SOLUTIONS3

CYBER ESSENTIALS

FINDINGS & RECOMMENDATIONS

ADDRESS
637 Wyckoff Avenue
PMB 352
Wyckoff, NJ 07481
201.891.0477

PREPARED FOR:
Solutions3
PREPARED BY:

Revision: 1.0
Assessment Date: 8/1/2024
Submission Date: 8/10/2024

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

PROPRIETARY NOTICE

Protection and Use of Company Confidential Information

The information contained in this Cyber Essentials assessment constitutes intellectual property, trade secrets, and/or information considered confidential and proprietary.

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

TABLE OF CONTENTS

Proprietary Notice ii
Table of Contents iii
Registered Trademarks & Acronyms v
1.1 Registered Trademarks v
1.2 Acronyms – vi
1. Executive Overview 7
1.1 Introduction 7
1.2 Approach and Methodology 7
1.3 Assessment Value 8
1.4 Importance of Cyber Resilience 8
1.5 Creating a Culture of Risk Awareness 9
1.6 Importance of Executive Sponsorship 9
1.7 Roadmap to Compliance 9
1.8 Closing Remarks 10
2. Assessment Approach 12
2.1 Overview 12
2.2 Strategic Objectives 12
2.3 Current State Assessment 12
2.4 Path to Desired State 13
3. CYBER ESSENTIALS Overview 14
3.1 Introduction 14
3.2 Critical Security Controls v8 Description 14
3.3 Key Characteristics of CYBER ESSENTIALS 14
3.4 The CYBER ESSENTIALS 14
3.5 Value of Implementing CYBER ESSENTIALS 16
3.6 Conclusion 17
4. Current State Definition 18

4.1 Capability Maturity Scoring Key 18
4.2 Maturity Rating Table and Spider Diagram Overview 18
4.3 Sample Maturity Ranking Table and Spider Diagram 19
5. CYBER ESSENTIALS Current State Findings 20
5.0 Overall CYBER ESSENTIALS Current State Diagram 20
5.1 Data Protection 21
6. Formal Recommendations 38
6.1 Overall Recommendations 38
6.2 Overall Benefits 38
7. Executive Summary 39

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

REGISTERED TRADEMARKS & ACRONYMS

REGISTERED TRADEMARKS

ACRONYMS

CISA	Cybersecurity and Infrastructure Security Agency	ITSM	IT Service Management
CPD	Create-Protect-Deliver (Digital Business/Mission Value)		
CSI	Continual Security Improvement	NIST	National Institute of Standards and Technology
CSM	Cyber Security Management	NIST-CSF	NIST Cybersecurity Framework
DVMS	Digital Value Management System	NIST-RMF	NIST Risk Management Framework
DHS	Department of Homeland Security	POA&M	Plan of Action & Milestones
GRC	Governance, Risk Management, and Compliance	SSP	System Security Plan
IRP	Incident Response Plan	SME	Subject Matter Expert
ITIL®	IT Infrastructure Library®	VILT	Virtual Instructor Led Training
ITOM	IT Operations Management	VDI	Virtual Desktop Infrastructure

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

1. EXECUTIVE OVERVIEW

INTRODUCTION

The Solutions³ LLC team was asked to assist Solutions3 with a Cyber Essentials assessment based on the CYBER ESSENTIALS industry-recognized framework.

The Cyber Essentials framework is a comprehensive approach to cybersecurity developed by the Cybersecurity and Infrastructure Security Agency (CISA) to help organizations, particularly small businesses and local government agencies, implement essential cybersecurity practices. This framework breaks down complex cybersecurity concepts into manageable, actionable steps that can be understood and implemented by both IT staff and leadership. The Cyber Essentials toolkit is structured around six key domains: Yourself (The Leader), Your Staff (The Users), Your Systems, Your Surroundings, Your Data, and Your Crisis Response. Each domain focuses on specific aspects of cybersecurity, from driving strategy and culture to protecting data and responding to incidents. The framework emphasizes the importance of viewing cybersecurity as a business risk and integrating it into overall business strategy. By providing practical guidance, resources, and tools, the Cyber Essentials framework aims to create a culture of cyber readiness and improve an organization's overall cybersecurity posture, helping to protect against common cyber threats and vulnerabilities.

APPROACH AND METHODOLOGY

In today's rapidly evolving cyber threat landscape, maintaining robust security measures is not just a necessity but a strategic imperative. Our organization embarked on a comprehensive CYBER ESSENTIALS assessment to evaluate your current cybersecurity posture against the specific framework or approved industry standard. This assessment was conducted methodically, covering each of the controls and their associated safeguards or objectives, to identify areas of strength and opportunities for improvement.

Our approach was systematic and thorough:

1. **Scoping**: We defined the scope of the assessment, identifying critical assets, data flows, and business processes.
2. **Survey**: Primarily through interviews, recommended documentation, and industry recommended maturity ranking guidelines, we gathered enough relevant information on current security practices to gain valuable insight into IT & Cybersecurity operations at SOLUTIONS3.
3. **Analysis**: We compared existing practices against the recommended CYBER ESSENTIALS controls, highlighting gaps and potential vulnerabilities.

4. **Assessment**: The Solutions³ CYBER ESSENTIALS team evaluated the current capabilities, functionality, and required documentation for gaps in alignment with the formal control objectives or safeguards.
5. **Remediation**: The Solutions³ CYBER ESSENTIALS team developed an actionable list of recommendations to address identified gaps, aligned with best practices and organizational goals.

ASSESSMENT VALUE

The CYBER ESSENTIALS Assessment provides significant value to the SOLUTIONS3 organization:

- **Enhanced Security Posture**: By identifying and addressing security gaps, you enhance your defenses against cyber threats. This proactive stance ensures that you are not only compliant with current standards but also prepared for emerging threats.
- **Compliance Readiness**: Aligning with CYBER ESSENTIALS controls positions SOLUTIONS3 well for regulatory compliance and industry certifications, ensuring you can meet and/or exceed the requirements of SOLUTIONS3 clients and regulatory bodies.
- **Risk Reduction**: Prioritized recommendations help mitigate the most critical risks to your business operations. This includes protecting digital assets, safeguarding sensitive information, and ensuring business continuity.
- **Strategic Insights**: The assessment provides a clear roadmap for improving your cybersecurity framework and ensuring long-term resilience. It highlights areas where the SOLUTIONS3 organization can invest to maximize your security ROI.

IMPORTANCE OF CYBER RESILIENCE

Cyber resilience is the ability to prepare for, respond to, and recover from cyber-attacks. This assessment underscores the importance of building cyber resilience within the SOLUTIONS3:

- **Protection of Digital Assets**: SOLUTIONS3's digital assets are the lifeblood of your business. Protecting these assets from unauthorized access, data breaches, and other cyber threats is paramount. This assessment helps you understand your vulnerabilities and implement measures to safeguard these critical resources.
- **Continuous Improvement**: Cyber threats are constantly evolving. Our approach emphasizes the need for continuous monitoring, regular updates to your security measures, and staying ahead of potential threats.

