cyber Requirements Compliance

The following table summarizes compliance with critical cybersecurity requirements identified by CyberPools. These requirements represent essential controls that significantly reduce organizational risk.

NO.	REQUIREMENT	COMPLIANCE

Note: Items marked "No" represent areas requiring immediate remediation to ensure compliance with cybersecurity best practices and insurance requirements.

1.0

Inventory and Control of Assets

96%

Overview

> Inventory and Control of Assets refers to the practice of keeping track of all the devices an organization owns or uses, such as computers and servers. This enables the organization to know where everything is, who owns it, and whether there are any security issues. Having control over assets means implementing processes to manage, secure, and track them effectively, and to prevent unauthorized access. It also helps to identify unauthorized and unmanaged assets to remove or remediate them, reducing cybersecurity risks. Maintaining an inventory and control of assets is a critical component of any organization's cybersecurity program.

Importance

Having an up-to-date inventory and control of assets helps organizations identify and prioritize security risks and implement the appropriate controls to mitigate them. Many regulatory and insurance requirements may mandate that organizations maintain an inventory of their assets. Failing to do so can result in non-compliance and potential penalties and fines. Having a complete and accurate inventory of assets enables organizations to quickly determine the extent of a security incident and respond appropriately. Having an inventory and control of assets helps organizations make informed decisions about resource allocation and prioritize the protection of their most critical and valuable assets. Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Having control over assets helps organizations monitor network activity and detect security threats, improving their overall security posture. In summary, having an inventory and control of enterprise assets (physical and software) is crucial for organizations to effectively manage risk, maintain compliance, and improve their overall security posture.

Controls Assessment

0.0 Unknown Question (ID: 4e256554...)

Control Status: FULLY IMPLEMENTED (1)   Impact: MODERATE (3)   Risk Score: 3 - LOW

Comments:

> Google sheet that we use to inventory devices. Notate MACs, SNs, and other details. We also manage them on the Google admin console for chromebooks

0.0 Unknown Question (ID: 42e46a89...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> RADIUS server for internal network auth

0.0 Unknown Question (ID: 49b1fdb8...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> Spreadsheet, Learn Platform also lists the software the org uses

0.0 Unknown Question (ID: 2ddff9d2...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Not currently

2.0

Account Management

67%

Overview

Account management is the practice of managing user accounts and their access to an organization's systems and data. This includes creating and deleting accounts, setting permissions and access levels, and regularly reviewing and updating account information. Cybersecurity best practices recommend implementing strong password policies, multi-factor authentication, and limiting access to only what is necessary for each user's job function. Regular monitoring and auditing of account activity can help detect and respond to potential security incidents.

Importance

Effective account management is critical for managing cybersecurity risks and preventing unauthorized access, as it limits access to only authorized users and reduces insider threats. By enforcing strong password policies, regularly reviewing account activity, and promptly detecting and responding to security incidents, organizations can enhance password security and mitigate the risk of potential security incidents. Additionally, effective account management enables organizations to comply with regulations and standards, avoiding costly fines and reputational damage. In summary, a good account management process is essential for maintaining the confidentiality, integrity, and availability of an organization's systems and data.

Controls Assessment

0.0 Unknown Question (ID: ddc56966...)

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 25 - HIGH

Comments:

> They have a separate login for the vpn, then another login for the network. No MFA currently

0.0 Unknown Question (ID: 8864a47a...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> MFA on Skyward on SIS. MFA enabled on admins as well.

0.0 Unknown Question (ID: c3d35793...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> MFA on Skyward for finance and SIS. SSO with CLever for staff members, which requires MFA.

0.0 Unknown Question (ID: e5c8fefc...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Spreadsheet where if a staff member is removed/resigned, IT people responsible for each building, flags them, notifies them, and disables them. Summer sweeps performed, and even over winter break. Bi Anually.

0.0 Unknown Question (ID: 52800943...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Spreadsheet where a new staff member gets added, IT alerted, accounts created. Team is alerted any time changed on that spreadsheet occur.

0.0 Unknown Question (ID: 21eb4c81...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Spreadsheet update where if a staff member is removed/resigned, IT people responsible for each building, flags them, notifies them, and disables them.

0.0 Unknown Question (ID: 75e0f1f6...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> Active Directory and Google Admin Console Segmentation between admins/users. Service accounts all have expirations.

0.0 Unknown Question (ID: 6ffb751c...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> 12+ , with upper, lower, special, and number. 60 day renewal.

0.0 Unknown Question (ID: d6b5984b...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> MFA for employees, Google

5.0

Data Protection

56%

Overview

> Data protection is the practice of protecting sensitive and confidential information from unauthorized access, use, or damage. This requires implementing technical, administrative, and physical controls to ensure the confidentiality, integrity, and availability of data. Effective data protection is essential for maintaining customer trust, complying with regulations and standards, and preventing data breaches. By implementing robust data protection measures, organizations can reduce the risk of cyber-attacks, data loss, or theft, and safeguard the continuity of their operations.

