Sienna Group

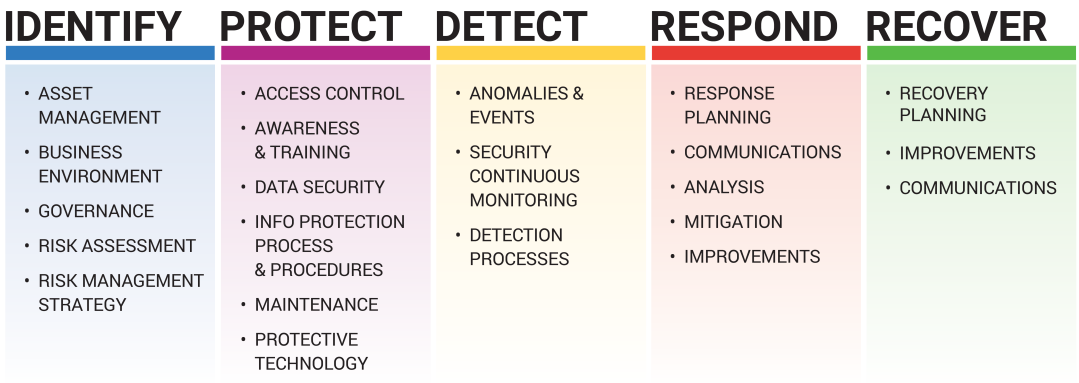
Sample Client Company

Risk Assessment Report
Completed On: 05 Nov 2018

Thank you for taking the time to respond to this NIST Security Risk Assessment. The goal of this assessment is to arrive at a quick sense of your strengths and weaknesses, and to provide advice as to what improvements you should be considering.

Your results have been measured against the National Institute of Standards and Technology (NIST) model regarding their cybersecurity for small business. This standard is referred to as the NIST CSF and is considered a best practice in the Security Industry.

The Standard measures five key areas to help you in understanding and safeguarding critical business information.



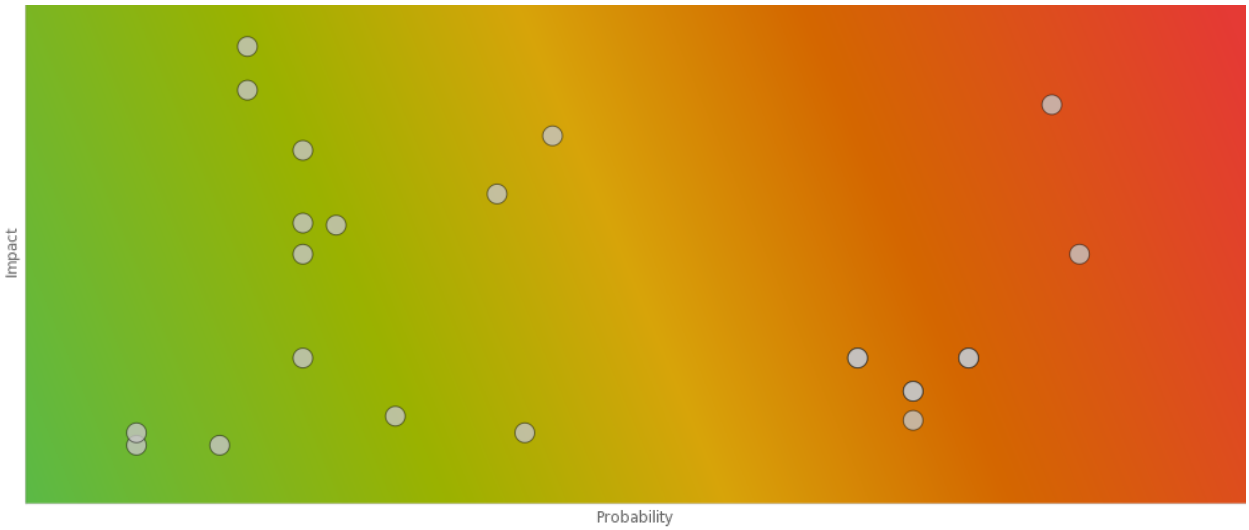
Your results will be measured against those of similar size as a metric of where your security practices align to the framework. The following link will take you directly to the NIST site where you can download the document for your own reference:

https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

OVERALL RISK ASSESSMENT

Your overall risk rating is **HIGH**

Your overall rating for this assessment raises some concerns as to your ability to detect and prevent threats that would negatively impact your organization. You should pay careful attention to the recommendations and remediate as many of the high risk items as you can.