CREATING A CULTURE OF RISK AWARENESS

A robust cybersecurity framework is built on a foundation of risk awareness. Creating a culture of risk awareness within our organization involves:

- **Executive Leadership**: Executive leadership is crucial in driving this culture change. Leaders must advocate for cybersecurity, allocate necessary resources, and lead by example.
- **Employee Engagement**: Engaging employees at all levels to understand the importance of cybersecurity and their role in maintaining it. Regular training and awareness programs are essential.

IMPORTANCE OF EXECUTIVE SPONSORSHIP

The success of this initiative and the recommended remediation hinges on strong executive sponsorship. Without it, the hopes of success are slim to none. Executive leadership plays a critical role in:

- **Driving Cultural Change**: Promoting a culture of security and risk awareness across the organization starts from the top. Leaders must be visible advocates for cybersecurity, emphasizing its importance in every aspect of the business.
- **Allocating Resources**: Ensuring the availability of necessary funding for software tools, training programs, and professional services. Investment in these areas is crucial for building a robust cybersecurity posture.
- **Empowering Teams**: Providing the authority and support needed for teams to implement security improvements effectively. This includes backing security initiatives and supporting teams during the training and implementation phase.

ROADMAP TO COMPLIANCE

Implementing the recommendations from this assessment requires a coordinated effort and adequate resources. Key components of this roadmap include:

- **Adopting a Culture of Continual Improvement**: Establishing a methodology for continuous improvement in SOLUTIONS3 cybersecurity practices. This includes regular assessments, feedback loops, and iterative enhancements to our security measures. By fostering a culture of continual improvement, you will ensure that your defenses evolve in response to new threats and vulnerabilities.
- **Defined Policies & Practices**: Developing and maintaining comprehensive, well-defined policies that govern your cybersecurity practices. This includes clear documentation and regular policy reviews to ensure our practices remain current and

effective. Well-defined policies provide a solid foundation for consistent and effective security measures.

- **Effective Governance**: Implementing strong governance frameworks to oversee SOLUTIONS3 cybersecurity efforts. This includes establishing accountability, monitoring compliance, and ensuring adherence to established protocols. Effective governance ensures that your cybersecurity practices are consistently applied and aligned with our organizational goals and regulatory requirements.
- **Investment in Technology**: Procuring advanced security tools to enhance your detection, prevention, and response capabilities. These tools are essential for maintaining a strong security posture.
- **Ongoing Training**: Implementing a robust and structured cybersecurity training program is vital. This includes:
  - **Cybersecurity Awareness Training**: Regular programs to educate all employees about the latest cyber threats, safe practices, and their role in maintaining security.
  - **Cybersecurity and IT Skills Training**: Advanced training for IT and security professionals to enhance their technical skills and stay updated with the latest tools and techniques.
  - **Cybersecurity Business Training**: Specialized training programs, such as those offered by the DVMS Institute®, to understand the strategic importance of cybersecurity in business operations and digital value management.
- **Professional Services**: Engaging with cybersecurity experts to assist in implementing complex solutions and conducting periodic reviews. Expert guidance ensures that we are following best practices and effectively addressing our security needs.

Executive support and corporate backing are essential to ensure these components are effectively integrated into the SOLUTIONS3 cybersecurity strategy. By committing to a RoadMap to Compliance, SOLUTIONS3 not only improves their security posture but also safeguards your business, customers, and stakeholders from potential cyber threats.

CLOSING REMARKS

We extend our sincere gratitude to all stakeholders, sponsors and team members involved in this assessment. Your dedication and collaboration have been instrumental in identifying your cybersecurity strengths and areas for improvement. As we move forward with implementing the recommendations, your continued support and commitment will be crucial to our success.

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

Together, we can build a resilient, secure, and future-ready organization. Thank you for your unwavering commitment to safeguarding your digital assets and supporting the journey towards comprehensive cybersecurity compliance.

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

3. ASSESSMENT APPROACH

OVERVIEW

The Solutions³ LLC CYBER ESSENTIALS team implemented a strategic approach designed to achieve rapid improvements in the current cybersecurity posture while laying the groundwork for attaining the desired future state. Our approach leverages industry best practices and generally accepted methodologies to enhance the effectiveness and efficiency of current cybersecurity capabilities.

STRATEGIC OBJECTIVES

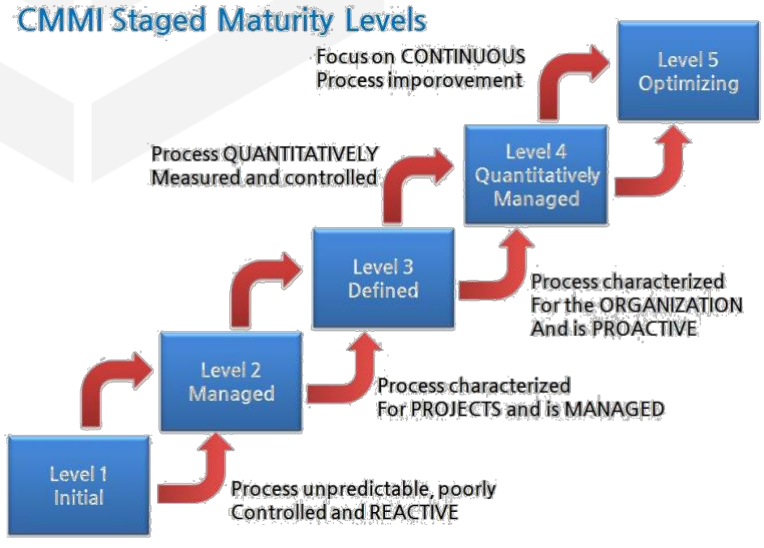
Our strategy was centered on assisting the SOLUTIONS3 team in advancing from their current maturity levels to higher levels on the cybersecurity maturity curve. The goal is not necessarily to achieve a Level 5 – Optimized status in all service areas, but to reach the maturity level that best aligns with SOLUTIONS3's overall business objectives and requirements.

CURRENT STATE ASSESSMENT

Initial discussions indicate SOLUTIONS3 is currently positioned at various stages within the following maturity levels:

- **Level 1 (Initial)**: Processes are Ad Hoc and Chaotic. The SOLUTIONS3 team has basic cybersecurity measures in place but lacks structured processes and formal documentation.
- **Level 2 (Managed)**: Processes are planned and executed according to policy. The SOLUTIONS3 team has some documented processes, but they are not standardized or consistently followed.

Our primary objective is to elevate SOLUTIONS3 from Levels 1 and 2 to the following:



- **Level 3 (Defined)**: Processes are well-documented, standardized, and integrated into a cohesive framework. This level brings about the needed stability and effectiveness, ensuring that cybersecurity practices are consistently applied across the organization.
- **Level 4 (Quantitatively Managed)**: Processes are measured and controlled. The **Error! Unknown document property name.** team will focus on improved efficiencies, using metrics and KPIs to manage and optimize cybersecurity processes.

