

Risklet Logo

CYBER RISK ASSESSMENT REPORT

Comprehensive Evaluation and Strategic Recommendations
for Enhanced Cybersecurity Posture

Prepared for

SeaComp

Prepared by

Risklet

Date of Report: 2025-06-13

EXECUTIVE SUMMARY

This Cyber Risk Assessment Report provides a comprehensive evaluation of SeaComp's cybersecurity posture. The assessment focused on identifying critical risks, prioritizing mitigation strategies, and aligning practices with internationally recognized frameworks such as CIS CSC v8.1, NIST CSF 2.0, ISO 27001:2022, and regulatory requirements including NIS2, DORA, and GDPR. Conducted by StackSight LLC, the assessment leveraged data provided by representatives of SeaComp, insights from consultancy and industry reports, and threat intelligence sources to deliver actionable guidance tailored to SeaComp's unique operational environment.

Key findings from the assessment reveal several areas where SeaComp faces heightened cybersecurity risks, particularly within the domains of phishing, ransomware, vendor risks, and unpatched software vulnerabilities. These identified risks pose significant threats to operational continuity, sensitive data, and regulatory compliance. The top risks are detailed in the findings section of this report.

To address these challenges effectively, a strategic roadmap comprising targeted safeguards is proposed. Each safeguard is prioritized based on its potential effectiveness in reducing both the likelihood and impact of identified risks. Key recommendations include the deployment of advanced email filtering systems, organization-wide enforcement of multi-factor authentication (MFA), implementation of a comprehensive patch management program, utilization of Endpoint Detection and Response (EDR) tools, ensuring frequent and securely stored data backups, and the establishment of robust vendor security standards coupled with continuous monitoring.

Implementation of these recommendations is projected to yield substantial quantifiable and qualitative benefits for SeaComp, including an estimated 75% reduction in financial exposure stemming from cyber incidents through targeted risk mitigation, increased adherence to relevant regulatory mandates, and enhanced operational continuity with significantly reduced downtime during potential cyber events.

KEY FINDINGS

The assessment revealed several areas where SeaComp faces heightened cybersecurity risks. These risks pose significant threats to operational continuity, sensitive data, and regulatory compliance. The top risks identified are: - **Phishing Attacks:** High likelihood due to reliance on email communication and remote workforce operations.

- **Phishing Attacks:** Assessed with a high likelihood, primarily attributed to the organization's reliance on email communication and the prevalence of remote workforce operations.
 - **Ransomware Incidents:** Evaluated as having an elevated impact, capable of threatening critical data assets and operational systems, potentially causing significant disruption.
 - **Vendor Risks:** Indicating increased exposure resulting from reliance on a substantial number (more-than-5) of third-party vendors without the presence of robust monitoring mechanisms.
 - **Unpatched Software Vulnerabilities:** (Identified as a contributing factor to risks like Ransomware Infection and addressed by recommended controls).
-

RECOMMENDATIONS

To address the identified risks effectively, we propose a strategic roadmap of targeted safeguards. These safeguards are prioritized based on their potential effectiveness in reducing risk likelihood and impact. Key recommendations are categorized by the risks they primarily mitigate:

Phishing Risk Mitigation:

- Deploy advanced email filtering systems to significantly reduce the volume of spam and malicious emails reaching end-users.
- Enforce multi-factor authentication (MFA) organization-wide to secure access to systems and data, adding a critical layer of defense against compromised credentials.
- Conduct regular phishing simulations and comprehensive security awareness training programs to enhance employee vigilance and their ability to identify and report suspicious activity.

Ransomware Prevention and Recovery:

- Implement a comprehensive patch management program to promptly address known software vulnerabilities across all relevant systems and applications.
- Utilize endpoint detection and response (EDR) tools to provide real-time monitoring, detection, and containment capabilities against malicious activities, including ransomware.
- Ensure frequent and verified data backups are performed, stored securely offline or in an immutable state, to enable effective recovery in the event of a ransomware attack or other data loss incidents.

Vendor Risk Management:

- Establish and enforce robust vendor security standards aligned with recognized frameworks such as ISO 27001, requiring third parties to meet defined security requirements.
- Conduct regular third-party risk assessments to evaluate the security posture of vendors, monitor their compliance with established standards, and identify and address potential vulnerabilities introduced through the supply chain.

- Integrate continuous monitoring solutions for vendor activities, particularly those accessing critical systems or sensitive data, to detect and respond to suspicious behavior promptly.

VALUE PROPOSITION

By diligently implementing the recommendations outlined in this report, SeaComp is positioned to achieve significant strategic and operational benefits:

- **Estimated 75% Reduction in Financial Exposure:** Through the targeted mitigation of high-impact cyber risks, the potential financial losses associated with security incidents can be substantially reduced.
- **Increased Compliance with Regulatory Mandates:** Alignment with frameworks such as GDPR, NIS2, and DORA will be enhanced, reducing the risk of non-compliance penalties and reputational damage.
- **Enhanced Operational Continuity and Reduced Downtime:** Proactive risk mitigation and improved incident response capabilities will minimize the likelihood and impact of disruptive cyber events, ensuring business operations remain resilient.

NEXT STEPS

We formally recommend initiating a phased implementation plan to address the identified risks. The initial phase should prioritize the deployment of high-impact safeguards, including organization-wide MFA enforcement, establishing a robust patch management program, and conducting initial vendor risk assessments to address the most pressing risks identified in this report. Concurrently, a structured and regular risk register review cycle should be established to ensure the organization's cybersecurity posture continuously adapts to the evolving threat landscape and changes in the operational environment.

