Cyber Maturity Assessment Report

SILVERSKY

Prepared for:

Word of Life Fellowship Inc.

Table of Contents

Cyber Maturity Assessment

1. Introduction

1.1 User Profile

First Name	Matt	Last Name	Hager
Email	matth@wol.org	Job Title	Director of IT
Date of Survey	September 11, 2023		

1.1 Company Profile

Company Name	Word of Life Fellowship Inc.		
Industry	Education	Employee Size	251-500

Cyber Maturity Assessment

1. Introduction

1.2 Executive Summary

The SilverSky Cyber Maturity Assessment is based off a combination of several industry frameworks to provide a simple best practice assessment that can measure your cyber program's maturity. This report helps identify maturity improvement areas and provides recommendations to assist your organization in prioritizing risk mitigation improvements. The report also provides insight into how your cyber maturity measures up to your industry peers and like sized organizations. The following Executive report summarizes the results of your Cyber Maturity Assessment. Detailed sections on these finding below can be found within this report.

Based on the answers to the SilverSky's Cyber Maturity Assessment your organization falls within the of Cyber Security Maturity. This classifies your organizational cyber maturity within the phase of

73%	percentile.
Intermediate	

Evolving maturity is characterized as those organizations that have begun to invested in Cyber security and may show strong maturity in one or more cyber domains but are still in need of maturing across multiple cyber domains.

Core Cyber Pillar Assessment

The assessment first analyzed your current Cybersecurity program from four (4) critical core functional cyber security pillars. These pillars evaluated your organizational capabilities to identify and assess risk, your ability to implement protection controls, your ability to detect threats and your ability to respond and recover from an incident.

Your organization can gain the most initial maturity improvement impact within the cybersecurity Pillar of

Detect

Cyber Domain Maturity Assessment

As a second phase of the assessment, SilverSky went a level deeper to measure your organization's cyber maturity across fourteen (14) common cyber security domains that fall within these four critical core functional cyber security pillars. As a result of this assessment SilverSky identified the top 5 cyber domains that your should invest in to enhance your cyber maturity. Those domains are listed in order of importance from most significant.

Top Domains to Mature	Current Maturity Level	Maturity Score
No Result		

SilverSky Service Recommendations

Lastly, SilverSky has compiled a list of services that SilverSky provides that map to your areas of maturity improvement. This list can be used as a strategic roadmap or solutions you should consider to help increase your organizational cyber maturity.

Top Domains to Mature	SilverSky Recommended Services
No Result	

Cyber Maturity Assessment
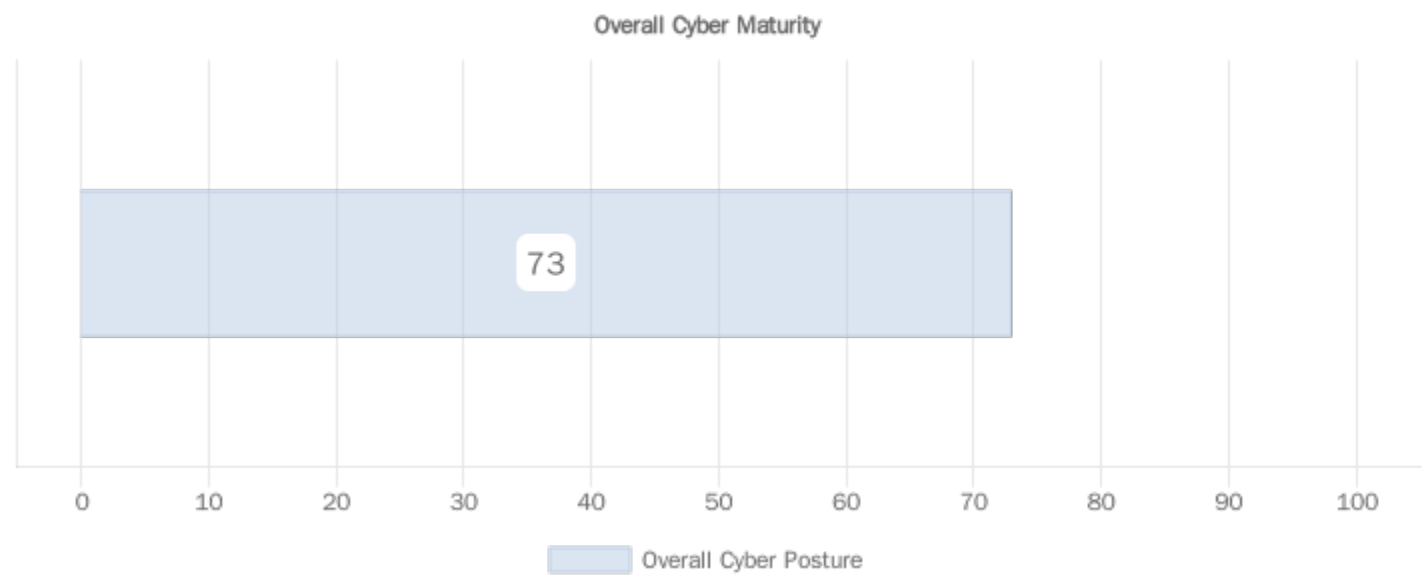
2. Cyber Maturity Assessment

