| Prepared For: City of Saint Paul Alaska
| Validated By: FRSecure LLC

S2ORG
Powered by S2SCORE

Executive Summary Report

NOTE: The physical phase of the assessment was based on interview and did not include a physical walkthrough.

| Date: October 3, 2024

City of Saint Paul Alaska Overall Results

The overall S2SCORE (or risk rating) is **597.28.**

The S2SCORE represents a comprehensive, authoritative, and objective information security risk value. The S2SCORE enables business leaders to quickly identify and relate to the amount of information security risk that is present in their organization, and a S2SCORE also allows the organization to succinctly communicate the level of risk to interested third-parties.

A S2SCORE of **597.28** translates to "**Poor**". A detailed explanation of the S2SCORE and further definition of its meaning can be found in the S2SCORE Full Report. The S2SCORE is calculated in a range from 300 to 850. The lower the score, the higher the risk and vice versa. A S2SCORE of **660.00** or "**Good**" is acceptable to most organizations and should be the goal for City of Saint Paul Alaska.

S2SCORE Scale

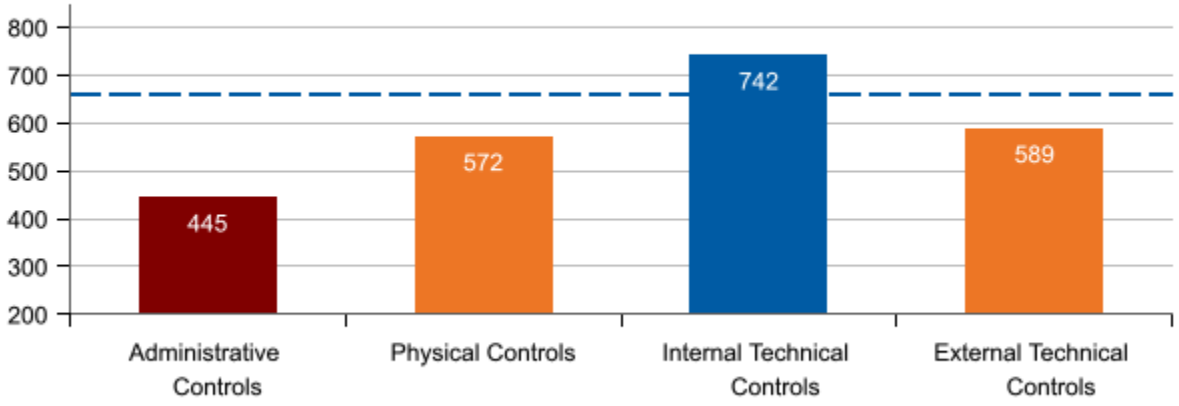
S2SCORE Average Across Industries

Industry: Local Government, excluding schools and hospitals (OES Designation)(999300)

The average third-party validated S2SCORE is **606.66** for this NAICS industry (North American Industry Classification System). According to our calculations, there is roughly 1.5% more risk in the City of Saint Paul Alaska information security program than other programs in similar organizations.

S2SCORE phase-by-phase Comparison

There are four phases in a Full S2SCORE: Administrative Controls, Physical Controls, Internal Technical Controls, and External Technical Controls. An "acceptable" level of security is 660.