INHERENT LIMITATIONS

This assessment, while conducted with due professional care and based on available information, is subject to certain inherent limitations that warrant explicit mention:

Dynamic Nature of Cyber Threats:

The landscape of cybersecurity threats is inherently dynamic, characterized by rapid advancements in attack techniques, continuous changes in technology, and the emergence of new vulnerabilities. This report represents a "point-in-time" snapshot of the organization's risk landscape as assessed on the report date and does not account for changes or new threats that may materialize subsequent to the assessment. Regular, periodic updates to the risk assessment are therefore crucial to ensure the organization remains resilient against emerging threats.

For instance, a phishing risk rated as medium during this assessment could potentially escalate rapidly in severity due to unforeseen external factors, such as a sudden surge in highly sophisticated targeted attacks specifically directed at the healthcare industry.

Focus on Risk Management Frameworks:

This assessment adopts a risk-based approach, aligning findings and recommendations with established international frameworks such as ISO 27001, CIS CSC v8.1, NIST CSF 2.0, and relevant regulatory requirements including GDPR, NIS2, PCI DSS, and DORA. While these frameworks provide a comprehensive basis for cybersecurity governance, they are not exhaustive. The recommendations provided are tailored to SeaComp's specific organizational priorities and risk tolerances; however, it is important to acknowledge that residual risks will inevitably remain even after the implementation of recommended controls. Residual risk is an inherent characteristic of any risk management approach.

Residual Risk:

Residual risk is formally defined as the level of risk that persists after the implementation of all feasible and recommended controls. By way of example, while the implementation of multi-factor authentication (MFA) is highly effective in significantly reducing phishing risks, a small degree of

residual risk may still persist due to factors such as potential human error or the emergence of novel attack vectors not fully mitigated by current controls.

Scope and Context:

This report is an organization-level assessment, emphasizing risks related to strategic and operational cybersecurity governance. It does not provide a system-level evaluation (e.g., penetration testing or vulnerability scanning) or an asset-level analysis of specific infrastructure components, devices, or applications.

For a more detailed understanding of individual systems or assets, supplementary assessments, such as technical audits, vulnerability scans, or penetration tests, are recommended.

Control Maturity Assumptions:

Residual risk calculations presented in this report are predicated on the assumption that all recommended controls are implemented and maintained at the highest achievable maturity levels (e.g., aligned with CMMI Level 5 principles for process management). However, the actual maturity level of implemented controls within SeaComp may vary in practice, influenced by factors such as available resources, implementation timelines, and the effectiveness of ongoing maintenance and operational efforts.

For example, while a comprehensive patch management program is designed to significantly reduce software vulnerabilities, its ultimate effectiveness is directly dependent on operational factors such as the frequency and timeliness of patch deployment and adherence to established organizational policies and procedures.

Scope of External Factors:

While this assessment focuses primarily on internal cybersecurity risks that are largely within SeaComp's direct control, it does not encompass an evaluation of broader external factors that could potentially impact the organization's risk profile. These external factors may include, but are not limited to, geopolitical risks, the impact of natural disasters on infrastructure, or systemic vulnerabilities inherent within wider third-party ecosystems beyond SeaComp's immediate vendor relationships.

Dependency on Timely Implementation:

The effectiveness of the recommendations provided in this report in reducing risk is directly dependent upon the timely and effective implementation of the proposed controls. Delays in implementation, partial adoption of recommendations, or inadequate ongoing maintenance of controls may result in higher residual risks than those estimated in this assessment.

For instance, a delayed adoption and operationalization of endpoint detection and response (EDR) tools could leave the organization exposed to the full impact of ransomware attacks for a longer duration than would otherwise be necessary.

Regular Reassessment Requirement:

This report serves as a baseline assessment of SeaComp's cybersecurity risks at a specific point in time. Given the dynamic nature of cyber threats, continuous changes in technology, and evolving business processes, we formally recommend periodic reassessments of the cybersecurity risk landscape. Such reassessments are essential to keep the risk register updated, ensure alignment with the evolving threat environment, and validate the effectiveness of implemented controls.

A risk initially identified as low severity at the time of this report might increase significantly in severity over time due to changes in prevalent attack vectors, shifts in the regulatory environment, or organizational growth and expansion.

APPROACH AND METHODOLOGIES

Methodology Overview

The risk assessment methodology employed in the preparation of this report is formally rooted in the principles and guidance outlined in the NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments. This widely recognized standard defines risk as a function of the likelihood of a threat exploiting a vulnerability and the resulting impact. This methodology is broadly adopted across industries due to its scalability and inherent alignment with organizational risk management needs. The approach is also compliant with key international standards and frameworks, including ISO 27001, ISO 31000, PCI DSS, ENISA guidelines, and the CSA Cloud Controls Matrix (CCM), by focusing on the following common key elements:

1. **Risk Identification:** The systematic process of identifying potential threats, existing vulnerabilities, and the potential adverse impacts that could result from a cybersecurity event.
2. **Risk Assessment:** The formal evaluation of identified risks, involving the determination of both the likelihood of occurrence and the severity of the potential impact.
3. **Risk Mitigation/Treatment:** The process of selecting and implementing appropriate strategies and controls to reduce, transfer, or formally accept identified risks based on organizational risk tolerance.
4. **Documentation:** Maintaining a detailed and accurate record of the entire risk assessment process, including methodologies, findings, analysis, and treatment decisions.
5. **Continuous Monitoring:** Establishing ongoing processes to monitor the risk environment, assess the effectiveness of implemented controls, and identify new risks as they emerge.
6. **Communication:** Ensuring that risk findings, assessment results, and treatment plans are effectively communicated to relevant stakeholders across the organization.