Importance

In today's distributed digital landscape, data is often stored beyond an enterprise's borders on the cloud, portable devices used for remote work, or shared with partners and online services across the world. As a result, protecting sensitive financial, intellectual property, and customer data is critical, especially given the many international regulations related to personal data. Effective data privacy management involves appropriate use and management of data throughout its entire lifecycle, not just encryption. Though privacy rules can be complex, fundamental principles apply to all multinational enterprises.

Controls Assessment

0.0 Unknown Question (ID: 5c1a240b...)

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> no

0.0 Unknown Question (ID: ee21191d...)

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 15 - MODERATE

Comments:

> No separation of accounts

0.0 Unknown Question (ID: b2a06977...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> BitLocker on all endpoints. On prem backups are encrypted w/ VEEAM Sophos running on servers EDR, and Sentinel 1 MDR

4.0

Secure Configuration of Enterprise Assets

95%

Overview

> Secure configuration of enterprise assets refers to the process of configuring devices such as firewalls, routers, servers, and laptops in a secure and standardized manner. This involves ensuring that default configurations are changed, unnecessary services are disabled, and software is patched and updated regularly. Effective secure configuration reduces the attack surface of an organization's systems and prevents many common security vulnerabilities.

Importance

Default configurations for enterprise assets and software are often geared towards ease-of-use, rather than security, and can include exploitable vulnerabilities. As a result, secure configuration updates must be managed and maintained throughout the lifecycle of enterprise assets and software. Effective secure configuration involves tracking and approving configuration updates through a formal workflow process to maintain a compliance record. Implementing secure configuration of enterprise assets is crucial for reducing the attack surface of an organization's systems and preventing many common security vulnerabilities. By configuring devices in a secure and standardized manner, organizations can enhance their security posture and reduce the risk of data breaches and other security incidents.

Controls Assessment

0.0 Unknown Question (ID: 71c04895...)

Control Status: FULLY IMPLEMENTED (1)   Impact: MODERATE (3)   Risk Score: 3 - LOW

Comments:

> Camera's on all entrances, and key card access to certain. IDF and MDF are secured by lock and key, with only IT team and custodian.

0.0 Unknown Question (ID: 00be77b9...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> Google admin console. and golden image for windows machines.

0.0 Unknown Question (ID: 9782ade0...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> On server side, they get patched monthly by vendor, Sentinel technologies

0.0 Unknown Question (ID: 0347bdfc...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Sentinel technologies handles all patching.

0.0 Unknown Question (ID: cfc6760b...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> we have configuration files, that we have backups from. Ruckus cloud config template, and firewall config templates. Switches hardened, and ports modified as needed.

0.0 Unknown Question (ID: ef9e6b1d...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> We get alerts for Sentinel devices. For Ruckus, we get alerts, and we perform updates.

0.0 Unknown Question (ID: b8a56435...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> CyberPools

0.0 Unknown Question (ID: 25922a65...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> Is set to 10 minutes, but staff can change this setting.

0.0 Unknown Question (ID: 6fa75575...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> 2 SSID's: D98 for student/staff, guest for anyone, 3rd for peripherals (IoT)

0.0 Unknown Question (ID: 02fb049d...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> NAC's in place to separate student/staff.

0.0 Unknown Question (ID: 7644e4a9...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> WPA2

0.0 Unknown Question (ID: 5c46e5bb...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> RADIUS used.

0.0 Unknown Question (ID: 7a360ec9...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> Preshared Key, changed annually

5.0

Malware Defense

83%

Overview

> Preventing the installation, spread, and execution of malicious software on enterprise assets is critical for malware defense. To achieve this goal, organizations need preventative controls such as antivirus software and DNS (Domain Name System) filtering, as well as detective controls like endpoint detection and response (EDR) tools. By monitoring endpoint activity, EDR tools can detect and respond to threats in real-time, reducing the risk of data breaches and reputational damage. Implementing a comprehensive malware defense strategy that includes preventative and detective controls can significantly enhance an organization's security posture.

Importance

Malware is an evolving and dangerous aspect of internet threats, which can have a range of purposes from stealing data to destroying it. Effective malware defense requires timely updates, automation, and integration with other processes like vulnerability management and incident response. Deploying malware defenses across all possible entry points and enterprise assets is crucial to detect, prevent, and control the execution of malicious software. By implementing robust malware defense measures, organizations can reduce the risk of cyber-attacks, data breaches, and reputational damage.