2.1 Overall Cyber Maturity Posture

Based on the answers to the SilverSky's Cyber Assessment your organization's cyber maturity falls within the:

73%

percentile, which classifies your organizational cyber maturity within category of

Intermediate

Overall Cyber Maturity

| Baseline	Baseline maturity is characterized as those organizations meeting minimum expectations recommended by best practice security, industry frameworks and regulations.	
Evolving	Evolving maturity is characterized as those organizations that have begun to invested in cyber security and may show strong maturity in one or more cyber domains but are still in need of maturing across multiple cyber domains.	
Intermediate	Intermediate maturity is characterized as those organizations that have started their cyber journey by building solid maturity across multiple cyber domains but may be lacking maturity in a few cyber domains.	X
Advance	Advanced maturity is characterized as those organizations that have committed to building a comprehensive cyber program and show solid maturity across all cyber domains but may be lacking maturity in a one or more cyber domains.	
Invested	Invested maturity is characterized as those organizations that have a strong commitment to cyber security and have invested in the people, processes and technologies to show comprehensive cyber maturity in all assessed cyber domains.	

Cyber Maturity Assessment

2. Cyber Maturity Assessment

2.2 Maturity Across Core Functional Areas

The core functional assessment looks at your organizational cyber maturity across four functional areas that help make up a cyber program. Those functional areas are comprised of the Identify, Protect, Detect and Response/Recovery phases. These four functions, when combined, provide the key program areas for building out a comprehensive cyber program.

- **Identify** – Assessment of the Organization's ability to develop, understand and manage cyber security risk
- **Protect** - Assessment of the Organization's ability to develop and implement appropriate safeguards to ensure protection controls
- **Detect** – Assessment of the Organization's ability to develop processes to identify the occurrence of a cybersecurity event
- **Respond/Recover** - Assessment of the Organization's ability to develop processes to take action and restore from a cybersecurity event

Based on the results of SilverSky's assessment the following chart displays your current maturity across these four functional areas from least mature to most mature. Your organization's biggest opportunity for increasing cyber maturity is within the functional pillar of:

Maturity by Domain
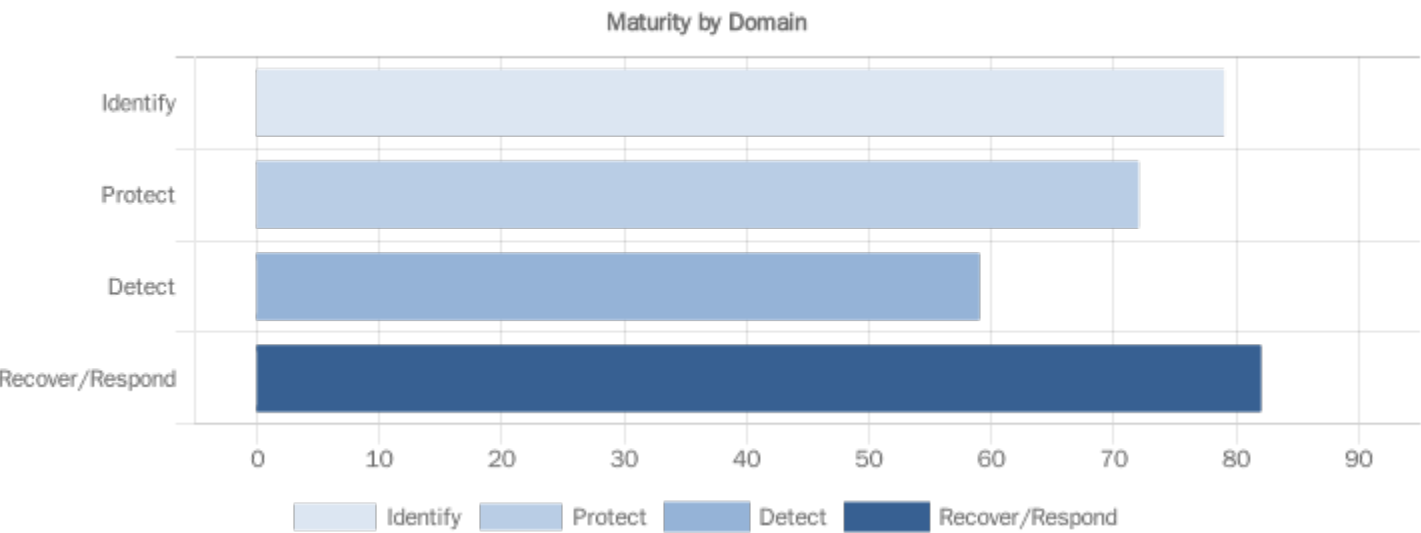
Your organization's biggest opportunity for increasing cyber maturity is within the functional pillar of:	Detect	59%
Functional Pillar	**Cyber Maturity Score**	**Improvement Priority**
Identify	79%	Low
Protect	72%	Low
Detect	59%	Medium
Respond/Recover	82%	Very Low

Cyber Maturity Assessment

2. Cyber Maturity Assessment

2.3 Maturity Across Cyber Domains

Below is a single view of all the capabilities covered in this assessment and their results. SilverSky measured your organization's

cyber maturity across fourteen (14) common domains and four (4) key pillars or functions.

The questions represented in this survey are SilverSky's representation of best practices relating to each of these domains and pillars and will assist in providing strategic guidance on where to focus time and energy in building additional cyber capabilities. The red color in the chart represents areas of low or no maturity, orange represents areas where some or weak maturity exists and green represents areas of heightened maturity.

Identify	Oversight	100%
	IT Asset Management	50%
	Risk Assessment	67%
	Third Party Risk	100%
Protect	Training/Culture	50%
	Infrastructure Management	100%
	Patch Management	67%
Detect	Threat Intelligence and Information	67%
	Monitoring and Analyzing	50%
	Threat and Vulnerability Detection	40%
	Event Detection	80%
Respond & Recover	Planning	80%
	Testing	67%
	Mitigation and Recovery	100%

Cyber Maturity Assessment

3. Cyber Capability Assessment

3.1 Identify

During the assessment your organization showed a maturity score within the Identify functional cyber capability area of:	79%

Why is the Identify Functional Program Area important to a cyber program?

The Identify capability in cybersecurity is critical to the development of an organization's understanding of cybersecurity risks to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

The Identify Category is comprised of four capabilities as part of SilverSky's Cyber Maturity Assessment:

Oversight Measures if proper structure is in place including people, policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements.

Asset Management Measures the organizational process that exists to identify and manage the devices and systems that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

Risk Assessment Measures if the organization understands the cybersecurity risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Third Party Risk Measures the organizational maturity around its third party and supply chain risk management processes.

Capability	Capability Level				
	Very Low	Low	Medium	High	Very High
Oversight					✕
IT Asset Management			✕		
Risk Assessment				✕	
Third Party Risk					✕

Cyber Maturity Assessment

3. Cyber Capability Assessment

3.2 Protect

During the assessment your organization showed a maturity score within the Protect functional cyber capability area of:	72%

Why is the Protect Functional Program Area important to a cyber program?