The long-term goal would be to reach Level 5 in key areas that most benefit and align with the business and strategic objectives of the overall SOLUTIONS3 organization.

- **Level 5 (Optimized)**: Continuous process improvement is enabled by quantitative feedback and from piloting innovative ideas and technologies. While not the ultimate goal in all areas, achieving optimization in key areas will ensure SOLUTIONS3 is resilient and adaptive to new challenges.

PATH TO DESIRED STATE

Our long-term strategy envisions SOLUTIONS3 team achieving a state of Continuous Security Improvement (CSI). This continuous improvement mindset is integral to maintaining a robust cybersecurity posture and adapting to evolving threats. By executing on the recommendations provided in this RoadMap to Compliance assessment, the SOLUTIONS3 team has taken a significant toward the path to Desired State.

Key components of this path include:

- **Strategic Planning**: Developing and updating strategic plans to address identified gaps and enhance security measures.
- **Assessment and Analysis**: Regular assessments to identify vulnerabilities and areas for improvement.
- **Implementation and Integration**: Implementing security solutions and integrating them into existing processes and systems.
- **Monitoring and Metrics**: Continuous monitoring of security measures and using metrics to gauge effectiveness and drive improvements.
- **Review and Adaptation**: Periodic reviews of the cybersecurity framework to adapt to new threats and changes in the business environment.

Achieving this desired state is a gradual process, requiring sustained efforts and a commitment to long-term strategic goals. By adhering to this approach, we aim to fortify SOLUTIONS3' cybersecurity posture, ensuring resilience, stability, and efficiency in their cybersecurity operations.

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

4. CYBER ESSENTIALS OVERVIEW

INTRODUCTION

In the modern digital landscape, cybersecurity has become a cornerstone of organizational resilience and business continuity. For this engagement, the Solutions³ team provided a CYBER ESSENTIALS assessment.

CRITICAL SECURITY CONTROLS V8 DESCRIPTION

DHS/CISA's Cybersecurity Essentials is a comprehensive initiative designed to enhance the cybersecurity posture of organizations by providing fundamental knowledge and practical guidance on protecting digital assets. This program focuses on critical areas such as risk management, incident response, and system security, offering tools and resources to help organizations identify vulnerabilities, implement effective security measures, and respond to cyber threats. By emphasizing best practices and foundational principles, Cybersecurity Essentials aims to bolster the resilience of organizations against evolving cyber threats and safeguard sensitive information across various sectors.

==========

KEY CHARACTERISTICS OF CYBER ESSENTIALS

The key characteristics of the CYBER ESSENTIALS include, but are not limited to:

1. **Prioritized Approach**: The [safeguards] are prioritized to help organizations address the most critical areas first, ensuring a focused and effective cybersecurity strategy.
2. **Actionable Guidance**: Each control includes detailed implementation steps, making it practical and actionable for organizations of all sizes and industries.
3. **Flexibility & Adaptability**: CYBER ESSENTIALS is designed to be flexible, allowing organizations to adapt the controls to their specific needs and environments.
4. **Alignment with Industry Standards**: The framework aligns with other major cybersecurity standards and regulations, facilitating compliance and integration with existing security programs.

THE CYBER ESSENTIALS

The CYBER ESSENTIALS includes the following [safeguards]:

1. **Access Control**: Ensuring access only to those who belong on your digital space.

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

2. **Multi-Factor Authentication (MFA**): Leveraging MFA for all users, especially for privileged, administrative, or remote-access users.
3. **Network Monitoring**: Learning who is on your network and monitoring user activities for anomalous behavior.
4. **Device Inventory**: Creating and maintaining an inventory of connected devices.
5. **Strong Password Policies**: Implementing unique and strong passwords for all user accounts.
6. **User Access Management**: Developing IT policies and procedures to address changes in user status (e.g., termination, separation, or department transfers).
7. **Principle of Least Privilege**: Granting access and admin permissions based on need-to-know and least privilege principles.
8. **Regular Access Reviews**: Identifying and deactivating unused accounts and removing unnecessary privileges.
9. **Secure Remote Access**: Implementing secure methods for remote access to the network.
10. **User Education**: Training staff on cybersecurity best practices and creating a culture of cyber readiness.
11. **Device Security**: Securing all devices connected to the network, including personal devices used for work (BYOD).
12. **Policy Development**: Creating and implementing comprehensive cybersecurity policies and procedures.
13. **Configuration Management**: Actively managing systems and configurations to minimize security risks.
14. **Incident Response Planning**: Developing and maintaining plans for responding to cybersecurity incidents.

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

VALUE OF IMPLEMENTING CYBER ESSENTIALS

Implementing the CYBER ESSENTIALS framework provides numerous benefits, including:

- **Enhanced Security Posture**: Reduces the risk of cyber-attacks by addressing the most critical security areas.
- **Regulatory Compliance**: Helps meet regulatory and industry-specific security requirements.
- **Operational Efficiency**: Streamlines security operations through well-defined and actionable controls.
- **Risk Management**: Provides a structured approach to identifying, assessing, and mitigating security risks.

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

CONCLUSION

The CYBER ESSENTIALS and associated framework and best practices is a powerful tool for organizations seeking to enhance their cybersecurity defenses and protect their digital assets. By implementing these controls, organizations can build a robust security foundation that not only meets current security challenges but also adapts to future threats. As we proceed with the assessment of each control, we will provide detailed insights and recommendations tailored to our organization's unique needs and objectives.

5. CURRENT STATE DEFINITION

CAPABILITY MATURITY SCORING KEY

The table below provides the ranking numbers, their maturity label, and associated description.

RATING	MATURITY	DESCRIPTION
0	Non-Existent	Little or no evidence to support the control or the function
1	Initial	Organization is genuinely aware of the need, but it's inconsistent, poorly controlled, not documented, and/or reactive. Process may be unpredictable.
2	Managed	Documented and/or defined, but is often reactive; not necessarily followed; users may or may not be aware, trained and/or held accountable
3	Defined	Clearly defined, documented and followed; characterized by organizational support and is proactive. Key Stakeholders in place and institutionalized.
4	Quantitatively Managed	Measured & Controlled; Key Attributes Institutionalized with Risk-Based Metrics. Contributor to organizational success and adaptive.
5	Optimized	Focus is on Continuous Improvement; Can be used to predict future results; Information used in decision making. “Best-in-Class Program”

MATURITY RATING TABLE AND SPIDER DIAGRAM OVERVIEW

For each control evaluated by the project team, formal tracking has been established for each Control Family and its associated safeguards. To visually represent the maturity of each safeguard, a spider diagram was created. This diagram displays both the current state and the desired state of maturity for each control area.

