# Cyber Maturity Assessment Report

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** | 7/26/2023 | | |

### 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 Cybersecurity 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 Assessment your organization falls within the of Cyber Security Maturity. This classifies your organizational cyber maturity within the phase of

0% percentile

Baseline

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 (4) 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 |
|---|---|---|
| Event Detection | Very Low | 0% |
| IT Asset Management | Very Low | 0% |
| Infrastructure Management | Very Low | 0% |
| Mitigation and Recovery | Very Low | 0% |
| Monitoring and Analysis | Very Low | 0% |

**SilverSky Service Recommendations**

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

| Top Domains to Mature | SilverSky Recommended Services |
|---|---|
| Event Detection | SilverSky Lightning MDR, MEDR |
| IT Asset Management | SilverSky's Insight Services |
| Infrastructure Management | SilverSky ProServ -IT Controls Review, Managed Firewall Service, Firewall Configuration Reviews (QSR), Managed DUO |
| Mitigation and Recovery | SilverSky MIR, SilverSky ProServices - IR Plan Development |
| Monitoring and Analysis | SilverSky Lightning MDR, MEDR |

# 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:

**0%**

percentile, which classifies your organizational cyber maturity within category of

**Baseline**


| | | |
|---|---|---|
| **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. | |
| **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

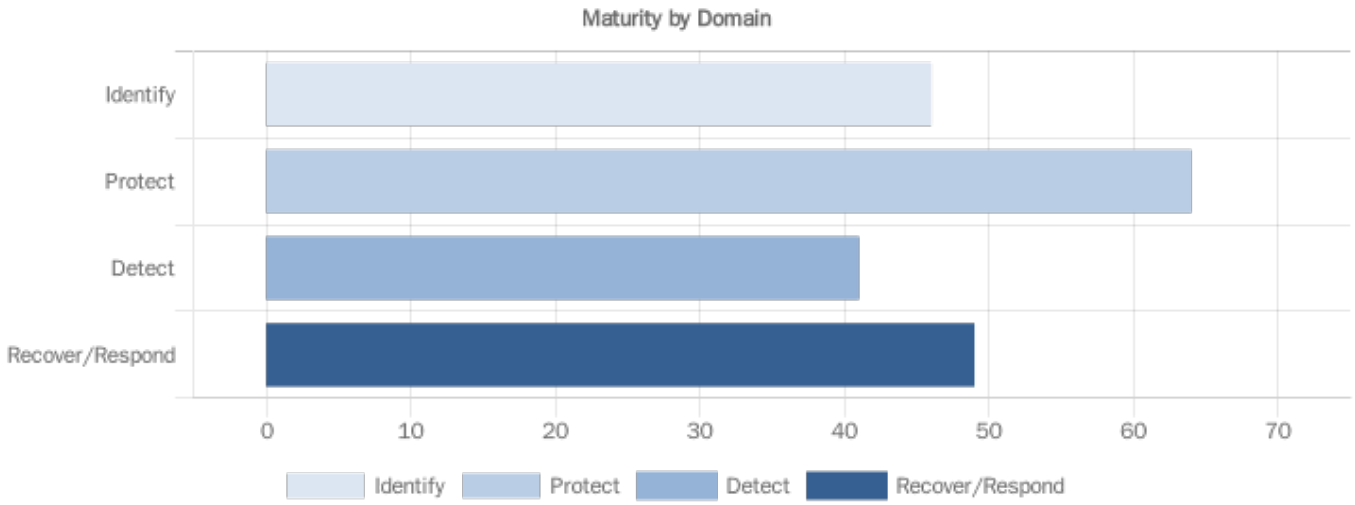
## 2. Cyber Maturity Assessment

### 2.2 Maturity Across Core Functional Areas

The core functional assessment looks at your organizational cyber maturity across four (4) functional areas that help make up a cyber program. Those functional areas are comprised of the Identify, Protect, Detect and Response/Recovery phases of a cyber program. 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
- **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:




| Your organization's biggest opportunity for increasing cyber maturity is within the functional pillar of: | Detect | 0% |
|---|---|---|
| **Functional Pillar** | **Cyber Maturity Score** | **Improvement Priority** |
| Identify | 0% | Very High |
| Protect | 0% | Very High |
| Detect | 0% | Very High |
| Respond/Recover | 0% | Very High |

# Cyber Maturity Assessment

## 2. Cyber Maturity Assessment

### 2.3 Maturity Across Cyber Domains

Below is a single view of all 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 reresents areas of hightened maturity.