The Protect capability area is a critical component of a cyber program because it measures the organization's ability to proactively protect organizational assets from cyber attacks on critical infrastructure. The protect function measures the organizational ability to limit or contain the impact of a potential cybersecurity event by having proactive measures in place.

The Identify Category is comprised of three capabilities as part of SilverSky's Cyber Maturity Assessment:

Training/Culture Measures the organization's maturity around providing personnel and partners cybersecurity awareness education and testing to enforce their duties and responsibilities consistent with related policies, procedures, and agreements.

Infrastructure Management Measures the organization's maturity around the ability to manage and maintain information system components consistent with policies and procedures.

Patch Management Measures the organization's ability to patch systems from potential threats and vulnerabilities that can expose systems to compromise.

CAPABILITY	CAPABILITY LEVEL				
	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
Training/Culture			✕		
Infrastructure Management					✕
Patch Management				✕	

Cyber Maturity Assessment

3. Cyber Capability Assessment

3.3 Detect

During the assessment your organization showed a maturity score within the Detect functional cyber capability area of:	59%

Why is the Detect Functional Program Area important to a cyber program?

The Detect function is critical to a cyber security program since it involves the processes and procedures necessary for the timely discovery of cybersecurity events within an organization. The quicker potential issues are detected will drastically reduce the overall impact a cyber event will have across an organization.

The Detect Category is comprised of four areas as part of SilverSky's Cyber Maturity Assessment:

Threat Intelligence and Information Measures how well an organization can acquire and analyze information to identify, track, and predict cyber capabilities, intentions, and activities

Monitoring and Analyzing Measures how well your information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures

Threat and Vulnerability Detection Measures an organizations ability to detect and eradicate threats and vulnerabilities within their environment.

Event Detection Measures an organizations ability to detect malicious activity within their networks.

CAPABILITY	CAPABILITY LEVEL				
	VERY LOW	**LOW**	**MEDIUM**	**HIGH**	**VERY HIGH**
Threat Intelligence and Information				✕	
Monitoring and Analyzing			✕		
Threat and Vulnerability Detection		✕			
Event Detection				✕	

Cyber Maturity Assessment

3. Cyber Capability Assessment

3.4 Respond and Recover

During the assessment your organization showed a maturity score within the Response and Recover functional cyber capability areas of:	**82%**

Why is the Response and Recovery Functional Program Area important to a cyber program?

The Respond and Recover elements play a key role in a cyber program. The Respond capability ensures organizations have implemented the appropriate procedure that will allow them to take action regarding a detected cybersecurity incident. While the Recover Function examines the organizations capability to resume operations after a potential cybersecurity incident.

The Respond and Recovery Categories are comprised of three capabilities as part of SilverSky's Cyber Maturity Assessment:

Response Planning Measures the organizational maturity around how response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

Testing Measures the organizational readiness to handle an incident through its ability to communicate and test their incident response processes.

Response and Mitigation Measures the organizational capability to prevent expansion of an event, mitigate its effects, and resolve the incident.

CAPABILITY	CAPABILITY LEVEL				
	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
Response Planning				✕	
Testing				✕	
Response and Mitigation					✕

Cyber Maturity Assessment

4. Summary of Recommended Actions

4.1 Maturity Improvement Areas

Based on the results of the assessment, your organization would experience the highest level of Cyber maturity growth by focusing on the following cyber domains:

Priority	Current Maturity	Maturity Score	Domain	Why is it Important to Cyber?
No Result				

Cyber Maturity Assessment

4. Summary of Recommended Actions

4.2 How SilverSky Can Help

Based on your top maturity improvement areas, SilverSky has generated a list of the top service offerings that we offer that would help you enhance your Cyber Maturity. These recommendations are listed in the order of important to your cyber program.

Priority	Improvement Domain	Matching SilverSky Services	How Theses Service Helps Improve Maturity
No Result			