Methodology

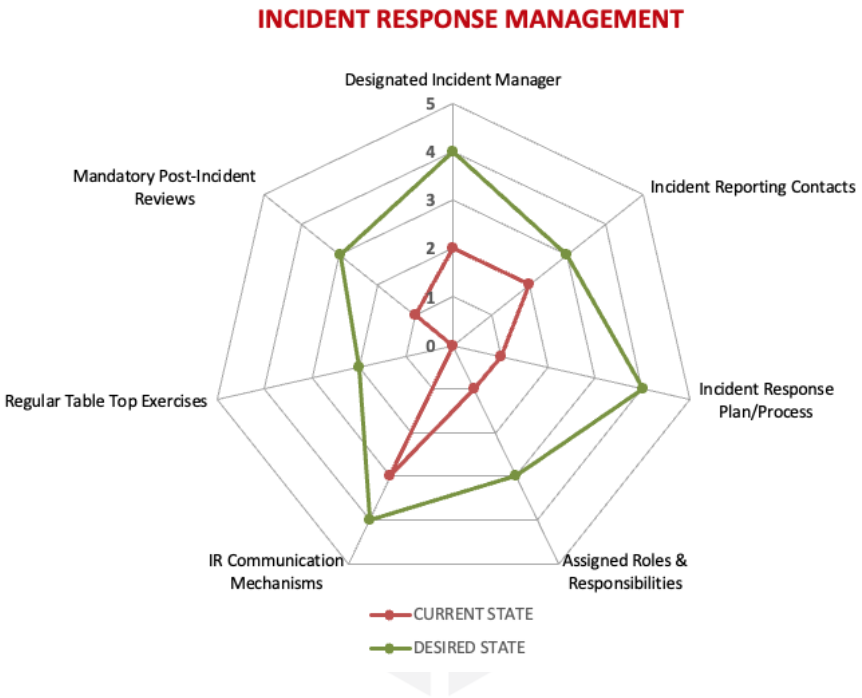
- **Current State Assessment**: The current maturity level of each safeguard was assessed and plotted on the spider diagram. The overall rating for each control area was calculated by totaling the values of each safeguard and dividing by the number of safeguards within that control.
- **Desired State Projection**: In addition to the current state, a desired state graph was generated. This projection assumes that the recommended improvements will be implemented within a reasonable timeframe (i.e., 12-18 months). An important point to keep in mind is that once the desired state is achieved, it becomes the new current state. The desired state is then redefined, and a new implementation plan is developed to reach this newly defined desired state. By continuing this approach, a state of Continual Service Improvement (CSI) is maintained.

Visual Representation

The diagram below provides a sample Maturity Ranking Table along with an example of a Current/Desired State spider diagram. This visual representation helps in understanding the current cybersecurity posture and the potential improvements after implementing the recommendations.

SAMPLE MATURITY RANKING TABLE AND SPIDER DIAGRAM

The chart below shows a sample of what a Current State/Desired State Rating might look like with its associated spider diagram.



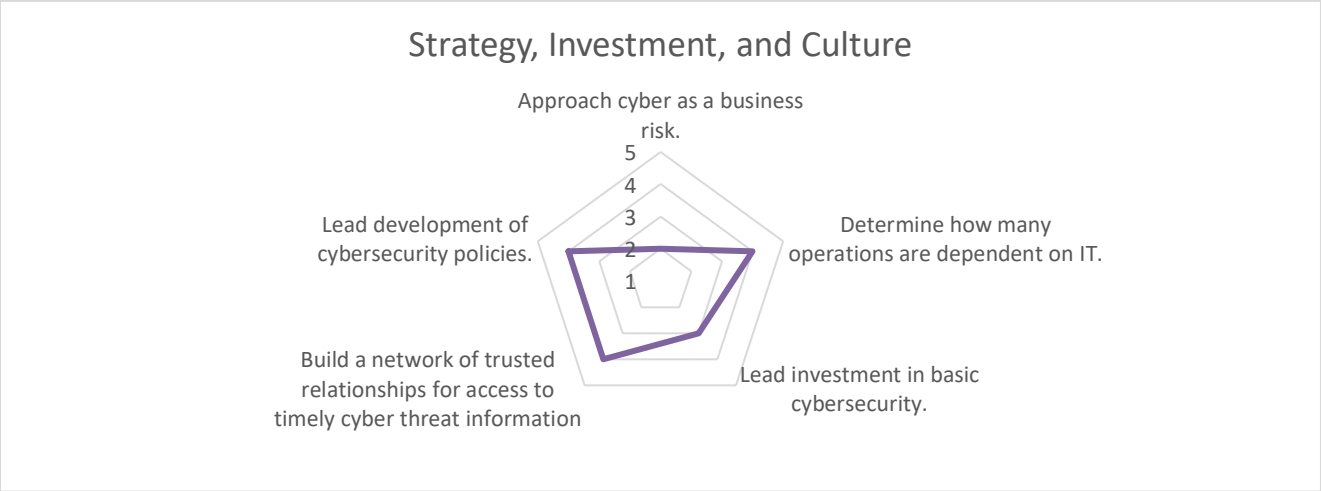
17	INCIDENT RESPONSE MANAGEMENT	CURRENT STATE	DESIRED STATE
	Designated Incident Manager	2	4
	Incident Reporting Contacts	2	3
	Incident Response Plan/Process	1	4
	Assigned Roles & Responsibilities	1	3
	IR Communication Mechanisms	3	4
	Regular Tabletop Exercises	0	2
	Mandatory Post-Incident Reviews	1	3
	INCIDENT RESPONSE MANAGEMENT RANKING	**1.43**	**3.29**