| | | |
|---|---|---|
| Identify | Oversight | 0% |
| | IT Asset Management | 0% |
| | Risk Assessment | 0% |
| | Third Party Risk | 0% |
| Protect | Training/Culture | 0% |
| | Infrastructure Management | 0% |
| | Patch Management | 0% |
| Detect | Threat Intelligence and Information | 0% |
| | Monitoring and Analyzing | 0% |
| | Threat and Vulnerability Detection | 0% |
| | Event Detection | 0% |
| Respond & Recover | Planning | 0% |
| | Testing | 0% |
| | Mitigation and Recovery | 0% |

# 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: | 0% |
|---|---|

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

The Identify capability in cybersecurity is ciritical to 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 domains 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 | X | | | | |
| IT Asset Management | X | | | | |
| Risk Assessment | X | | | | |
| Third Party Risk | X | | | | |

# 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: | 0% |

**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 organizations ability to proactively protect organizational assests from cyber attacks on critical infrastructure. The protect function measures the orginazational ability to limit or contain the impact of a potential cybersecurity event by having proactive measures in place.

**The Identify Category is comprised of four domains 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 comprimise.

| CAPABILITY | CAPABILITY LEVEL | | | | |
|---|---|---|---|---|---|
| | VERY LOW | LOW | MEDIUM | HIGH | VERY HIGH |
| Training/Culture | X | | | | |
| Infrastructure Management | X | | | | |
| Patch Management | X | | | | |

# 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: | 0% |

**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 procedure necessary to timely discover cybersecurity events within a 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 domains 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 | X | | | | |
| Monitoring and Analyzing | X | | | | |
| Threat and Vulnerability Detection | X | | | | |
| Event Detection | X | | | | |

# 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: | 0% |

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

The response and recover elements play a key role in a cyber program. The Respond capability ensure 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 domains 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 | X | | | | |
| Testing | X | | | | |
| Response and Mitigation | X | | | | |

# Cyber Maturity Assessment

## 4. Summary of Recommeded 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? |
|---|---|---|---|---|
| 1 | Very Low | 0% | Event Detection | Event logging and detection play critical roles in a security program by providing valuable information that can help prevent, detect, and respond to security incidents. Event logging involves the collection of data on activities occurring within a system or network. The ability to detect events across critical system components like perimeter activity, email activity, endpoint activity and user activity are critical for the ability to reconstruct what happened during a security incident. |
| 2 | Very Low | 0% | IT Asset Management | Maintaining an inventory of organizational assets, prioritizing assets based on criticality/value to the business, assigning accountability for maintaining the inventory of assets, and having a formal change management process are vital components for effective cybersecurity management. Developing processes around asset management helps organizations understand their digital landscape, assess risks, detect threats, manage vulnerabilities, control access, respond to incidents, and comply with regulations.<br><br>The lack of an asset inventory process affects an organizations ability to perform other critical cyber security tasks such as Risk Managment, Threat Detection and Response, Patch and Vulnerability Management, Incident Response and Compliance management. |
| 3 | Very Low | 0% | Infrastructure Management | Effective infrastructure management ensures that the organization's critical systems and networks are secure. Infrastructure management focuses on maintaining the availability and reliability of systems and networks. It includes tasks such as capacity planning, performance monitoring, fault tolerance, and disaster recovery planning.<br><br>In addition, Infrastructure Management involves implementing security measures such as firewalls, intrusion detection systems, access controls, and encryption to protect against cyber threats. Regular monitoring, patching, and updating of infrastructure components are also a vital role within Infrasturcutre Management in order to address vulnerabilities and stay resilient against emerging risks. |
| 4 | Very Low | 0% | Mitigation and Recovery | A cyber incident, such as a data breach or a ransomware attack, can disrupt business operations and systems. A business resumption plan works in conjunction with an organization's incident response plan. While the incident response plan focuses on the immediate actions to address a cyber incident, the business resumption plan takes a broader perspective and encompasses the recovery and restoration of business operations.<br><br>Business resumption plans are vital to a cyber program because they enable organizations to effectively respond to cyber incidents, minimize downtime, ensure continuity, enhance incident response capabilities, mitigate financial and legal risks, and promote stakeholder confidence. |
| 5 | Very Low | 0% | Monitoring and Analysis | Monitoring and analysis are critical components of any comprehensive cybersecurity program because they help to detect and review potential security threats in a timely manner. The Monitoring and analysis function provides continuous review of network activity, system logs, and other sources of information to detect any signs of suspicious or malicious activity.<br><br>By detecting security threats early, organizations can take immediate action to limit the damage of the potential threat and limit it's impact to the organization. By monitoring and performing analysis of network traffic, system logs, and other data sources, organizations can identify vulnerabilities, understand attack patterns, and make informed decisions |
| 6 | Very Low | 0% | Oversight | Establishing a robust security program is crucial for any organization looking to protect itself against cyber threats. As part of any good cyber program it's important to have a dedicated person responsible for ongoing oversight, such as CISO or Head of Security. A CISO is critical to ensuring that your program is comprehensive, up-to-date and align to mitigate risk.<br><br>Assigning someone oversight to the program ensures that the board or executive team is informed of risk and threats to the business and that the proper strategy is in place to mitigate risk. Equally important to having a CISO to oversee the program is the need to make sure there are clearly assigned security roles and responsibilities to all other members of the security organization. |