Controls Assessment

0.0 Unknown Question (ID: 5a80ba2c...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> DNS - FortiNet firewall has DNS filtering, and Ruckus also does filtering

0.0 Unknown Question (ID: 64577c3f...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Google Email Filter, GoGuardian

0.0 Unknown Question (ID: a7bdcd9b...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Sentinel One anti-malware

0.0 Unknown Question (ID: 9215cad3...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Sophos Intercept X on all endpoint

6.0

Data Recovery

25%

Overview

> Effective data recovery practices are crucial for protecting critical data and ensuring business continuity. Organizations should implement procedures to restore enterprise assets to a pre-incident state, including regularly backing up critical data, testing recovery processes, and implementing failover systems. By maintaining robust data recovery practices and incident response procedures, organizations can reduce the impact of security incidents and ensure compliance with regulations and standards.

Importance

Effective data recovery practices are essential for ensuring the continuity of business operations and protecting critical data. By establishing procedures to restore in-scope enterprise assets to a trusted state, organizations can reduce the impact of security incidents and minimize downtime. Additionally, maintaining robust data recovery practices helps organizations comply with regulations and standards, maintain customer trust, and protect their reputation.

Controls Assessment

0.0 Unknown Question (ID: feeab3b0...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Yes

0.0 Unknown Question (ID: ba30b5bc...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> Twice a week backups to VEEAM. on site storage on a NAS, not in cloud.

0.0 Unknown Question (ID: cd72f5cf...)

Control Status: PARTIALLY IMPLEMENTED (3) Impact: MODERATE (3) Risk Score: 15 - MODERATE

Comments:

> tabled for a response

0.0 Unknown Question (ID: e95173e9...)

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 25 - HIGH

Comments:

> Can't say we do it often.

7.0

Security Awareness

106%

Overview

> Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Importance

Cyber security awareness is essential for organizations to protect their systems, data, and reputation from cyber threats. By educating employees on cyber risks and best practices, organizations can reduce the risk of data breaches, malware infections, and other security incidents. Additionally, cyber security awareness helps to promote a culture of security within the organization, improving compliance with regulations and standards. Finally, cyber security awareness training can help organizations prepare for potential security incidents and respond effectively if they do occur, minimizing the impact on operations and reputation.

Controls Assessment

0.0 Unknown Question (ID: c57ac602...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> CyberPools phishing and training

0.0 Unknown Question (ID: 4d15f50e...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> Quarterly campaigns

0.0 Unknown Question (ID: acb6e426...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 1 - LOW

Comments:

> Follow up training to users based on their performance ont he assessment

8.0

Vendor Management

103%

Overview

> Develop and maintain process to evaluate vendors who hold sensitive data or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately. Additionally, there should be an emphasis placed on secure financial practices throughout the organization with respect to payment of vendors.

Importance

In today's connected world, enterprises rely on third-party vendors and partners to manage their data or supply critical infrastructure for core functions. However, third-party breaches can significantly affect an enterprise, compromising sensitive data or causing disruption to business operations. Third-party providers are attractive targets for cyber-attacks, as they often have access to multiple clients' networks. By effectively managing service providers, implementing strict security and financial controls, organizations can reduce the risk of third-party breaches and ensure the security of their systems and data.

Controls Assessment

0.0 Unknown Question (ID: 255e7396...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> SOPPA compliance for all vendors

0.0 Unknown Question (ID: bd3192a9...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 1 - LOW

Comments:

> We have a program called Learn platform, that allows us to house vendor information, and see usage.

0.0 Unknown Question (ID: 4f878db9...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> W-9s collected, and vendors only paid by check. W-9 verifies vendors. Any new/out of the ordinary requests, will get verified prior to fulfilling.

0.0 Unknown Question (ID: 0d554ad2...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> W-9s collected, and vendors only paid by check. W-9 verifies vendors. Any new/out of the ordinary requests, will get verified prior to fulfilling.

0.0 Unknown Question (ID: 7b903cea...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> W-9s collected, and vendors only paid by check. W-9 verifies vendors. Any new/out of the ordinary requests, will get verified prior to fulfilling.

9.0

Incident Response Management

73%

Overview

> Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Importance

Effective incident response is a critical component of a comprehensive cybersecurity program. By quickly identifying and responding to threats, organizations can prevent their spread and minimize the impact of security incidents. Incident response also plays a crucial role in understanding the full scope of an incident, identifying its root cause, and implementing measures to prevent future occurrences. Without effective incident response capabilities, organizations risk being stuck in a reactive pattern, constantly addressing symptoms rather than root causes.

Controls Assessment

0.0 Unknown Question (ID: 3fe16317...)

Control Status: PARTIALLY IMPLEMENTED (3) Impact: MODERATE (3) Risk Score: 9 - LOW

Comments:

> Partially started - almost finished

0.0 Unknown Question (ID: d626ce23...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> Responsibilities all established for all involved

0.0 Unknown Question (ID: 4c59c42f...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 1 - LOW

Comments:

> CISO - Gary and Tim

0.0 Unknown Question (ID: 349d6344...)

Control Status: PARTIALLY IMPLEMENTED (3) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> almost done

0.0 Unknown Question (ID: 66fb305d...)

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 15 - MODERATE

Comments:

> No testing yet.