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

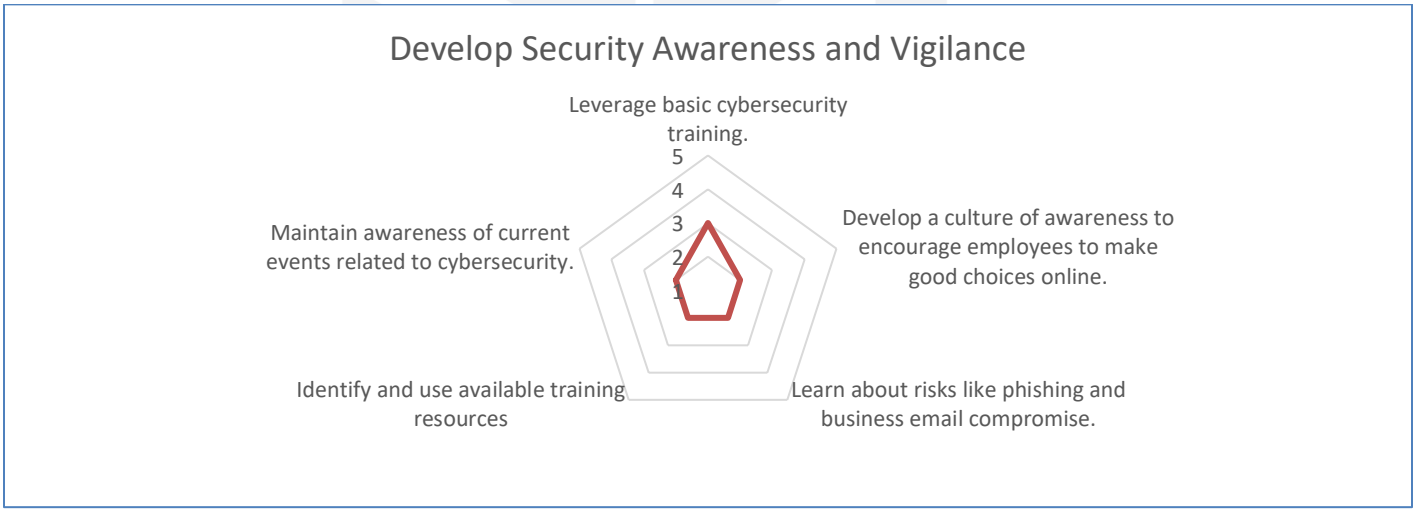
6. CYBER ESSENTIALS CURRENT STATE FINDINGS

6.0 OVERALL CYBER ESSENTIALS CURRENT STATE DIAGRAM

Based on a detailed review of all the key areas described in the key safeguard, areas, the diagram below shows the overall Current State of the SOLUTIONS3's cyber posture. The following sections will provide the details of each of the areas and the project team's findings in each of those areas.

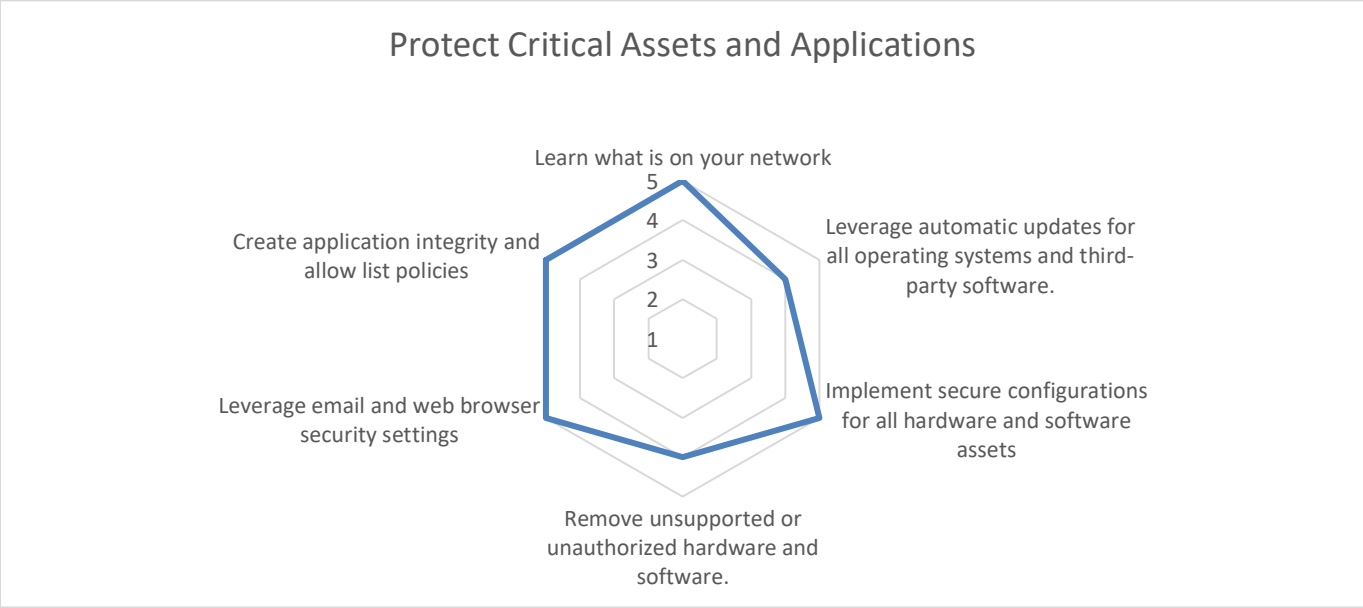


This spider diagram represents the current state of SOLUTIONS3's posture according to the 'Strategy, Investment, and Culture' toolkit.

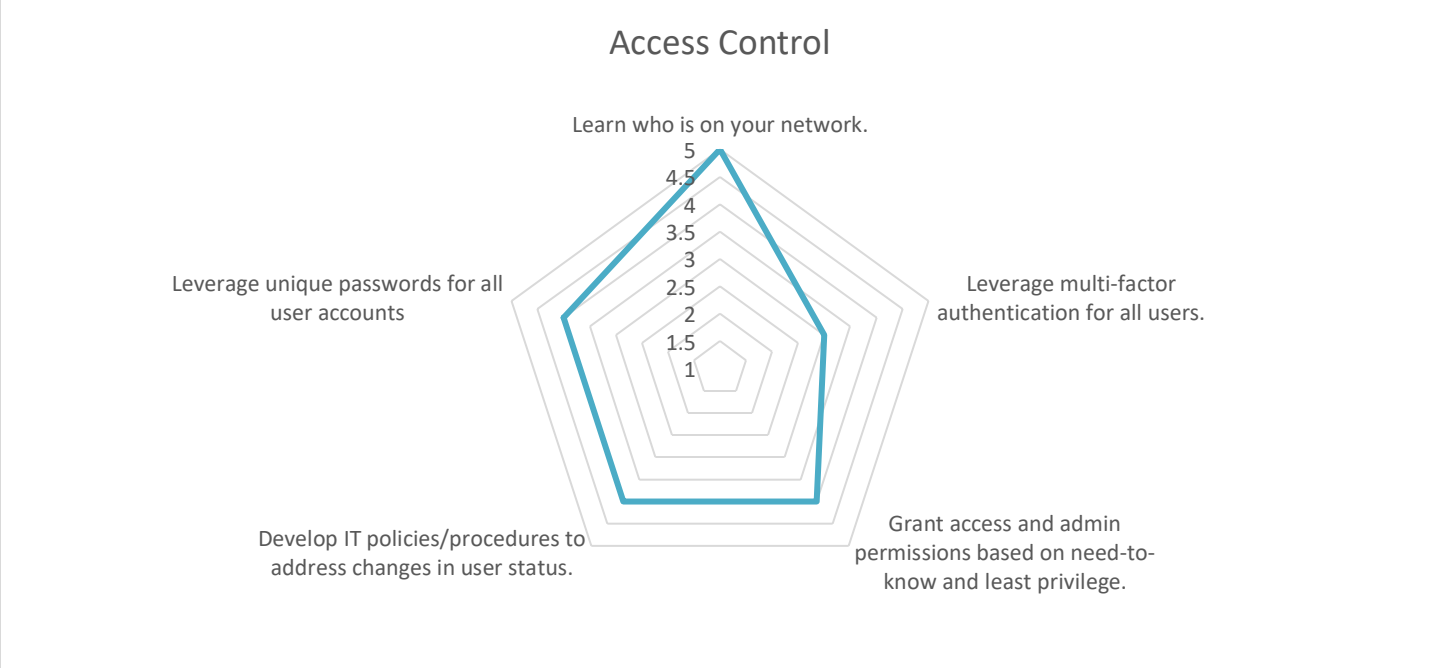


This spider diagram represents the current state of SOLUTIONS3's posture according to the 'Develop Security Awareness and Vigilance' toolkit.