| Priority | Current Maturity | Maturity Score | Domain | Why is it Important to Cyber? |
|---|---|---|---|---|
| 7 | Very Low | 0% | Patch Management | Patch management is critical for maintaining the security, stability, and integrity of software systems, protecting against known vulnerabilities, and reducing the risk of cyber attacks.<br><br>Software and operating systems often contain vulnerabilities that can be exploited by cyber attackers. Patches are updates released by software vendors to fix these vulnerabilities and strengthen the security of the software. By promptly applying patches, organizations can protect their systems from known security flaws and reduce the risk of successful cyber attacks. |
| 8 | Very Low | 0% | Response Planning | In today's Cyber world it is not a question of "if" but "when" an attack will occur. To minimize the damage of a Cybersecurity incident requires quick and decisive action. By having an effective incident response planning process in place organizations will minimize the potential damage "when" a cyber incident occurs.<br>A critical part of the response planning process is to develop an incident response plan. Having an incident response plan ensures that organizations have pre-defined processes and procedures to follow when an incident occurs. By having a well-defined and documented plan in place, organizations can respond swiftly and appropriately to incidents, limiting their impact and reducing the time it takes to recover. |
| 9 | Very Low | 0% | Response Testing | Testing of your incident response plan is critical for a cyber program because it helps to identify any weaknesses or gaps in your plan before an actual cyber attack occurs. A common process in response testing is to perform table top tests or walk throughs of a plan which simulate real incident scenarios. By simulating different types of cyber attacks and scenarios, you can evaluate the effectiveness of your incident response plan and ensure that it is comprehensive and well-coordinated. |
| 10 | Very Low | 0% | Risk Assessment | Performing ongoing Risk Assessments are one of the most important part of a cyber program and serves as the foundation to which a strong cyber program. By implementing a risk management strategy, organizations can prioritize risks based on their potential impact and likelihood of occurrence. This allows them to allocate their resources effectively and focus on addressing the most critical risks that could have severe consequences for their operations, reputation, or data. In addition,<br><br>A risk assessment involves evaluating the potential threats that an organization may face, such as malware, phishing attacks, or insider threats. By understanding these threats, organizations can develop appropriate countermeasures and controls to mitigate the risks effectively. Many industries and regulatory frameworks recognize the importance of risk analysis and therfore require organizations to perform risk assessments as part of their compliance obligations. |
| 11 | Very Low | 0% | Third Party Risk | Many organizations rely on third-party vendors for various services, such as cloud computing, software development, data storage, and customer support. These vendors often have access to sensitive data and systems in order to provide services to your organization. Organization's increased use of third-party vendors has resulted in an expanded attack surface for organization's that extend beyond the boundraries of a traditional network.<br><br>Cybercriminals may target these vendors in attempts to gain unauthorized access to your organization's systems or data. Having a mature third-party risk program helps assess the security posture of these vendors and ensures they have appropriate cybersecurity measures in place to protect your data. |
| 12 | Very Low | 0% | Threat Intelligence and Information | Threat intelligence and information plays a crucial role in a security program because it provides valuable information and context about potential threats and adversaries that can be used to improve the organization's security posture.<br><br>By collecting and analysing threat intelligence, security teams can gain insights into the tactics, techniques, and procedures (TTPs) used by cybercriminals, nation-state actors, hacktivists, and other threat actors. This information can be used to identify potential vulnerabilities in the organization's infrastructure, applications, and systems, and to develop effective countermeasures to prevent or mitigate attacks. |
| 13 | Very Low | 0% | Threat and Vulnerability Detection | Threat and vulnerability detection processes such as vulnerability scanning, penetration testing, email security and end point detection controls are essential components of a comprehensive cybersecurity program because they help to identify and mitigate potential security risks before they can be exploited by attackers. This early detection can help organizations respond quickly and prevent damage or loss of a potential cyber threat. Threat and vulnerability detection can help identify and protect critical assets, such as customer data or intellectual property, from cyber-attacks. This protection is particularly important for organizations that rely heavily on their reputation and brand. |
| 14 | Very Low | 0% | Training/Culture | Human error is still a leading cause of security breaches within most organizations. While technology plays a crucial role in cybersecurity protection, people are still an area of weakness in most security programs. An educated and trained employee (AKA "The human firewall") is a critical component to a strong security program. Seventy Percent (70%) of all attacks start with social engineering or phishing of users.<br><br>Employees who are unaware of cybersecurity best practices or who fall for phishing scams can unintentionally compromise their organization's security. Regular security training helps employees understand the importance of cybersecurity and how to protect against threats. In addition, regular phishing testing helps employees recognize the signs of a phishing attack and respond appropriately before they are faced with the real scenario. |

