GROVE TECHNOLOGIES

WHITE PAPER 2021

Cybersecurity Risk Assessments For Small Businesses

Consultants Network

WELCOME

About

We work with clients big and small across a range of sectors and we utilize our resources to ensure that your problems are handled with care. We believe that analysis of your company and its systems is key in responding effectively to your systematic needs and we will work with you to fully understand your business tech needs to achieve the greatest amount of success as possible so that you can see a true value from your tech investment.

We have a number of different teams within our agency that specialize in different areas of business so you can be sure that you won't receive a generic service and although we can't boast years and years of service we can ensure you that is a good thing in this industry. Our teams are up to date with the latest technologies, media trends and are keen to prove themselves in this industry and that's what you want from an technology agency, not someone who is relying on the same way of doing things that worked 10 years, 5 years or even a year ago.

Whatever the level of support you require, we are sure that we will have a package that meets your needs. All of our virtual professionals are highly experienced in the areas in which they work and have been through a thorough recruitment process to ensure they deliver to the high standard that you would want for your business.

We will work with you to fully understand your business and your technology needs and digital strategy. Using the outcomes from the Technology Analysis, we will put together a plan for the most effective technology strategy to get the best results for your business

TABLE OF

Contents

Everything a small business owner needs to know about traversing the cybersecurity space in search of compliance.

CYBERSECURITY

Why is a risk assessment so important?

A cyber security risk assessment is a critical activity performed on your company's security policy procedures and infrastructure to reveal potential threats to key corporate assets and vulnerabilities in your current security controls as implemented.

100%

What is the goal of a risk assessment?

The goal of a security risk assessment is to define the appropriate safeguards that your company will need to implement in order to align to your company's risk assessment objective, profile, and priorities.

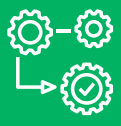
An organization faces many types of threats and risks that can impact its overall cybersecurity posture. While many organizations think of risks in terms of things, they understand such as natural disasters insider threats, the majority of risks faced by an organization are based on a combination of logical and technical controls on key assets and systems not being implemented or hardened to a level of security needed. In the evolving cybersecurity landscape, threats that may not have existed a few years ago or their impact have increased significantly.

This can lead to increasing vulnerabilities that an organization may not be aware of or have gaps in their current cybersecurity posture as implemented. Ransomware, for example, is an evolving and highly impactful cybersecurity threat that requires a complex combination of logical, technical, and policy-based controls that need to be carefully implemented to reduce this overall risk. Organizations might find that they have not implemented adequate controls to reduce this risk.

They might still be vulnerable without the proper cybersecurity professionals reviewing their security posture to help determine gaps in their implementation.

Another major factor for an organization to have a security risk assessment performed is in order to achieve a cybersecurity compliance certification that is required by a customer or a specific contract. In many cases, an organization is motivated to pursue a cybersecurity certification such as SOC 2 or ISO 27001 in order to win new work or a new customer mandates they have it in place prior to performing the work or accepting the contract.

This is often part of a third-party supply chain risk requirement that certifies your organization's level of attestation that certain cybersecurity controls are implemented, and this baseline is maintained as part of their ongoing compliance work. A security risk assessment can provide you with an independent review your cybersecurity posture to see where your risks are and help you address specific risk concerns that your organization might have.



"Their responsiveness is second to none and they clearly take pride in the service that they provide. I can recommend this business with full confidence and look forward to continuing our partnership."

-- Eleven Peppers Sudios

Always work with a trusted partner.

Expertise matters when it comes to performing a risk assessment. Always work witha certified consultant and use a framework that is trusted and verified.

A key aspect of having a security risk assessment performed is to understand how your budget should be allocated for future security spending on a security controls to maintain your baseline. It is often said no amount of money can solve all of your cybersecurity issues and this is especially true with the diverse issue's companies face such as hackers, malicious threats, phishing, data integrity, etc.

If companies have a budget do, they really know where the money is going for the return of investment on the implemented cyber security controls to reduce the overall risk? Should money be allocated for higher priority actions that would have a greater impact on the overall baseline then other key areas for future spend?

A security risk assessment will help provide an organization a plan to determine future budget allocation for comprehensive controls that can meet or exceed the cybersecurity baseline they need to align to.

Certain security frameworks are more complex or rigorous than others which will subsequently increase the size and scope that is required.

Typically, the price will vary by the risk assessment objectives for the size of your organization and the types of security tests to be performed for the security risk assessment.

Compliance level objectives such as meeting higher attestation requirements as well for a larger organization can increase the project complexity and price.

Often times organizations may only want to have a subset of controls be assessed that they might not have the expertise in house in order to perform or understand the requirements.

Correctly sizing the risk assessment service to your company will ensure that they are in tune with your size and type of business which our vCISO will perform when having the initial kickoff call to determine the best objectives and needs of your organization.