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

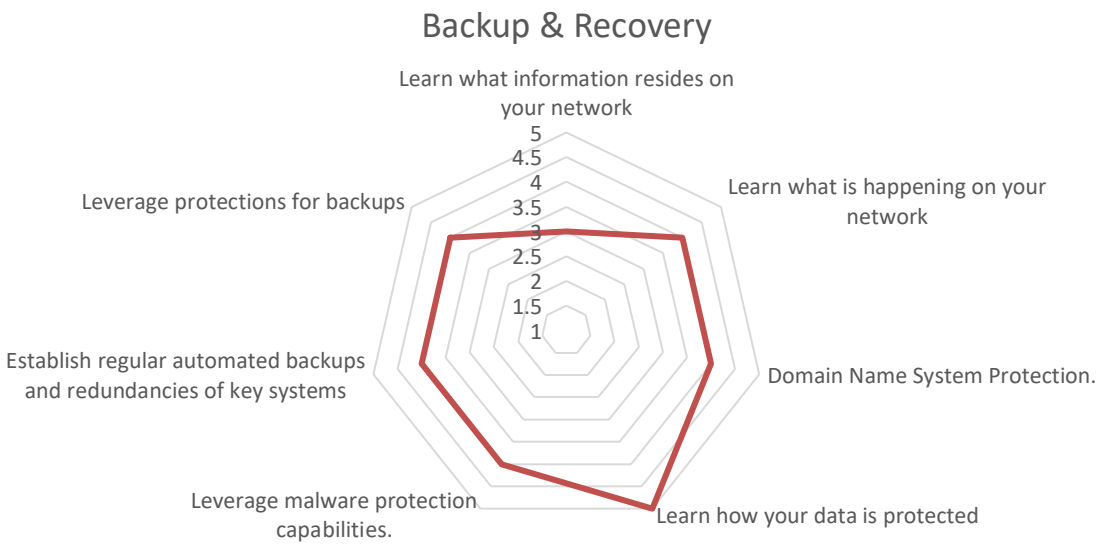


This spider diagram represents the current state of SOLUTIONS3's posture according to the 'Protect Critical Assets and Applications' toolkit.

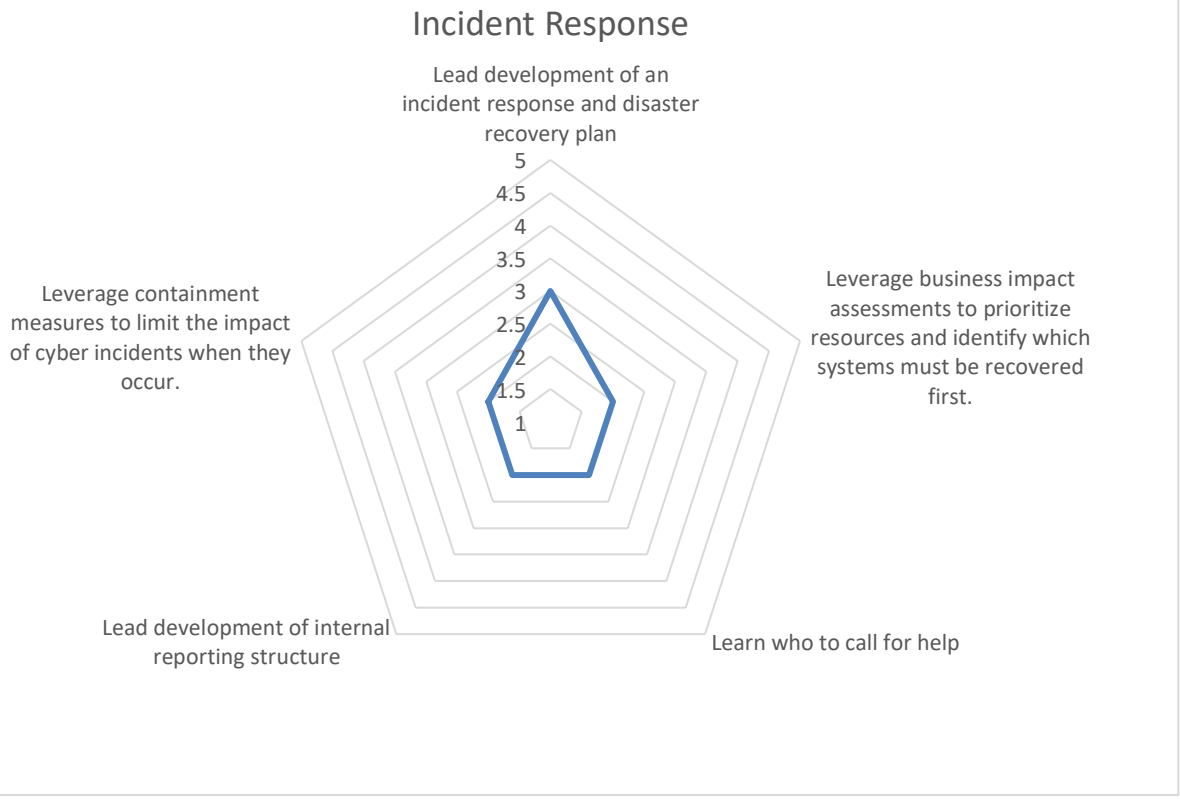


This spider diagram represents the current state of SOLUTIONS3's posture according to the 'Access Control' toolkit.

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com



This spider diagram represents the current state of SOLUTIONS3's posture according to the 'Backup & Recovery' toolkit.



637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

This spider diagram represents the current state of SOLUTIONS3's posture according to the 'Incident Response' toolkit.

Control Area Assessment Table

The area of **Developing Security Awareness and Vigilance** is rated as **"2.2.** There are some areas that are being done well but other areas that are not in line with the specific control safeguards.

CONTROL: Security Awareness	
OVERALL LEVEL: Process Defined & Documented for Projects but is Often Reactive. Several Attributes in Place and Realized but Still Missing Certain Risk-Addressing Attributes	**OVERALL SCORE: 2.2**

The project team has identified the gaps with each control objective along with recommendations for remediation and their associated benefits. By incorporating these recommendations, you will strengthen your security awareness practices and align with the associated CYBER ESSENTIALS safeguards.