Inputs and Data Collection

This assessment was specifically tailored to SeaComp's operational context using a combination of internal data and external threat intelligence. The primary inputs from SeaComp included:

- **Organizational Scale:** Data pertaining to employee headcount and annual revenue, providing context for potential financial impact calculations.
- **Technology Landscape:** Information on critical applications, network architecture, and segmentation, informing the identification of technical vulnerabilities and dependencies.
- **Regulatory Frameworks:** Details on applicable regulatory requirements and compliance obligations, such as GDPR, ISO 27001, and NIST CSF compliance status.
- **Operational Context:** Information regarding the industry sector in which SeaComp operates and the extent of its reliance on third-party vendors, informing the assessment of sector-specific and supply chain risks.

These internal insights were further enriched by incorporating relevant data and trend analysis from leading industry and consultancy sources.

RISK ASSESSMENT PROCESS - SCALES

For determining likelihood, StackSight LLC utilizes a commonly referenced scale, presented below:

LIKELIHOOD SCORE	PROBABILITY OF HAPPENING IN A YEAR	DESCRIPTOR	CRITERIA
1	0-10%	Rare	Has never occurred or has not occurred in the prior 10 years. Highly unlikely, but it may occur in exceptional circumstances. It could happen, but probably never will.
2	11-24%	Unlikely	Has occurred in the past 10 to 4 years. Not expected, but there's a slight possibility it may occur at some time.
3	25-50%	Probable	Has occurred in the past 4 to 2 years. The event might occur at some time as there is a history of casual occurrence at similar organizations.
4	51-89%	Likely	Has occurred in the past 2 to 1 years. There is a strong probability the event will occur as there is a history of frequent occurrence at similar organizations.
5	90-100%	Almost Certain	Currently occurs or has occurred in the last year. The event is expected to occur in most circumstances as there is a history of regular occurrence at similar organizations.

The risk impact is formally scored using the following definitions and corresponding operational recovery metrics (RPO/RT0):

IMPACT/ SEVERITY	COST	REPUTATION (INTERNAL & EXTERNAL)	MANAGEMENT EFFORT	OPERATIONAL RESOURCES	COMPLIANCE/ SOX/CRA/ NIS2 IMPACT
Insignificant (1)	0% to .04% of Gross Revenue	Unaware - A reasonable person does not have knowledge of the situation or fact. Additionally there is no obligation to divulge the incident.	Normal Activity - Usual, average or typical company processes. Typically no extra managements cumulative time needed.	Additional Resources - No extra Internal or External personnel needed to bring resolution to the issue outside of normal processes.	Low direct regulatory implications. Baseline operational obligations and internal controls are expected to be maintained.
Significant (2)	~.05% to .25% Gross Revenue	Minimum Concern - If a reasonable person obtains knowledge of the situation or fact and there is no reaction either positive or negative. Additionally, there is no obligation to divulge the incident.	Minimum Management Effort - 1-10hrs of managements cumulative time.	Minor Operational Resources - Internal or External personnel may be needed to bring resolution to the issue, typically 4-40hrs worth of cumulative time.	Primarily an internal control issue. Notification to designated authorities may be required. Potential for initial warnings or minor penalties depending on the nature.

IMPACT/ SEVERITY	COST	REPUTATION (INTERNAL & EXTERNAL)	MANAGEMENT EFFORT	OPERATIONAL RESOURCES	COMPLIANCE/ SOX/CRA/ NIS2 IMPACT
Severe (3)	~.25% to .5% Gross Revenue	Moderate Concern – A reasonable person obtain knowledge of the situation that could violate, laws, regulations or compliance but the narrative is that management is in control and are rectifying the situation appropriately.	Moderate Management Effort - 10 to 20 hrs. of managements cumulative time.	Moderate Operational Resources - Internal or External personnel may be needed to bring resolution to the issue, typically 40 - 80hrs (2 weeks) worth of cumulative time.	A clear deviation from expected operational or product/ service standards, requiring notification and remediation actions. Mandatory reporting to authorities. Risk of financial penalties and increased regulatory scrutiny.

IMPACT/ SEVERITY	COST	REPUTATION (INTERNAL & EXTERNAL)	MANAGEMENT EFFORT	OPERATIONAL RESOURCES	COMPLIANCE/ SOX/CRA/ NIS2 IMPACT
Material (4)	~ .5% to 1% Gross Revenue	Severe Concern – A reasonable person obtains knowledge of the situation that could violate, laws, regulations or compliance and the narrative is that management is acting in a negligent manner to rectify the situation.	Severe Management Effort - 20 to 40hrs of managements cumulative time	Severe Operational Resources - Internal or External personnel may be needed to bring resolution to the issue, typically 80hrs (2 weeks) - 160hrs (4 weeks) worth of cumulative time.	Serious non- compliance with established standards. Risk of significant operational disruptions, including potential product/ service restrictions or recalls. Mandatory and detailed reporting to authorities is required. High likelihood of substantial financial penalties, potential suspension of services, and personal accountability for responsible management.

IMPACT/ SEVERITY	COST	REPUTATION (INTERNAL & EXTERNAL)	MANAGEMENT EFFORT	OPERATIONAL RESOURCES	COMPLIANCE/ SOX/CRA/ NIS2 IMPACT
Major (5)	~ 1% Gross Revenue	Outrage from a reasonable person – A reasonable person obtains knowledge of the situation that violates, laws, regulations or compliance and the narrative is that management is acting in a negligent manner to rectify the situation or is not rectifying the situation.	Precarious Management Effort - 40hrs or more of managements cumulative time, potential management will be removed from their position.	Precarious Operational Resources - Internal or External personnel may be needed to bring resolution to the issue over 160 hrs. (4 weeks) worth of cumulative time.	Systemic failure with severe consequences. Significant regulatory sanctions expected. Mandatory, multi-stage, and comprehensive reporting to authorities is required. Maximum financial penalties are likely, with potential for temporary prohibition of managerial functions and other stringent enforcement actions. The possibility of criminal liability may be considered depending on applicable law or regulation.