Quality

How much will a risk assessment cost?

The cost of a security risk assessment depends on the scope and complexity of the project itself. There is no monolithic price structure for a defined risk assessment.

The size and the scope will have to be defined as well as the security framework to which the assessment will occur against.

Cost Effective Solutions
Our innovatave approach to Risk Assessments saves you money by targeting the systems you need to harden on day one. Our risk assessment will give you the tools you need at a fraction of the cost of the other guys.

EC-Council
E|HA
ETHICAL HACKING ASSOCIATE

CYBERSECURITY

How Long Will It Take?

The time frame to complete a security risk assessment again depends on several organizational specific factors.

A more complex assessment will inevitably take a longer amount of time because the attestation level for security controls that must be tested are increased. A full NIST 800-53 compliance assessment may have between 100-400 unique controls that have to be assessed against an organization based on the classification rating and scope.

Another crucial factor is the responsiveness and readiness of your organization for the security assessment. To achieve the best results and have the greatest level of communication with our vCISO, it is recommended that all available documentation and personnel resources be available for interviews or follow ups as needed during the risk assessment process.

Typically, most risk assessments take three to five weeks to perform with dedicated resources available from the organization.

We try to minimize the gap analysis time by having the organization provide us with as many documents as we can up front in order for us to get started.

A security risk assessment performed by a third-party organization such as Grove can allow a company to help determine what you need to increase your compliance for various control requirements.

Trust our team of experts to help provide a cybersecurity roadmap, guide and plan.

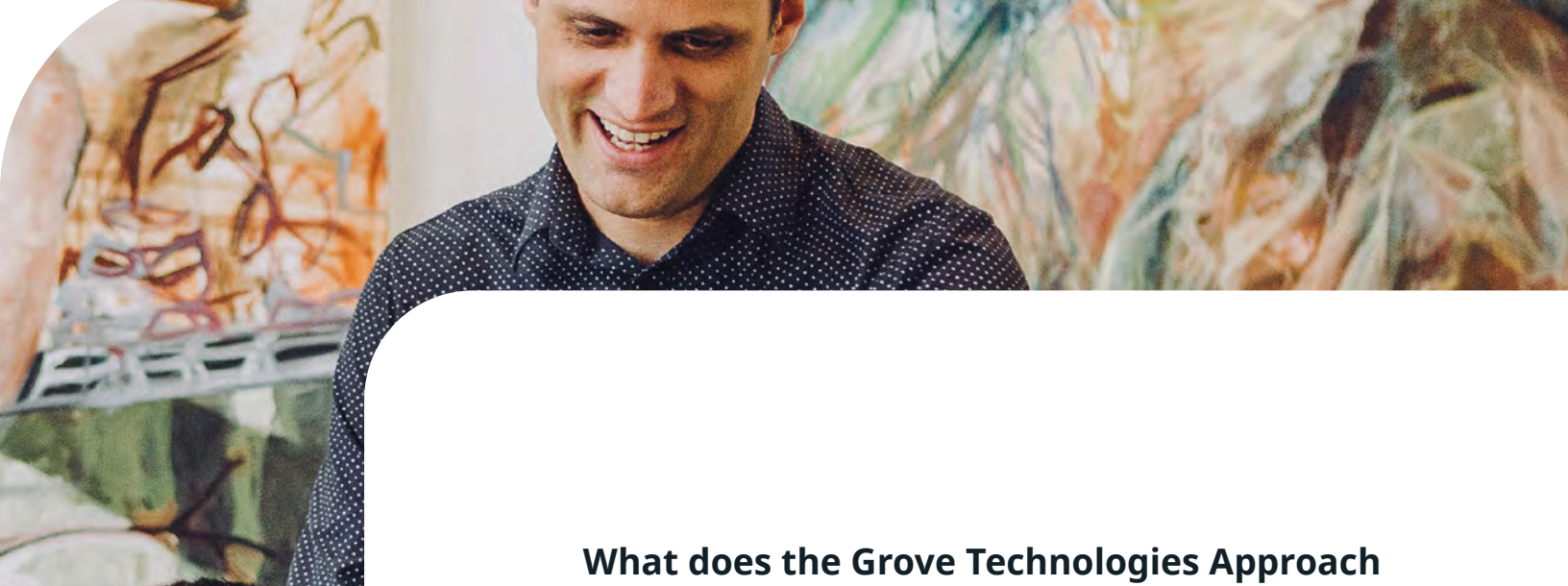
What is the entire risk assessment process look like?

Our security risk assessment process begins with a thorough gap analysis of your overall organizational posture.

Our vCISO will review your existing policies and procedures as well as any other supporting documentation to determine potential gaps or areas that need to be addressed against your target cyber security framework.