# Cyber Maturity Assessment

## 4. Summary of Recommeded 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 CyberMaturity. These recommendations are list in the order of important to your cyber program.

| Priority | Improvement Domain | Matching SilverSky Services | How Theses Service Helps Improve Maturity |
|---|---|---|---|
| 1 | **Event Detection** | SilverSky Lightning MDR, MEDR | Silversky Lightning services help provide the expert team to help your organization to monitor user activity, detect suspicious behavior, and respond to potential security incidents in a timely manner. Our team are experts in security information and event management (SIEM) and other advanced analytics tools, they can help you to establish a baseline of normal system and network activity, detect deviations, and investigate any suspicious activity. They can also assist with implementing processes to detect unauthorized devices on your network and establishing clear and documented escalation procedures for incident response. |
| 2 | **IT Asset Management** | SilverSky's Insight Services | SilverSky's Insight service is an AI based, cloud agnostic, cyber security platform designed specifically to take the complexity out of vulnerability management while providing visabilityto assets and risk based context to each threat. SilverSky's Insight uses supervised machine learning based on our global attack and threat intelligence database to accurately rate risks and issue immediate alerts and recommendations that prevent potential cyber-attacks. |
| 3 | **Infrastructure Management** | SilverSky ProServ -IT Controls Review, Managed Firewall Service, Firewall Configuration Reviews (QSR), Managed DUO | SilverSky offers a wide array of services to help our customers with the ongoing manangement of their infrastucture through the experties of our security device management teams. In addition, SilverSky's consulting team can provide ongoing controls assessment and configuration health reviews to ensure your infrastructure is keeping pace with security best practices. |
| 4 | **Mitigation and Recovery** | SilverSky MIR, SilverSky ProServices - IR Plan Development | Silversky can help your organization extend beyond traditional SOC operations with the addition of SIlverSky's Managed Incident Response service. SilverSky's MIR services are bundled with all of the key services needed in developing an comprehensive rescovery process. The SilverSKy MIR includes a bundle of Incident Response retainer hours through our Incident response partner, S-RM that will engage upon a declared incident and help implement a business resumption strategy to get your business up an operational as quickly as possible. |
| 5 | **Monitoring and Analysis** | SilverSky Lightning MDR, MEDR | As part of the Silverky Lightning MDR services, the Silversky team works with your organization to ensure we are ingesting the most critical data feeds and the right telemetry into the Lightning platform. Silversky's logging processes for threat detection are also essential in preventing, detecting, and minimizing the impact of a data compromise and providing feedback to help mitigate threats within your environment. SilverSky's lightning MDR takes the burden off your internal resources so that you can ensure that your organization is covered 24/7, meeting compliance and regulatory requirements, minimizing data breaches, and responding quickly to any incidents that occur. |
| 6 | **Oversight** | SilverSky's vCISO Services | SilverSky's vCISO services can assist customer's in managing and maintaining their cyber program at a strategic level by providing seasoned professionals with decades of industry security expertise. SilverSky's vCISO can be used as much or as little as you need them. They can help fill a specific gap or project or be a more consistent resource to help build and manage the growth of your cyber program. |
| 7 | **Patch Management** | SilverSky Partner Network- Patch Management | Effective patch management is crucial to maintaining the security of your systems and reducing the risk of cyberattacks. However, patch management can be a time-consuming and complex process that requires expertise and resources. SilverSky has a vast partner network of IT technology solutions partners. While Silversky focuses on the vulernability and risk remediation part of patch management, we have several partners that offer solutions around patch management. These patch management services when combined with our SilverSky Insight vulnerability management offerings provide a fully outsourced lifecycle solution for our customers. |