TOP RISK AREAS

Critical	PR.AT-1 - All users are informed and trained
Critical	RC.RP-1 - Recovery plan is executed during or after an event
Critical	ID.RA-3 - Threats, both internal and external, are identified and documented
Critical	RS.RP-1 - Response plan is executed during or after an event
Critical	DE.CM-3 - Personnel activity is monitored to detect potential cybersecurity events
Critical	DE.AE-2 - Detected events are analyzed to understand attack targets and methods
Critical	DE.CM-1 - The network is monitored to detect potential cybersecurity events
High	ID.RA-2 - Threat and vulnerability information is received from information sharing forums and sources

High ID.RA-1 - Asset vulnerabilities are identified and documented

TOP RISK AREA RECOMMENDATIONS

PR.AT-1: All users are informed and trained — Critical

Q: Do you require Information Security training for your employees?

A: No

Importance:
It is essential to your business to ensure your employees are trained on the constantly changing security treats and how to avoid these threats.

Remediation Steps:
There are several on-line security awareness training company and sign your employees up for annual security awareness training.

RC.RP-1: Recovery plan is executed during or after an event — Critical

Q: Are recovery processes and procedures documented and reviewed?

A: No

Importance:
It is critical to businesses ability to respond to and recover from a security event and you don't have a process or plan to do so.

Remediation Steps:
Implement a recovery and process and procedure to allow your business to recover from a security incident. Make sure to include a plan to test the process and procedure at least annually and to update it with the lessons learned from the test.

Q: Are you planning on developing recovery processes and procedures?

A: No

ID.RA-3: Threats, both internal and external, are identified and documented — Critical

Q: Are potential impacts from third parties identified and documented?

A: No

Importance:
Some of the largest data breaches to date have come as a result of a third-party contractors inability to protect their environment. Practices should be in place to ensure you know your risk of doing business with external entities.

Remediation Steps:
You should immediately create an inventory of your vendors, review your contracts for obligations to protect your data, and perform a risk assessment across your inventory so that you can determine the risks to your business

RS.RP-1: Response plan is executed during or after an event — Critical

Q: Do you have incident response processes and procedures in place which are being maintained on a regular basis?

A: No

Importance:
It is critical to businesses ability to respond to and recover from a security event and you don't have a plan to do so.

Remediation Steps:
Create a business continuity and disaster recovery plan for your business. Work with a security consulting firm if you need assistance creating these plans.

Q: Are you planning on developing incident response processes and procedures?

A: No

Importance:
It is critical to businesses ability to respond to and recover from a security event and you don't have a plan to do so.

Remediation Steps:
Create a business continuity and disaster recovery plan for your business. Work with a security consulting firm if you need assistance creating these plans.

DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events — Critical

Q: Are you using an email filtering solution?

A: No

Importance:

Malware and other malicious software is most often spread through email. Unfiltered enterprise emails can be frustrating for both the administrators and your users.

Remediation Steps:
You should add an email filtering tool to your environment. The spam blocker or filter prevents unwanted emails from reaching your inbox and prevents any consequential harm to your business.

Q: Do you have web filtering or web site blocking set up?

A: No

Importance:
By not having web filtering you allow your employees to go to web sites which can potentially contain malicious software which can be downloaded and infect your environment.

Remediation Steps:
Implement a web filtering tool in your environment. Web filtering delivers many positive benefits for both organizations and end-users that go far beyond the basic implementation of preventing access to named websites or particular types of websites. The benefits and capabilities of web filtering are productivity, minimize liability, network and bandwidth management and data security.

DE.AE-2: Detected events are analyzed to understand attack targets and methods

Critical

Q: Do you have a threat detection product in place today?