The specific definition of material impact is contingent upon the organizational type and scale. For companies exceeding 1 billion USD in annual revenue, the materiality threshold for major impact is set at 1% of annual revenue. For organizations below this revenue threshold, it is set at 10%. For non-profit organizations, alternative, pre-defined guidelines are utilized.

RISK MATRIX

The Risk Score is calculated as the product of the Inherent Impact Score and the Inherent Likelihood Score.

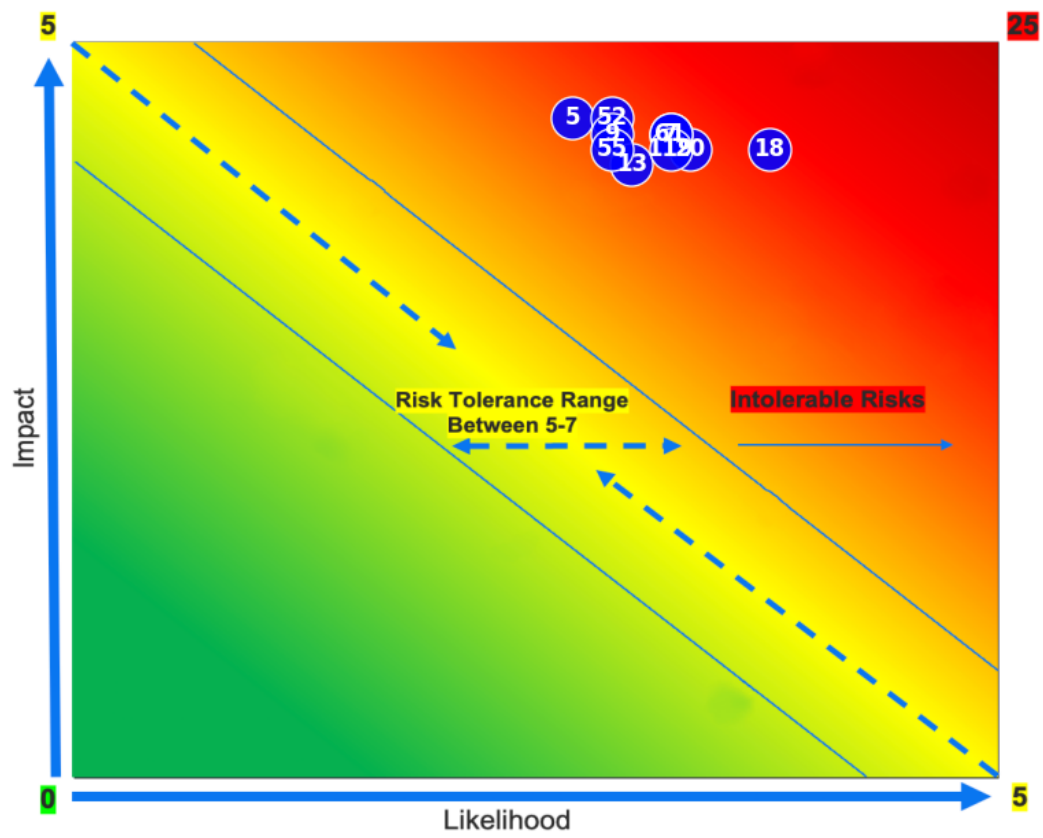
Likelihood ↓ / Impact →	Insignificant (1)	Significant (2)	Severe (3)	Material (4)	Major (5)
Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Probable (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Rare (1)	1	2	3	4	5

Risk Tolerance Range: Scores between 5 and 7 are generally considered within the acceptable risk tolerance range for capcarap, subject to formal acceptance by leadership.

Intolerable Risks: Risks with scores of 8 or above are formally classified as intolerable and require immediate treatment.

Risk Matrix Visualization - Inherent Risk

The chart below visually represents the inherent risk scores of the top 10 identified risks based on their Inherent Likelihood and Impact, mapped onto the risk matrix gradient. The size of the marker indicates the number of risks at that specific Likelihood/Impact intersection.



RESULTS AND RECOMMENDATIONS

Organizational Context:

SeaComp operates within the technology sector, employing 251-1000 personnel and annual revenues estimated to be between 250m-1b. The organization exhibits a major dependency on technology for its core operations and service delivery. The operational environment is subject to stringent regulatory mandates including but not limited to ['sox', 'cmmc']. These regulatory requirements underscore the critical need for robust and demonstrable cybersecurity governance and controls.

Top 10 Risks Identified:

Based on the comprehensive assessment methodology applied, the following top 10 cybersecurity risks have been formally identified and prioritized for SeaComp based on their inherent risk scores:

RISK ID	RISK NAME	INHERENT IMPACT	INTERENT LIKLIHOOD	INHERENT RISK SCORE	DESCRIPTION OF RISK
18	Ransomware Infection	4	4	16	
20	Cloud Provider Service Outage	4	4	16	
5	SSL Certificate Private Key Exposure	5	3	15	
52	Managed Service Provider Breach	5	3	15	
7	Misconfigured Cloud Services	4	3	12	
9	Source Code Exposure	4	3	12	
13	Third Party Code Compromise	4	3	12	
55	Data Center Power Event	4	3	12	
61	Privacy Regulation Violation	4	3	12	
119	Zero-Trust Architecture Bypass	4	3	12	

Each identified risk has been assigned an inherent impact and likelihood score, which are then used to calculate the inherent risk score. These risks are visually represented on the risk matrix chart to facilitate prioritization and understanding of their relative positions within the risk landscape.