| Priority | Improvement Domain | Matching SilverSky Services | How Theses Service Helps Improve Maturity |
|---|---|---|---|
| 8 | **Response Planning** | SilverSky MIR, SilverSky ProServ - IR Plan Development | Silversky can help your organization extend beyond traditional SOC operations with the addition of SIlverSky's Managed Incident Response service. SilverSky's MIR services are bundled with all of the key services needed in developing an comprehensive response process. The SilverSKy MIR service is tighly integrated with our SIlverSKy lighting services to minimize the time to response an engage during an incident. The MIR service includes a customer incident response plan, ongoing table top tests, a bundle of starter IR hours and annual health checks to provide a complete IR service add on. In addition to the SilverSky MIR services, SilverSky's professional services team can help you with the development of an incident response plan. |
| 9 | **Response Testing** | SilverSky MIR, SilverSky ProServ - Table Top Testing | Silversky can help your organization extend beyond traditional SOC operations with the addition of SIlverSky's Managed Incident Response service. SilverSky's MIR services are bundled with all of the key services needed in developing an comprehensive response process. Part of the MIR service bundle includes periodic testing of your IR functions through a online community approach. Through this service, organizations can test their incident response plan to identify weaknesses, improve response times, and minimize the impact of cyber incidents. Testing helps to simulatie various attack scenarios and involvies key parts of your external team, such as SilverSKy's SOC and our partner Incident Response firm, S-RM. This collaboration ensures a coordinated response and identifies potential gaps or weaknesses in the plan. |
| 10 | **Risk Assessment** | SilverSky's ProServ IT Risk Assessment | At SilverSky, we understand that conducting regular risk assessments is a critical component of maintaining a strong security posture. The SilverSky Consulting team can work with your organization to perform a comprehensive IT Risk assessment of your infrastructure to identify any known vulnerabilities and weaknesses and develop risk mitigations places. We will also help you determine whether your current security investments are aligned with your organization's risk profile and provide guidance on necessary security controls. Our risk assessment process takes into account the value of each asset to your organization, as well as the potential impact of any security incidents. This approach enables us to provide clear recommendations for specific security controls that can help mitigate risk and protect your critical assets. |
| 11 | **Third Party Risk** | Third Party Risk Services - Black Kite | At Silversky, we understand that the traditional attack surface has extended way beyond our traditional network perimeters as we rely more and more on third parties. SIlverSky's third party offerings include our professional services teams who can help build a third party progra to ensure you have proper oversight and risk evaluation. In addition, we have partnered with Black Kite, a leader in third party monitoring to provide an ongoing managed service around your third party risk profiles. BlackKite provides the industry's most accurate and comprehensive cyber intelligence, resulting in unparalleled visibility into the risk vendors introduce into our customer environments. |
| 12 | **Threat Intelligence and Information** | SilverSky Lightning MDR, MEDR | Staying informed about the latest cyber threats is critical to maintaining the security of your organization's network and systems. SilverSKy's Lightning services come integrated with both commercial and open source threat intelligence feeds that feeds our services. In addition, as part of the SilverSky MDR services, you benefit from the SilverSky cyber range where our team of data scientists on constantly testing new exploits and threats to add to our artificial intelligence back end. SilverSky security analysts gain valuable insights into emerging threats and tactics used by attackers through our thereat intelligence enrichment of the data. Our team continuously monitors and analyzes these threats to provide proactive threat detection and response, helping to protect your organization against new and evolving cyber threats. |
| 13 | **Threat and Vulnerability Detection** | SilverSky Insight | Silversky can help you through performing regular internal and external vulnerability scans and annual penetration testing of your organization. These services are critical steps in maintaining a strong security posture and identifying potential vulnerabilities that can be exploited by cybercriminals.<br><br>Silversky can assist with it's SilverSky Insight service that t provides vulnerability assessment tools and performance of regular scans to identify and prioritize vulnerabilities in the organization's network, systems, and applications.<br><br>SilverSky's Continuous Validation services can also assist you to enhance maturity of this control by performing deep-level testing combining multiple attack vectors to confirm actual rather than theoretical exploitability of vulnerabilities and misconfigurations present on external devices and critical business systems |
| 14 | **Training/Culture** | SilverSky Aware | Silversky's can reduce the burden of having the continually train and test your staff through SilverSky's Aware service. Powered by the industry leading KnowBe4 knowledge management and phishing platform, SilverSky's team of cyber security experts will provide a fully outsoruced and managed solution while providing strategic guidance to reduce the risk of employees falling victim to phishing threats within your environment. SilverSky's training and testing lifecycle helps employees train on the latest tactics and techniques, Silversky ensures that your organization's "human firewall" is strong and resilient. Then through regular testing, we help your employees build develop better practices to identify and respond to social engineering attacks, including phishing. |