A: No

Importance:
Not being able to detect threats with an automated threat detection system is a gap in your overall security posture.

Remediation Steps:
Implement a threat detection solution that can detect threats in real time. Perch Security is one that works well for companies your size

DE.CM-1: The network is monitored to detect potential cybersecurity events

Critical

Q: Do you scan your environment for rogue access points?

A: No

Importance:

Having access points within your environment which you don't know about can lead to vital business assess being stolen without your knowledge.

Remediation Steps:
You should scan your environment for rogue access points and remove them from your network.

Q: Are your monitoring your IT environment for anomalous events?

A: No

Importance:
Not being able to monitor and detect threats in your IT environment can lead to unnecessary downtime or security incidents.

Remediation Steps:
Implement a monitoring solution for detect and alert on anomalous behavior in your environment.

Q: Do you perform vulnerability scans in your environment?

A: No

Importance:
Not performing vulnerability scans in your environment can lead to undetected threats which can be exploited within your environment.

Remediation Steps:
Purchase a vulnerability scanning tool to implement regular vulnerability scans of your environment. Consider doing third-party vulnerability scans on a yearly basis.

ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources

High

Q: Do you receive threat intelligence information from sharing sources such as ISAC's?

A: No

Importance:
Leveraging Threat intelligence is important as you can gain vital information about your business sector thast would enable you to detect and defend against known attacks. You should find out for sure if you are receiving this important information. Not having this information is a significant gap

Remediation Steps:

Check with your security team to see if you are receiving threat intelligence information. If you are not receiving this information seek out an ISAC that aligns to your business model and leverage the available tools on the market to enable a threat intelligence capability for your company.

ID.RA-1: Asset vulnerabilities are identified and documented

High

Q: Does your organization have an internal process for assessing risk?

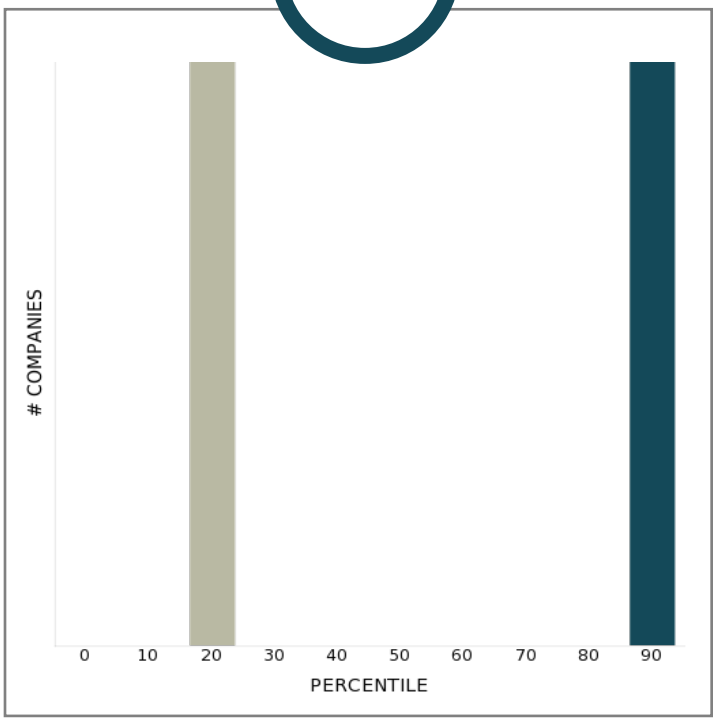
A: No

Importance:
Along with having security policies, a risk assessment is the most fundamental element to protecting your vital business assets. By not having one performed you are essentially blind to the risks and severity of the risks that can impact your business.