RISKS WITH RESIDUALS

Risk Treatment Plan:

To effectively address the identified risks, a comprehensive risk treatment plan is formally proposed. This plan prioritizes the implementation of controls based on their assessed capacity to reduce the inherent risk. Standard risk treatment strategies considered include:

1. **Mitigation:** Implementing specific safeguards and controls designed to reduce the likelihood of a risk event occurring or minimize its potential impact.
2. **Avoidance:** Making a conscious decision to refrain from engaging in activities or adopting architectures that introduce a specific high-level risk.
3. **Transference:** Shifting the financial or operational impact of a risk to a third party, typically through mechanisms such as cybersecurity insurance or contractual agreements with vendors.
4. **Acceptance:** An informed decision by organizational leadership to acknowledge a specific risk and choose not to implement further controls, based on a formal assessment that the residual risk is within acceptable tolerance levels.

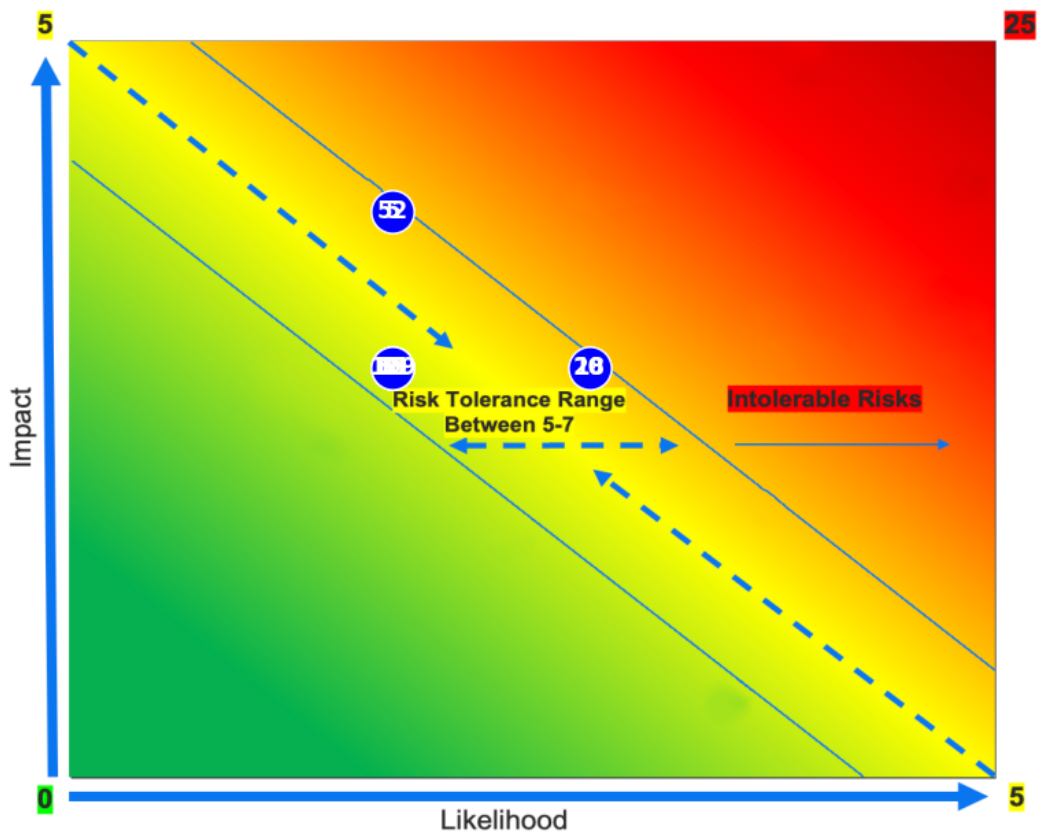
Where the implementation of controls is assessed as feasible and effective, all risks should be formally treated. Based on the established risk assessment procedure, any risk with an inherent risk score of 8 or above is formally classified as intolerable and must be treated in a timely and prioritized manner to reduce it to an acceptable residual level.

Prior to formally considering the acceptance of any risk, a rigorous evaluation must be conducted to ensure that the risk has been reduced to the smallest possible residual level through the application of one or more appropriate risk treatment approaches.

RISK ID	RISK NAME	INHERENT IMPACT	INHERENT LIKELIHOOD	INHERENT RISK SCORE	RESIDUAL IMPACT	RESIDUAL LIKELIHOOD	RESIDUAL RISK SCORE
18	Ransomware Infection	4	4	16	3	3	9
20	Cloud Provider Service Outage	4	4	16	3	3	9
5	SSL Certificate Private Key Exposure	5	3	15	4	2	8
52	Managed Service Provider Breach	5	3	15	4	2	8
7	Misconfigured Cloud Services	4	3	12	3	2	6
9	Source Code Exposure	4	3	12	3	2	6
13	Third Party Code Compromise	4	3	12	3	2	6
55	Data Center Power Event	4	3	12	3	2	6
61	Privacy Regulation Violation	4	3	12	3	2	6
119	Zero-Trust Architecture Bypass	4	3	12	3	2	6

RISK MATRIX VISUALIZATION - RESIDUAL RISK

The chart below visually represents the residual risk scores of the top 10 identified risks based on their Residual Likelihood and Impact after applying proposed mitigating controls. The size of the marker indicates the number of risks at that specific Likelihood/Impact intersection.



FRAMEWORK ALIGNMENT

CIS Critical Security Controls (CSC) v8.1:

The CIS Critical Security Controls (CSC) v8.1 is a globally recognized, prioritized set of cybersecurity best practices designed to help organizations improve their cyber defenses against known attack vectors. Developed by the Center for Internet Security (CIS), the framework provides a structured approach to implementing and managing essential cybersecurity safeguards. CIS CSC v8.1 consists of 18 top-level Controls, each supported by a set of Safeguards (formerly known as Sub-Controls). The framework is designed to be actionable and provide a clear path for organizations of varying sizes and complexities to enhance their cybersecurity posture effectively.