The gap analysis process includes reviewing artifacts and interviewing key personnel that oversee cybersecurity controls for your organization to determine their procedure as aligned to any documented processes that are implemented.

The vCISO will carefully go through all of the controls with the provided documentation and using their expertise and understanding of the control requirement determine the level of compliance for that control requirement. To keep things understandable for a wide target audience, the vCISO will mark a control as either compliant, not compliant, or partially meets



What does the Grove Technologies Approach Mean to your small business?

requirements to simplify remediation efforts that might be required. If the control is compliant, then the organization has sufficiently met or exceeded the requirements stated to be implemented.

If the control is not compliant the organization has not implemented whatsoever any of the control requirements as required.

> Their expertise and dedication to service excellence is second to none. Grove Technologies has been an integral part of our IT Departments success and they are a valued asset to our organization. -- Food & Water Watch

Finally, if the control is considered meeting partial requirements, then there will be gaps identified in that control implementation. If a control is not implemented or gaps are identified by the vCISO, then they will provide to the client recommended steps to either implement or close the gap to be compliant for those controls.

These controls cover a multitude of areas including identity access management, encryption, audit and logging, configuration management, and secure communication to name a few.

By utilizing a gap analysis combined with a remediation plan, an organization has a blueprint in order to start closing the gaps or increasing their overall cyber security baseline based on the findings the vCISO is recommending.

and any questions that might arise. Our team is dedicated to ensuring a quality risk assessment report is being delivered

CYBERSECURITY

What should I do after receiving the security assessment results?

After the vCISO delivers the risk assessment report and remediation plan, they will have a review session with your organizational leadership and technical liaisons to go over findings

as well as any questions no matter how big or small are answered to your satisfaction. The remediation report will categorize findings based on a high, moderate, or low scale.

The organization should consider implementing the highest impact issues first based on budget, complexity, and fastest increase to the overall cyber security baseline as well as personnel available. Grove offers additional consulting services including vCISO services to help your organization address and implement any of the remaining findings or questions that might arise after the assessment occurs.

Grove also offers security engineering services to do the implementation where applicable for organization of the remediation findings or work with your managed service provider in ensuring these things are done in a timely fashion.

How do I get started?

Still have additional questions about the risk assessment process? Schedule an appointment with us today! Our Grove vCISO have the expertise and knowledge to support a wide range of various security compliance requirements that will be tailored and scoped to your organization to provide the best return on investment in order to maximize your cyber security baseline for your intended compliance framework.

Compliance Advisors

We know what it takes to ensure your policies and procedures are compliant to various cybersecurity requirements frameworks (SOC2, NIST, HIPAA, PCI DSS, etc.). We design and develop BCDR policies and procedures tailored to your organization.

Awareness Training

Your business is only as good as the people that work there. Its time to train your employees the right way with our security awareness program.

With next generation analysis of key security metrics to rank your employees by their associated risk level with our Employee Vulnerability Assessment.

CALL US (888) 253-9103

Risk Assessments

Most companies aren't fully covered in either security or compliance, and they are generally unaware of the many vulnerabilities that need to be protected.

Complete Visibility

This vital assessment gives you complete visibility into your entire network and data to reveal vulnerabilities and gaps that need to be addressed.

Cutomized Plan

What emerges from the thorough risk assessment is the Executive Summary, an invaluable blueprint that we will use to target, prioritize, and address trouble areas.

Policy Portal

We have developed a fully managed streamlined service, which provides a portal that takes you through a simple step by step compliance and best practices process.

Control Frameworks

Control frameworks can be highly challenging and expensive to implement. In addition, it is costly and time consuming to train your staff and keep up with the volume of change controls.

Lowering Costs

When you partner with a qualified cybersecurity company you will lower your risk exposure but also your costs in terms of getting up to speed on compliance.

Your Cybersecurity Team

Jon Brown
CEO & CMMC RP
jon@grovetech.co

Jon is a charismatic leader, entrepreneur, teacher & mentor who helps businesses take their Mac, Cybersecurity & Networks to the next level.

Scott Campbell
CISO, CCSP, CMMC RP
scott@grovetech.co

20 years of experience in providing executive consulting for cybersecurity and IT clients needs in a vCISO role for compliance, CMMC and more.

Michael Tedesco
CISO, CISSP
michael@grovetech.co

With a background in the US Coast Guard, Michael helps the needs of our Government companies stay within the boundaries of compliance.

CISSP® Certified Information Systems Security Professional

CCSP® Certified Cloud Security Professiona

Consultants Network

Our Office:

1030 15th St NW Suite 1050w,
Washington, DC 20005

E-mail and Web:

support@grovetech.co
www.grovetech.co

Phone:

+862-251-8712
+240-451-8688