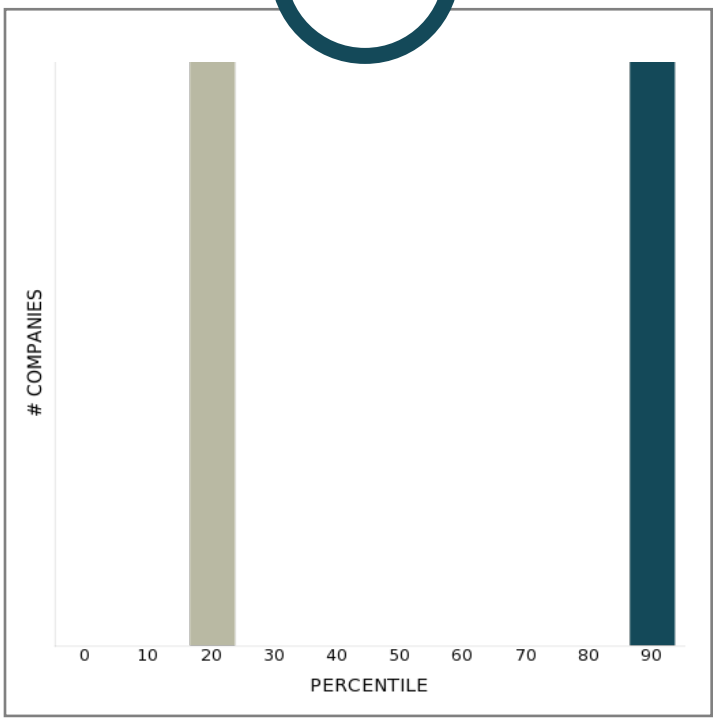
Remediation Steps:
Create a policy for performing periodic risk assessments, and work with a skilled professional to schedule an assessment.