NIST Cybersecurity Framework (CSF) 2.0:

The NIST Cybersecurity Framework (CSF) 2.0 provides a structured and flexible approach for organizations to understand, manage, reduce, and communicate cybersecurity risks. Developed by the National Institute of Standards and Technology (NIST), CSF 2.0 maintains the core structure of its predecessor but introduces enhancements, including a new Govern function to emphasize cybersecurity governance. The framework is organized around six key functions that represent the lifecycle of managing cybersecurity risk: Identify, Govern, Protect, Detect, Respond, and Recover. CSF 2.0 is designed to be adaptable to various technologies and sectors, providing a common language for internal and external stakeholders to discuss and manage cybersecurity risks effectively.

Cybersecurity Capability Maturity Levels (CMMI Adaptation):

The table below presents an assessment of the organization's cybersecurity capabilities across key functions derived from the NIST CSF 2.0, mapped against maturity levels adapted from the Capability Maturity Model Integration (CMMI) framework. These levels describe a progression from initial, chaotic processes (Level 1) to optimized, continuously improving processes (Level 5).

NIST CSF 2.0 FUNCTION	LEVEL 1 (INITIAL)	LEVEL 2 (MANAGED)	LEVEL 3 (DEFINED)	LEVEL 4 (QUANTITATIVELY MANAGED)	LEVEL 5 (OPTIMIZING)
Govern	Reactive and ad hoc.	Nascent and unreliable.	Established, predictable, reliable.	Provides direction and shapes program.	Key pillar, known and reportable state.
Identify	Little to no identification.	Immature process.	Standard, well-defined process.	Proactively monitored periodically.	Continuously monitored, incorporated into business decisions.
Protect	Reactive and ad hoc.	Implemented across environment.	Formally defined, protected in accordance with classification.	Proactively monitored via protective technologies.	Operationalized through automation and advanced technologies.
Detect	Not detected timely.	Established through tools and procedures.	Baseline of 'normal' activity established and applied.	Continuous monitoring program established for real-time threats.	Continuously learning behaviors and adjusting capabilities.
Respond	Reactive or non-existent.	Reactive or non-existent.	Analysis capabilities applied consistently by IR roles.	IR Plan defines steps for preparation, analysis, containment, eradication, post-incident.	Times and impacts monitored and minimized.
Recover	Applied consistently to incidents impacting business operations.	Continuity & Disaster Recovery Plan defines steps to continue critical functions and resume operations.	Recovery times and impacts monitored and minimized.	Capabilities of all IT personnel, procedures, technologies regularly tested and updated.	Capabilities of all IT personnel, procedures, technologies regularly tested and updated.

INDUSTRY AND CONSULTANCY BENCHMARKS

The insights and analysis presented in this report were informed by incorporating data and trend analysis from leading industry and consultancy publications. These sources provide valuable context regarding prevalent threats, attack methodologies, and effective control strategies observed across various sectors.

RISKS WITH MITIGATING CONTROLS

The following section details the top identified risks and lists relevant mitigating controls. The controls are referenced using their corresponding CIS CSC v8.1 identifier and are assigned a weight indicating their relative effectiveness or importance in mitigating the specific risk. Controls are listed in numerical order by Safeguard ID.

Risk: Ransomware Infection

Mitigating Controls:

- Allowlist Authorized Software - Weight: 5
- Securely Manage Enterprise Assets and Software - Weight: 5
- Require MFA for Externally-Exposed Applications - Weight: 5
- Establish and Maintain a Remediation Process - Weight: 4
- Standardize Time Synchronization - Weight: 4
- Ensure Use of Only Fully Supported Browsers and Email Clients - Weight: 3
- Deploy and Maintain Anti-Malware Software - Weight: 5
- Establish and Maintain a Data Recovery Process - Weight: 4
- Deploy a Host-Based Intrusion Detection Solution - Weight: 5
- Train Workforce on Data Handling Best Practices - Weight: 4

Risk: Cloud Provider Service Outage

Mitigating Controls:

- Establish and Maintain a Data Inventory - Weight: 5
- Establish and Maintain a Data Classification Scheme - Weight: 5
- Use Unique Passwords - Weight: 3
- Require MFA for Externally-Exposed Applications - Weight: 5
- Establish and Maintain a Vulnerability Management Process - Weight: 4
- Establish and Maintain a Data Recovery Process - Weight: 5
- Perform Automated Backups - Weight: 5
- Ensure Network Infrastructure is Up-to-Date - Weight: 4
- Establish and Maintain a Service Provider Management Policy - Weight: 4
- Monitor Service Providers - Weight: 4

Risk: SSL Certificate Private Key Exposure

Mitigating Controls:

- Encrypt Sensitive Data in Transit - Weight: 5

- Require MFA for Externally-Exposed Applications - Weight: 4
- Establish and Maintain a Vulnerability Management Process - Weight: 4
- Perform Automated Application Patch Management - Weight: 5
- Establish and Maintain a Secure Network Architecture - Weight: 5
- Use of Secure Network Management and Communication Protocols - Weight: 4
- Train Workforce Members to Recognize Social Engineering Attacks - Weight: 4
- Establish and Maintain a Secure Application Development Process - Weight: 5
- Use Standard Hardening Configuration Templates for Application Infrastructure - Weight: 5
- Designate Personnel to Manage Incident Handling - Weight: 5

Risk: Managed Service Provider Breach

Mitigating Controls:

- Establish and Maintain Detailed Enterprise Asset Inventory - Weight: 5
- Allowlist Authorized Software - Weight: 4
- Require MFA for Externally-Exposed Applications - Weight: 5
- Establish and Maintain a Vulnerability Management Process - Weight: 5
- Establish and Maintain a Data Recovery Process - Weight: 4
- Establish and Maintain an Inventory of Service Providers - Weight: 4
- Ensure Service Provider Contracts Include Security Requirements - Weight: 5
- Establish and Maintain a Secure Application Development Process - Weight: 5
- Train Developers in Application Security Concepts and Secure Coding - Weight: 5
- Establish and Maintain Contact Information for Reporting Security Incidents - Weight: 4

Risk: Misconfigured Cloud Services

Mitigating Controls:

- Establish and Maintain Detailed Enterprise Asset Inventory - Weight: 5
- Address Unauthorized Software - Weight: 4
- Establish and Maintain a Secure Configuration Process - Weight: 5
- Implement and Manage a Firewall on Servers - Weight: 4
- Securely Manage Enterprise Assets and Software - Weight: 4
- Require MFA for Externally-Exposed Applications - Weight: 4
- Establish and Maintain a Vulnerability Management Process - Weight: 5
- Establish and Maintain a Secure Application Development Process - Weight: 5
- Conduct Application Penetration Testing - Weight: 5
- Designate Personnel to Manage Incident Handling - Weight: 4

Risk: Source Code Exposure

Mitigating Controls:

- Establish and Maintain an Inventory of Service Accounts - Weight: 4
- Require MFA for Externally-Exposed Applications - Weight: 4
- Require MFA for Administrative Access - Weight: 4
- Establish and Maintain a Vulnerability Management Process - Weight: 5
- Establish and Maintain a Security Awareness Program - Weight: 5
- Assess Service Providers - Weight: 5
- Establish and Maintain a Secure Application Development Process - Weight: 5
- Train Developers in Application Security Concepts and Secure Coding - Weight: 4
- Leverage Vetted Modules or Services for Application Security Components - Weight: 4
- Implement Code-Level Security Checks - Weight: 5

Risk: Third Party Code Compromise

Mitigating Controls:

- Address Unauthorized Software - Weight: 4
- Allowlist Authorized Libraries - Weight: 5
- Establish and Maintain a Remediation Process - Weight: 4
- Standardize Time Synchronization - Weight: 3
- Establish and Maintain a Security Awareness Program - Weight: 5
- Assess Service Providers - Weight: 4
- Establish and Maintain a Secure Application Development Process - Weight: 5
- Use Up-to-Date and Trusted Third-Party Software Components - Weight: 4
- Apply Secure Design Principles in Application Architectures - Weight: 4
- Implement Code-Level Security Checks - Weight: 5

Risk: Data Center Power Event

Mitigating Controls:

- Establish and Maintain Detailed Enterprise Asset Inventory - Weight: 5
- Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory - Weight: 3
- Encrypt Sensitive Data in Transit - Weight: 4
- Implement and Manage a Firewall on Servers - Weight: 4
- Require MFA for Externally-Exposed Applications - Weight: 5
- Establish and Maintain a Vulnerability Management Process - Weight: 5
- Establish and Maintain a Data Recovery Process - Weight: 5
- Establish and Maintain a Secure Network Architecture - Weight: 4
- Establish and Maintain a Security Awareness Program - Weight: 4
- Designate Personnel to Manage Incident Handling - Weight: 5

Risk: Privacy Regulation Violation

Mitigating Controls:

- Establish and Maintain a Data Management Process - Weight: 5
- Encrypt Sensitive Data in Transit - Weight: 5
- Segment Data Processing and Storage Based on Sensitivity - Weight: 5
- Separate Enterprise Workspaces on Mobile End-User Devices - Weight: 4
- Require MFA for Externally-Exposed Applications - Weight: 5
- Perform Automated Application Patch Management - Weight: 4
- Deploy and Maintain Anti-Malware Software - Weight: 5
- Train Workforce Members to Recognize Social Engineering Attacks - Weight: 4
- Perform Root Cause Analysis on Security Vulnerabilities - Weight: 4
- Apply Secure Design Principles in Application Architectures - Weight: 4

Risk: Zero-Trust Architecture Bypass

Mitigating Controls:

- Address Unauthorized Assets - Weight: 5
 - Allowlist Authorized Software - Weight: 4
 - Restrict Administrator Privileges to Dedicated Administrator Accounts - Weight: 4
 - Require MFA for Externally-Exposed Applications - Weight: 5
 - Require MFA for Remote Network Access - Weight: 5
 - Perform Automated Vulnerability Scans of Internal Enterprise Assets - Weight: 4
 - Ensure Use of Only Fully Supported Browsers and Email Clients - Weight: 3
 - Establish and Maintain a Secure Network Architecture - Weight: 5
 - Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities - Weight: 5
 - Conduct Application Penetration Testing - Weight: 4
-

CIS CONTROL SAFEGUARD SUMMARY

The following table summarizes the CIS Control Safeguards referenced as mitigating controls for the identified risks and indicates the number of times each safeguard was listed across all risk mitigation sections. Safeguards are listed by their reference number and description, grouped by their respective CIS Control.