CONTROL: Security Awareness	
SAFEGUARD	**FINDINGS**
1. **Leverage basic cybersecurity training.** **Score**: 3.0	▪ [redacted]
2. Develop a culture of awareness to encourage employees to make good choices online. **Score** 2.0	▪ [redacted]

	[redacted]
3. Learn about risks like phishing and business email compromise. **Score**: 2.0	▪ [redacted]
4. Identify and use available training resources **Score**: 2.0	▪ [redacted]
5. Maintain awareness of current events related to cybersecurity. **Score**: 2.0	▪ [redacted]

REMEDIATION RECOMMENDATIONS

We would recommend looking into FedVTE: the Federal Virtual Training Environment as a means of training your employees even further. It provides free online cybersecurity training to state and smaller businesses like yourselves. Link provided:https://fedvte.usalearning.gov/public_fedvte.php

We recommend looking at the CISA Security Tip page as they have some great articles involving leadership and how CEOs or anyone in a position of leadership can share with their employees to further improve cybersecurity preparedness.

We recommend looking into the FTC's Talking Cybersecurity with your employee's document. It teaches the basics of cybersecurity urgency and ways to avoid risks and cyber-attacks. Link Provided: https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecurity_sb_discussion-guide_101218.pdf

Control Area 2:

The area of **Critical Assets and application** is rated as **"5".** There are some areas that are being done well but other areas that are not in line with the specific control safeguards.

CONTROL: Critical Assets and Application	
OVERALL LEVEL: Patching procedures and continually improved and best-in-class.	**OVERALL SCORE: 5**

The project team has identified the gaps with each control objective along with recommendations for remediation and their associated benefits. By incorporating these recommendations, you will strengthen your security awareness practices and align with the associated CYBER ESSENTIALS [safeguards].

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

CONTROL: Critical Assets and Application	
SAFEGUARD	**FINDINGS**
6. Learn what is on your network **Score**: 5	▪ [redacted]
7. Leverage automatic updates for all operating systems and third-party software. **Score** 4	▪ [redacted]
8. Implement secure configurations for all hardware and software assets **Score**: 5	▪ [redacted]
9. Remove unsupported or unauthorized hardware and software. **Score**: 4	▪ [redacted] ▪ [redacted]
10. Leverage email and web browser security settings **Score**: 5	▪ [redacted]

11. Create application integrity and allow list policies **Score**: 5	▪ [redacted]

REMEDIATION RECOMMENDATIONS

The CISA guide offers strategies for securing web browsers and defending against malvertising. This ensures robust protection from cyber threats.

- The CSI guide provides steps to secure web browsing, reducing vulnerabilities and enhancing overall cybersecurity posture. Following these guidelines helps maintain data integrity, confidentiality, and compliance with security standards.
- Following the guidelines in these documents would benefit a company by enhancing its web browser security, protecting against malicious advertising, and safeguarding sensitive data.

BENEFITS OF REMEDIATION

Implementing the recommendations from the CISA and CSI guides can significantly enhance the company's cybersecurity posture by securing web browsers and defending against malvertising. This not only protects sensitive data from being compromised but also ensures compliance with industry standards.

Control Area 3:

The area of **Access Control** is rated as **"4".** There are some areas that are being done well but other areas that are not in line with the specific control safeguards.

CONTROL: Access Control

OVERALL LEVEL: Measured and Controlled, all key attributes institutionalized with Risk – Based Metrics. **OVERALL SCORE: 4**

The project team has identified the gaps with each control objective along with recommendations for remediation and their associated benefits. By incorporating these recommendations, you will strengthen your security awareness practices and align with the associated CYBER ESSENTIALS safeguards.

CONTROL: Access Control	
SAFEGUARD	**FINDINGS**
12. **Learn who is on your network.** **Score**: 5.0	▪ [redacted]
13. Leverage multi-factor authentication for all users. **Score** 2.0	▪ [redacted]
14. ------ **Score**: ----	▪ -----
15. Grant access and admin permissions based on need-to-know and least privilege. **Score**: 2.0	▪ [redacted]

	▪ [redacted]
16. Develop IT policies/procedures to address changes in user status. **Score**: 2.0	▪ [redacted]
17. Leverage unique passwords for all user accounts **Score**: 2.0	▪ [redacted]

REMEDIATION RECOMMENDATIONS

- Regarding many of the password protections we discussed, we have a few recommendations for your approaches to handling user passwords.
- We recommend not only following Microsoft's password protocols but also coming up with your own ways to protect user passwords.
- We would recommend taking some time to looking into the NSA Actively Manages Systems and Configurations guide as it offers a wide range of techniques to minimize mission impacts regarding networks.
  https://media.defense.gov/2019/Sep/09/2002180326/-1/-1/0/ACTIVELY%20MANAGE%20SYSTEMS%20AND%20CONFIGURATIONS.PDF

BENEFITS OF REMEDIATION

- We would recommend taking some time to looking into the NSA Actively Manages Systems and Configurations guide as it offers a wide range of techniques to minimize mission impacts regarding networks.
- We recommend not only following Microsoft's password protocols but also coming up with your own ways to protect user passwords.
- It would be very cost effective to go through sharing this document and mandating the ways you can enforce password protection more on the users.

Control Area 4:

The area of **Backup & Recovery** is rated as **"4".** There are some areas that are being done well but other areas that are not in line with the specific control safeguards.

CONTROL: Backup & Recovery	
OVERALL LEVEL: Component are measured and controlled with risk-based metrics.	**OVERALL SCORE: 4**

The project team has identified the gaps with each control objective along with recommendations for remediation and their associated benefits. By incorporating these recommendations, you will strengthen your security awareness practices and align with the associated CYBER ESSENTIALS [safeguards].

CONTROL: Backup and Recovery	
SAFEGUARD	**FINDINGS**
18. Learn what information resides on your network **Score**: 5	▪ [redacted]
19. Learn what is happening on your network **Score** 3	▪ [redacted]
20. Domain Name System Protection. **Score**: 4	▪ [redacted]
21. Learn how your data is protected**.** **Score**: 4	▪ [redacted] ▪

22. Leverage malware protection capabilities. **Score**: 4	▪ [redacted]
23. Establish regular automated backups and redundancies of key systems **Score**: 5 24. Leverage protections for backups Score: 4	▪ [redacted]

REMEDIATION RECOMMENDATIONS

- We recommend looking into the CIS Controls implementation Groups document as it helps organizations classify themselves and focus their security resources and expertise while leveraging the value of the CIS Controls.

- We also recommend looking into the NIST National Cyber Security Center of Excellence document. It is a guide for managed service providers to conduct, maintain and test backup files; protecting data from ransomware and other data loss events.

- We recommend looking into the Cyber Readiness Institute's guide on educating employees on how to keep their host computer secure when connecting to the company's virtual desktop interface.

BENEFITS OF REMEDIATION

CIS Controls Implementation Groups: Helps the organization classify itself and prioritize security resources effectively. This ensures that security measures are tailored to the company's specific needs and risk levels.