INDUSTRY COMPARISONS

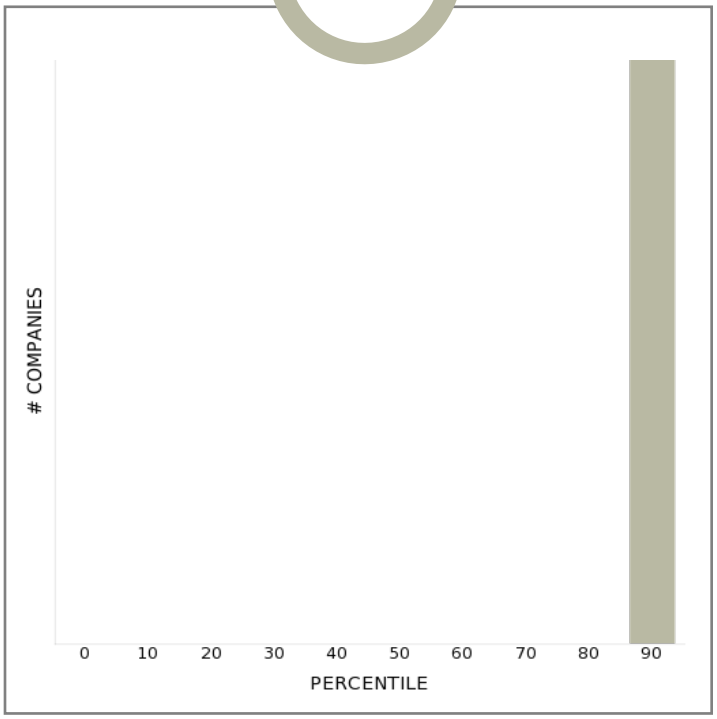
OVERALL 20TH PERCENTILE



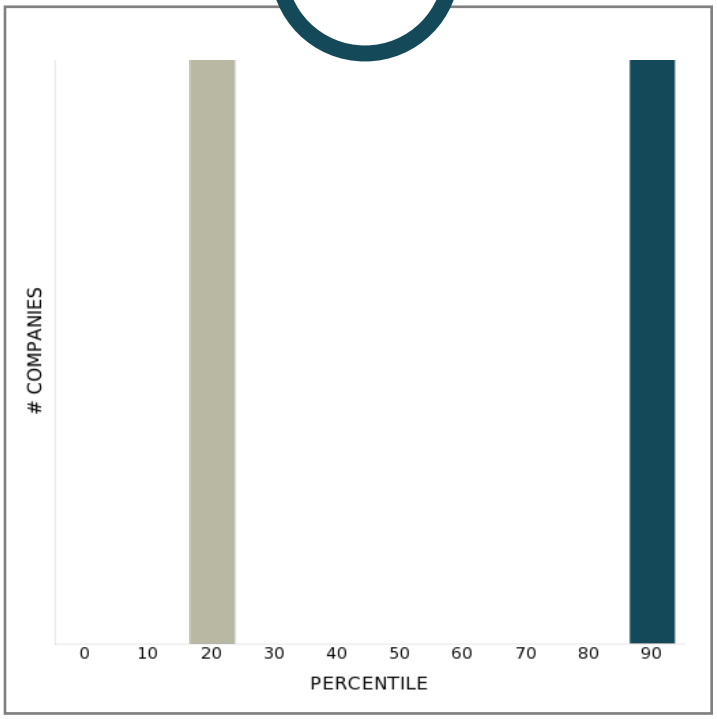
INDUSTRY 20TH PERCENTILE



COMPANY SIZE 90TH PERCENTILE



LOCATION 20TH PERCENTILE



APPENDIX / QUESTIONS

Q: Please enter your name.

> **A: John Tester**

Q: Please enter your email address.

> **A: tester@no-email.com**

Q: Please enter your company name.

> **A: Sample Client Account**

Q: Please enter your role in the organization.

> **A: Owner**

Q: Please select the industry of the company.

> **A: Financial Services**

Q: Please select the number of employees in the company.

> **A: 1-500**

Q: Where are you located?

> **A: United States**

Q: What best describes your annual revenue?

> **A: Up to $1M**

Q: Who manages your IT environment? (Choose all that apply)

> **A: MSP/ISP**

Q: Besides employees, who has access to your computer hardware? (Choose all that apply)

> **A: MSP/ISP**

APPENDIX / QUESTIONS

Q: Do you have a listing of all user accounts?

A: Yes

Q: Do any of your users have admin access?

A: Yes
Admin access allows users to install, delete, or modify applications and programs that may not be consistent with your business model

Remediation Steps:
Remove admin access, or limit the use of admin access for only those occasions where it is truly needed

Q: Do you have an inventory of devices such as printers, computers and scanners for your business?

A: No
Important business information as well as sensitive personal information could be stored on your IT devices. If you do not have an accurate inventory then these devices could be leveraged by people outside of your company for personal gain and damage to your business

Remediation Steps:
Implement an asset management process/product

Q: Is your physical office locked when vacant?

A: Yes

Q: How long before your computer screen is set to lock when not in use anytime you're away from your computer?

A: 15 minutes
It's good that you have configured your computers to lock automatically 15 minutes after non-use, best practice is to lock screens after 5 minutes of non-use.

Remediation Steps:
Implement an auto-lock feature for a set period of time no more than 5 minutes, and get into the practice of locking it manually consistent with the operating system that you are using

APPENDIX / QUESTIONS

Q: Do you perform background checks on your employees?

A: Yes

Q: How are background checks performed?

A: Only at new hire
Background checks should be performed on an annual basis as many items that may impact your business through an employees behavior may not be visible to you

Remediation Steps:
Update your policy, notify your employees, and perform background checks on an annual basis

Q: Are user credentials shared?

A: No

Q: Does your company have information security policies and procedures?

A: Yes

Q: Have your employees been made aware of your information security policies and procedures?

A: Yes

Q: Does your organization have an internal process for assessing risk?

A: No
Along with having security policies, a risk assessment is the most fundamental element to protecting your vital business assets. By not having one performed you are essentially blind to the risks and severity of the risks that can impact your business.

Remediation Steps:
Create a policy for performing periodic risk assessments, and work with a skilled professional to schedule an assessment.

APPENDIX / QUESTIONS

Q: Do you receive threat intelligence information from sharing sources such as ISAC's?

A: No

Leveraging Threat intelligence is important as you can gain vital information about your business sector thast would enable you to detect and defend against known attacks. You should find out for sure if you are receiving this important information. Not having this information is a significant gap

Remediation Steps:

Check with your security team to see if you are receiving threat intelligence information. If you are not receiving this information seek out an ISAC that aligns to your business model and leverage the available tools on the market to enable a threat intelligence capability for your company.