CONTROL ID	CONTROL NAME	SAFEGUARD ID	DESCRIPTION	COUNT
47	Access Control Management	6.3	Require MFA for Externally-Exposed Applications	9
53	Continuous Vulnerability Management	7.1	Establish and Maintain a Vulnerability Management Process	6
126	Application Software Security	16.1	Establish and Maintain a Secure Application Development Process	5
86	Data Recovery	11.1	Establish and Maintain a Data Recovery Process	4
10	Inventory and Control of Software Assets	2.5	Allowlist Authorized Software	3
22	Data Protection	3.10	Encrypt Sensitive Data in Transit	3
92	Network Infrastructure Management	12.2	Establish and Maintain a Secure Network Architecture	3
140	Incident Response Management	17.1	Designate Personnel to Manage Incident Handling	3
1	Inventory and Control of Enterprise Assets	1.1	Establish and Maintain Detailed Enterprise Asset Inventory	3
110	Security Awareness and Skills Training	14.1	Establish and Maintain a Security Awareness Program	3

32	Secure Configuration of Enterprise Assets and Software	4.6	Securely Manage Enterprise Assets and Software	2
54	Continuous Vulnerability Management	7.2	Establish and Maintain a Remediation Process	2
63	Audit Log Management	8.4	Standardize Time Synchronization	2
72	Email and Web Browser Protections	9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	2
79	Malware Defenses	10.1	Deploy and Maintain Anti-Malware Software	2
56	Continuous Vulnerability Management	7.4	Perform Automated Application Patch Management	2
111	Security Awareness and Skills Training	14.2	Train Workforce Members to Recognize Social Engineering Attacks	2
134	Application Software Security	16.9	Train Developers in Application Security Concepts and Secure Coding	2
8	Inventory and Control of Software Assets	2.3	Address Unauthorized Software	2
30	Secure Configuration of Enterprise Assets and Software	4.4	Implement and Manage a Firewall on Servers	2

138	Application Software Security	16.13	Conduct Application Penetration Testing	2
123	Service Provider Management	15.5	Assess Service Providers	2
137	Application Software Security	16.12	Implement Code-Level Security Checks	2
135	Application Software Security	16.10	Apply Secure Design Principles in Application Architectures	2
100	Network Monitoring and Defense	13.2	Deploy a Host-Based Intrusion Detection Solution	1
113	Security Awareness and Skills Training	14.4	Train Workforce on Data Handling Best Practices	1
14	Data Protection	3.2	Establish and Maintain a Data Inventory	1
19	Data Protection	3.7	Establish and Maintain a Data Classification Scheme	1
40	Account Management	5.2	Use Unique Passwords	1
87	Data Recovery	11.2	Perform Automated Backups	1
91	Network Infrastructure Management	12.1	Ensure Network Infrastructure is Up-to-Date	1
120	Service Provider Management	15.2	Establish and Maintain a Service Provider Management Policy	1

124	Service Provider Management	15.6	Monitor Service Providers	1
96	Network Infrastructure Management	12.6	Use of Secure Network Management and Communication Protocols	1
132	Application Software Security	16.7	Use Standard Hardening Configuration Templates for Application Infrastructure	1
119	Service Provider Management	15.1	Establish and Maintain an Inventory of Service Providers	1
122	Service Provider Management	15.4	Ensure Service Provider Contracts Include Security Requirements	1
141	Incident Response Management	17.2	Establish and Maintain Contact Information for Reporting Security Incidents	1
27	Secure Configuration of Enterprise Assets and Software	4.1	Establish and Maintain a Secure Configuration Process	1
43	Account Management	5.5	Establish and Maintain an Inventory of Service Accounts	1
49	Access Control Management	6.5	Require MFA for Administrative Access	1

136	Application Software Security	16.11	Leverage Vetted Modules or Services for Application Security Components	1
11	Inventory and Control of Software Assets	2.6	Allowlist Authorized Libraries	1
130	Application Software Security	16.5	Use Up-to-Date and Trusted Third-Party Software Components	1
4	Inventory and Control of Enterprise Assets	1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	1
13	Data Protection	3.1	Establish and Maintain a Data Management Process	1
24	Data Protection	3.12	Segment Data Processing and Storage Based on Sensitivity	1
38	Secure Configuration of Enterprise Assets and Software	4.12	Separate Enterprise Workspaces on Mobile End-User Devices	1
128	Application Software Security	16.3	Perform Root Cause Analysis on Security Vulnerabilities	1
2	Inventory and Control of Enterprise Assets	1.2	Address Unauthorized Assets	1

42	Account Management	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	1
48	Access Control Management	6.4	Require MFA for Remote Network Access	1
57	Continuous Vulnerability Management	7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	1
131	Application Software Security	16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	1

Note: The mapping of Safeguard IDs to CIS v8 Control Titles is based on the most relevant control description in CIS v8. Some Safeguard IDs in the source document may not align perfectly with the numbering conventions of the current CIS v8 framework.

CONTINUOUS IMPROVEMENT

Cybersecurity is formally recognized as a continuous journey, not a static destination. To effectively adapt to the evolving threat landscape and changes in the operational environment, SeaComp should establish processes for regular risk register reviews and cybersecurity maturity assessments. Implementing a structured cybersecurity improvement roadmap will ensure that controls remain effective, are continuously optimized, and remain aligned with organizational priorities and strategic objectives.

The risk register should be reviewed and updated on a regular, defined cycle. This review process must include a formal re-assessment of existing risks based on identified changes to organizational information systems, the environments in which the systems operate (change monitoring), and changes in the feasibility or effectiveness of ongoing risk response measures. Risks that have been formally accepted should also be re-evaluated during each cycle to confirm that the residual risk remains within acceptable tolerance levels. Concerted efforts should be made to optimize risk response measures where feasible, aiming for continuous reduction of residual risk.

Risklet Logo

Disclaimer

This report is provided for informational purposes only and is based on the data and information available to StackSight LLC at the time of the assessment. The findings and recommendations contained herein are intended solely to provide guidance to SeaComp in enhancing its cybersecurity posture. Cybersecurity risks are inherently dynamic and subject to continuous evolution. StackSight LLC makes no warranties, express or implied, regarding the completeness, accuracy, or suitability of this report for any specific purpose or outcome. The implementation of the recommendations outlined in this report does not constitute a guarantee of complete protection against all potential cyber threats or incidents.

SeaComp assumes full responsibility for all decisions made based on the content of this report and for the implementation, ongoing management, and effectiveness of its cybersecurity controls and risk management program. This report should not be construed as, nor relied upon as, legal or regulatory advice.