2. NIST National Cyber Security Center of Excellence: Offers guidelines for managed service providers to maintain and test backup files, protecting data from ransomware and other data loss events. This enhances data integrity and business continuity.

3. Cyber Readiness Institute's Guide: Educates employees on securing their host computers when connecting to the company's virtual desktop interface, reducing the risk of cyber threats entering through insecure endpoints.

These recommendations lower risks such as data breaches, ransomware attacks, and unauthorized access by ensuring robust security practices, improving employee awareness, and enhancing data protection.

Control Area 5:

The area of **Incident Response** is rated as **"2".** There are some areas that are being done well but other areas that are not in line with the specific control safeguards.

CONTROL: Incident Response	
OVERALL LEVEL: Process Defined & Documented for Projects but is Often Reactive. Several Attributes in Place and Realized but Still Missing Certain Risk-Addressing Attributes	**OVERALL SCORE: 2.2**

The project team has identified the gaps with each control objective along with recommendations for remediation and their associated benefits. By incorporating these recommendations, you will strengthen your security awareness practices and align with the associated CYBER ESSENTIALS [safeguards].

CONTROL: Incident Response	
SAFEGUARD	**FINDINGS**
25. **Lead development of an incident response and disaster recovery plan** **Score**: 3.0	▪ [redacted]

	[redacted]
26. Leverage business impact assessments to prioritize resources and identify which systems must be recovered first. **Score** 2.0	▪ [redacted]
27. Learn who to call for help **Score**: 2.0	▪ [redacted]
28. Lead development of internal reporting structure **Score**: 2.0	▪ [redacted]
29. Leverage containment measures to limit the impact of cyber incidents when they occur. **Score**: 2.0	▪ [redacted]
30. ----- **Score**: -----	▪ ------

REMEDIATION RECOMMENDATIONS

- Reading the NIST SP 800-184 can help formalize Incident Response documents and plans.

Haivng proper documentation is necessary so that you can continue update your policies throughout your time within the company.

- We recommend making your disaster recovery tests a bit more frequently. While yes quarterly is a good routine,

BENEFITS OF REMEDIATION

- Implementing the policies described in the NIST SP 800-184 Guide for Cybersecurity Event Recovery provides numerous benefits. It enhances the organization's resilience by ensuring comprehensive recovery planning, which minimizes the impact of cybersecurity incidents. This involves identifying and prioritizing resources, developing

effective recovery plans, and continuously improving these plans by learning from past events. These measures help maintain the continuity of essential functions, reduce downtime, and protect sensitive data, thereby lowering the risks associated with cyber incidents, such as data breaches, operational disruptions, and financial losses.

Control Area 6:

CONTROL: Strategy, Investment, and Culture	
OVERALL LEVEL: Component are measured and controlled with risk-based metrics.	**OVERALL SCORE: 4**

SAFEGUARD	**FINDINGS**
31. **Approach cyber as a business risk.** **Score**: 2.0	▪ [redacted]

32. Determine how many operations are dependent on IT. **Score** 4	▪ [redacted]
33. Lead investment in basic cybersecurity **Score**: 3	▪ [redacted]
34. Build a network of trusted relationships for access to timely cyber threat information. **Score**: 4	▪ [redacted]
35. Lead Development of Cybersecurity policies. **Score**: 4	▪ [redacted]

REMEDIATION RECOMMENDATIONS

- Develop a formal threat intelligence strategy and documentation process
- Implement a structured approach to collecting, analyzing, and disseminating threat intelligence
- Establish clear roles and responsibilities for threat intelligence management

BENEFITS OF REMEDIATION

- Improved consistency and efficiency in threat intelligence handling

- Enhanced ability to prioritize and respond to threats
- Better alignment of threat intelligence with organizational risk management

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

7. FORMAL RECOMMENDATIONS

OVERALL RECOMMENDATIONS

Of course, no one is perfect, and we acknowledge that! There is always room for improvement so that's why we created these recommendations. We feel that all the advice and resources we shared with you will further improve the company in the long term. Not only will it help make your employees more aware of the many cybersecurity risks and threats out there, but it will also help improve their communication because they will be educated enough to understand why awareness training is so important. These remediations will lower risks heavily as phishing schemes will have a much lower success rate due to employee and leader understanding. These recommendations lower risks such as data breaches, ransomware attacks, and unauthorized access by ensuring robust security practices, improving employee awareness, and enhancing data protection. Implementing the policies described in the NIST SP 800-184 Guide for Cybersecurity Event Recovery provides numerous benefits. It enhances the organization's resilience by ensuring comprehensive recovery planning, which minimizes the impact of cybersecurity incidents. This involves identifying and prioritizing resources, developing effective recovery plans, and continuously improving these plans by learning from past events. These measures help maintain the continuity of essential functions, reduce downtime, and protect sensitive data, thereby lowering the risks associated with cyber incidents, such as data breaches, operational disruptions, and financial losses.

OVERALL BENEFITS

Following the provided recommendations offers numerous benefits for the company and its employees. By implementing these measures, the organization can significantly enhance its cybersecurity posture and overall resilience. Employees will become more aware of various cybersecurity risks and threats, leading to improved communication within the company. This increased awareness will result in a lower success rate for phishing schemes and reduce the risks of data breaches, ransomware attacks, and unauthorized access. Implementing policies from the NIST SP 800-184 Guide enhances the organization's ability to recover from cybersecurity incidents through comprehensive recovery planning. This approach helps identify and prioritize resources effectively and continuously improve recovery plans by learning from past events. As a result, the organization can maintain essential functions more effectively, reduce downtime in case of cyber incidents, and better protect sensitive data. These measures collectively contribute to creating a more secure work environment, minimizing financial losses associated with cyber incidents, and improving the company's overall resilience in the face of evolving cybersecurity threats.

637 Wyckoff Ave
PMB 352
Wyckoff NJ 07481
Phone: 201-891-9977
www.Solutions3LLC.com

8. EXECUTIVE SUMMARY

This report strongly recommends implementing cybersecurity measures outlined in the Cyber Essentials toolkit to strengthen Solutions3's digital defenses. The Cyber Essentials scheme, developed by the US government, provides a solid foundation for protecting against common cyber threats. Our analysis reveals gaps in Solutions3's cybersecurity posture that malicious actors could exploit. The toolkit offers cost-effective, practical steps to address these vulnerabilities and could reduce our risk of falling victim to up to 80% of common cyber-attacks. Key recommendations include ensuring secure system configurations, controlling data access, implementing malware protection, and managing software updates effectively. Benefits of implementation include enhanced protection of company assets, improved cyber resilience, increased stakeholder confidence, potential reductions in cyber insurance premiums, and compliance with industry standards. While there are associated implementation costs, they are significantly outweighed by the possible financial and reputational damage of a successful cyber-attack. We strongly urge immediate action to adopt these essential cybersecurity measures to safeguard Solutions3's future in an increasingly digital landscape.