Q: Are potential impacts from third parties identified and documented?

A: No

Some of the largest data breaches to date have come as a result of a third-party contractors inability to protect their environment. Practices should be in place to ensure you know your risk of doing business with external entities.

Remediation Steps:

You should immediately create an inventory of your vendors, review your contracts for obligations to protect your data, and perform a risk assessment across your inventory so that you can determine the risks to your business

Q: Do you limit access to data for your employees?

A: Yes, employees only have access to data for their job role

Q: After termination, do you disable accounts?

A: Yes

APPENDIX / QUESTIONS

Q: How long after termination do you disable user accounts?

A: Within a week
User accounts of employees who are terminated or resign should be disabled immediately, waiting up to a week as you noted is too long. Work on a procedure to disable those accounts in a more timely manner.

Remediation Steps:
Create a policy and a process to monitor accounts and disable them as soon as possible but not later than 24 hours.

Q: Do you allow the use of USB ports?

A: Yes
Using USB ports can be useful for transferring files, doing backups and other routine operational procedures; however, they are an easy way for employees to copy and share confidential data that you would not want to be shared. They also pose a risk of introducing malware into your environment.

Remediation Steps:
Update or create a policy regarding restrictions of USB for business use. If you must allow them then you should have control over the inventory and not allow employees to use their own USB devices

Q: Do you provide surge protection to your computer systems?

A: Yes

Q: Do you keep up with the latest Critical Updates and Microsoft Windows updates?

A: Yes

Q: How are the updates completed?

A: Auto Updates

Q: Are all your software applications still supported by the manufacturer?

A: Yes

APPENDIX / QUESTIONS

Q: Do you keep software licensing agreements up to date?

> **A: Yes**

Q: Are you using a firewall between your internal network and the internet?

> **A: Yes**

Q: Who configures and manages your firewall? (Choose all that apply)

> **A: MSP/IT consultant**

Q: Have you changed the default password for your firewall?

> **A: Yes**

Q: Is your firewall set to log activity?

> **A: No**
> *Your firewall is designed to keep track of events such as failed login attempts, and events relating to the firewall rules that give you an indication if the rules are working or if you need additional items that are specific to your network. Not having this enabled means you do not have any insight as to the types of traffic or access attempts which can be harmful if your firewall is not properly configured*
>
> *Remediation Steps:*
> *You should configure your firewall to log activity as soon as you can, and establish a process to read the logs at reasonable intervals. Doing so can help you make valuable adjustments to your firewall settings*

Q: Are you using WiFi for your business?

> **A: Yes**

Q: Which authentication method do you use on your router?

> **A: WPA2 personal with AES encryption**

APPENDIX / QUESTIONS

Q: Have you changed the default administrative password on your wireless access device?

A: Yes

Q: How do you store/ protect the wireless access device password?

A: Remembered by one person
It's risky having a person remember your WiFi admin password. If they forget it you will have to reset your router to the default setting and lose any configurations you have made.

Remediation Steps:
There are password managers which give you the option to sync to multiple devices or keep them local only. Consider switching to one of these password managers instead of trying to remember all your passwords.

Q: Do you scan your environment for rogue access points?

A: No
Having access points within your environment which you don't know about can lead to vital business assess being stolen without your knowledge.

Remediation Steps:
You should scan your environment for rogue access points and remove them from your network.

Q: Are you using an email filtering solution?

A: No
Malware and other malicious software is most often spread through email. Unfiltered enterprise emails can be frustrating for both the administrators and your users.

Remediation Steps:
You should add an email filtering tool to your environment. The spam blocker or filter prevents unwanted emails from reaching your inbox and prevents any consequential harm to your business.

APPENDIX / QUESTIONS

Q: Do you have web filtering or web site blocking set up?

A: No
By not having web filtering you allow your employees to go to web sites which can potentially contain malicious software which can be downloaded and infect your environment.

Remediation Steps:
Implement a web filtering tool in your environment. Web filtering delivers many positive benefits for both organizations and end-users that go far beyond the basic implementation of preventing access to named websites or particular types of websites. The benefits and capabilities of web filtering are productivity, minimize liability, network and bandwidth management and data security.

Q: How are old equipment and data storage devices handled before disposal?

A: Old equipment is disposed of
Disposing of old equipment is good, but you need to make sure you remove all data before doing so.

Remediation Steps:
Implement a practice to remove data from old equipment before disposing of the equipment. The drives should be wiped of data using at least 3 passes of deletion. Reference these DoD standards for media sanitation https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Q: How are hard copy documents handled before disposal?

A: Documents are shredded in house then thrown away

Q: Do you require Information Security training for your employees?

A: No
It is essential to your business to ensure your employees are trained on the constantly changing security treats and how to avoid these threats.

Remediation Steps:
There are several on-line security awareness training company and sign your employees up for annual security awareness training.

APPENDIX / QUESTIONS

Q: Do you have a threat detection product in place today?

A: No
Not being able to detect threats with an automated threat detection system is a gap in your overall security posture.

Remediation Steps:
Implement a threat detection solution that can detect threats in real time. Perch Security is one that works well for companies your size

Q: Are your monitoring your IT environment for anomalous events?

A: No
Not being able to monitor and detect threats in your IT environment can lead to unnecessary downtime or security incidents.

Remediation Steps:
Implement a monitoring solution for detect and alert on anomalous behavior in your environment.

Q: Do you perform vulnerability scans in your environment?

A: No
Not performing vulnerability scans in your environment can lead to undetected threats which can be exploited within your environment.

Remediation Steps:
Purchase a vulnerability scanning tool to implement regular vulnerability scans of your environment. Consider doing third-party vulnerability scans on a yearly basis.

Q: Do you have incident response processes and procedures in place which are being maintained on a regular basis?

A: No
It is critical to businesses ability to respond to and recover from a security event and you don't have a plan to do so.

Remediation Steps:
Create a business continuity and disaster recovery plan for your business. Work with a security consulting firm if you need assistance creating these plans.

APPENDIX / QUESTIONS

Q: Are you planning on developing incident response processes and procedures?

A: No
It is critical to businesses ability to respond to and recover from a security event and you don't have a plan to do so.

Remediation Steps:
Create a business continuity and disaster recovery plan for your business. Work with a security consulting firm if you need assistance creating these plans.

Q: Are recovery processes and procedures documented and reviewed?

A: No
It is critical to businesses ability to respond to and recover from a security event and you don't have a process or plan to do so.

Remediation Steps:
Implement a recovery and process and procedure to allow your business to recover from a security incident. Make sure to include a plan to test the process and procedure at least annually and to update it with the lessons learned from the test.

Q: Are you planning on developing recovery processes and procedures?

A: No

ATTESTATION LETTER

Customer Name: Sample Client Company ("Customer")
Managed Service Provider: Sienna Group CW Test Account ("MSP")

Date: _____

The above-named MSP has recommended a specific course of action to the Customer to help improve the Customer's overall security posture (the "Report") and the Customer acknowledges it has been provided and has reviewed the Report. The Report provides a prioritized description of the risks to the Customer as aligned with the NIST Cybersecurity Framework (NIST CSF), which is considered a best-practices approach to follow. The recommendations contained within the Report represent the Customer's best interests and requires careful consideration.

The specific recommendation(s) being made by the MSP include the following:

_____

_____

_____

Given that the Customer has elected not to follow the recommendations of the MSP as noted above and as outlined within the Report, the Customer accepts the risks outlined in the Report and releases the MSP from any responsibility resulting from incidents related to such risks. The risks of not following the recommendations of the MSP have been fully explained to the Customer by the MSP. The Customer agrees that the MSP shall not be held responsible or legally liable for the decision or any future consequences of the Customer’s decision.

By signing below the Customer acknowledges that it has read this information and has elected not to follow the MSP's recommendations.

AGREED AND ACCEPTED:

SAMPLE CLIENT COMPANY

BY: _____

ITS: _____

DATE: _____