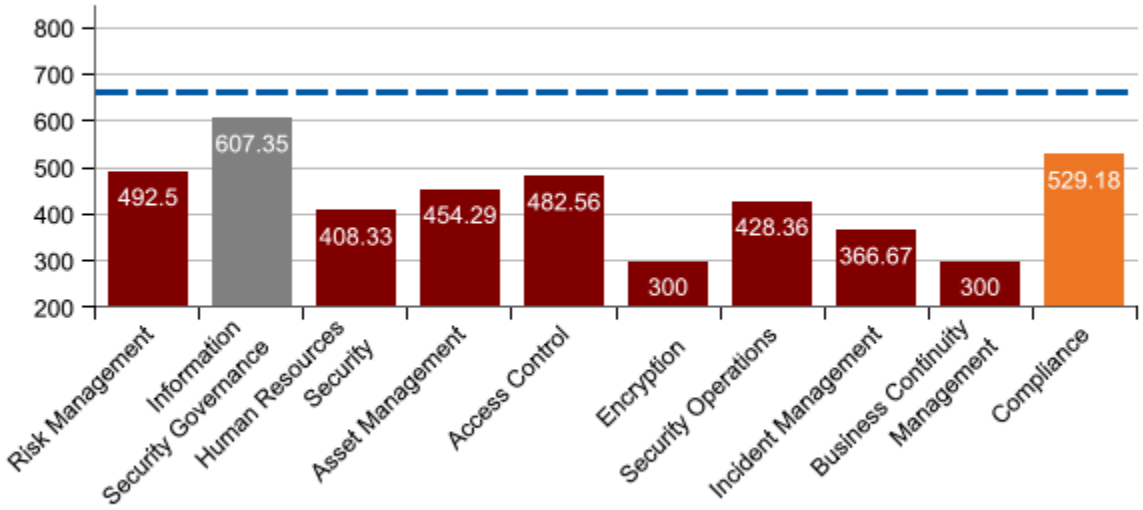


Administrative Controls Summary

Administrative Controls form the framework for managing an effective security program and they are sometimes referred to as the “human” part of information security. Administrative Controls inform people on how organizational leadership expects day-to-day operations to be conducted and they provide guidance on what actions or activities workforce members are expected to perform. Common Administrative Controls include policies, awareness training, guidelines, standards, and procedures. For more information about the City of Saint Paul Alaska Administrative Controls S2SCORE, see the section titled "Administrative Controls" in the full report.

The overall Administrative Controls S2SCORE is **445.08** or "**Very Poor**".

There are ten (10) sections within the administrative controls assessment and are summarized in the following chart.



Top Administrative Controls Recommendations

Risk Management Practices and Integration:

Ensure that risk management processes are formalized. Include the identification and prioritization of risks, overall risk tolerance, criteria for risk management, and plans to mitigate or accept risks. Formalized risk management activities will allow for a consistent and repeatable approach to risk mitigation practices.

Policies for Information Security:

Establish a comprehensive set of security policies that communicate management's expectations and the overall protection of company assets. Review FRSecure's templates and begin to build out a full set of information security policies. Security policies should be acknowledged by employees on a regular basis and sanctions enforced for policy violations. Collaborate with LMJ on appropriate policies. Consider utilizing FRSecure's free resources for this objective: https://frsecure.com/resources

Information Security Awareness, Education, and Training:

Establish a security awareness program that provides awareness and training to staff, so they understand their responsibilities. Include initial security awareness training during onboarding, annual refresher training, periodic emails, bulletins, or alerts to staff on current threats. Consider leveraging LMJ into this process.

Third-Party Security Risk Management:

Gather and document the current inventory of all vendors, including purpose, scope, and information security risk requirements, along with data access, and control requirements. Implement vendor information security reviews for all new vendors and periodically review vendor risk for existing vendors.

Incident Response Procedures:

Document and implement Incident Response procedures starting with the most critical systems, criteria for determining potential incident impact, team/vendor contacts, common incident workflows/playbooks and cyber security requirements. Ensure that all relevant people know the details of the plan and that the plan is tested on a regular basis. Ensure LMJ is included in this process.

Incident Management Roles and Responsibilities:

Define and document the process to report information security events and incidents within an incident response policy. Test the incident response procedures on a regular basis to ensure all relevant parties are prepared for potential incidents. Ensure LMJ is included in this process.

Physical Controls Summary

Physical Controls for information assets cannot be overlooked in an effective information security strategy. Physical Controls are the security controls that protect our assets from physical theft, modification, and destruction. Physical Controls can often be touched and provide assurances that our information will be safe. Common physical controls include doors, locks, camera surveillance, and alarm systems. For more information about the City of Saint Paul Alaska Physical Controls S2SCORE, see the section titled "Physical Controls" in the full report.

The overall Physical Controls S2SCORE is **572.12** or "**Poor**".

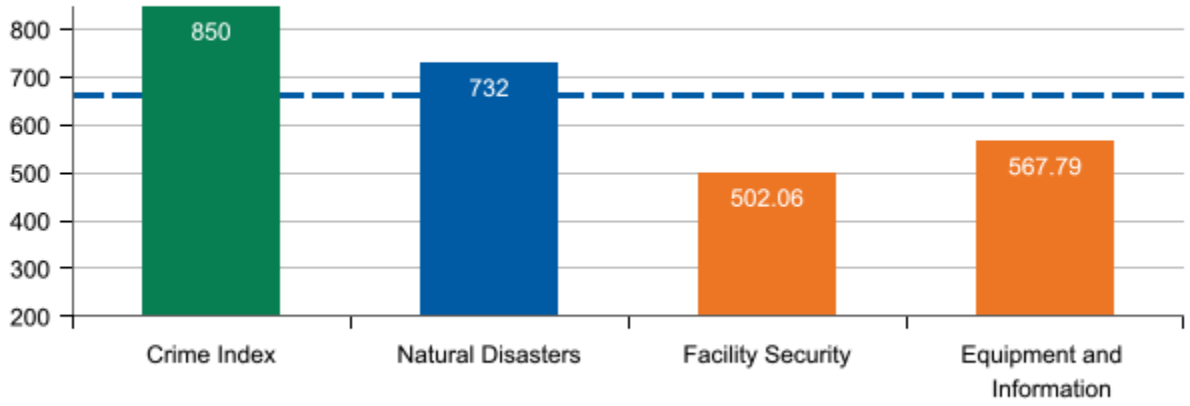
There is one (1) physical location that is in scope for this assessment. The in-scope physical location is:

- **Physical Location 1** - Headquarters

Physical Location (Headquarters)

Control Section Summary (Headquarters)

There are four (4) sections within the Headquarters physical location. The S2SCORE for each section is summarized in the following chart.



Top Physical Controls Recommendations

Planning and Preparedness:

Create and post evacuation routes/procedures. Conduct physical security exercises regularly. Develop formal physical security policies, procedures, and emergency response plans. Consider working with your local police/sheriff to do a formal risk assessment of the facility's emergency procedures. Ensure that employees are trained to respond to emergencies and conduct annual emergency drills.

Restricted Areas:

Develop a policy on the unauthorized use of recording equipment such as photographic, video, or audio devices in secured areas. Protect restricted areas by eliminating visibility into them, through tinted windows, shades, or other means.

Clear Desk/Screen:

Make sure that clear desk/screen requirements are documented in policy and communicated to all staff. Assign staff to spot check office areas and report findings.

Internal Technical Controls Summary

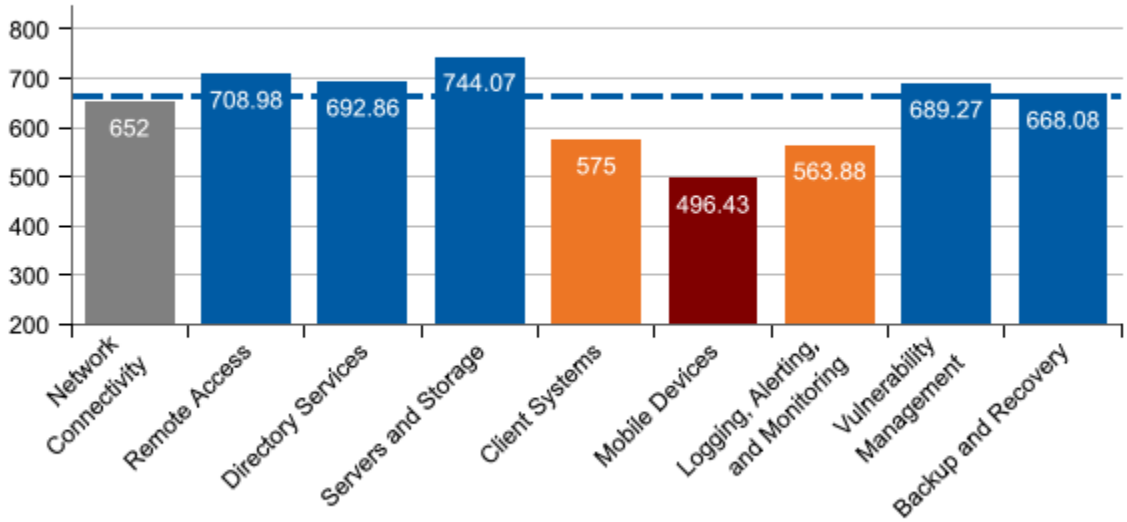
Internal Technical Controls are the controls that are technical in nature and used within your organization's technical domain (inside the gateways or firewalls). Internal technical controls include things such as firewalls, intrusion prevention systems, anti-virus software, and mobile device management (MDM). For more information about the City of Saint Paul Alaska Internal Technical Controls S2SCORE, see the section titled "Internal Technical Controls" in the full report.

The overall Internal Technical Controls S2SCORE is **742.38** or "**Good**".

Network Architecture Overview

The overall Network Architecture Overview S2SCORE is **656.60** or "**Fair**".

There are nine (9) sections within the internal technical controls assessment and are summarized in the following chart.



Vulnerability Scanning

The Vulnerability Scanning S2SCORE is **799.57** or "**Excellent**".

Top Internal Technical Controls Recommendations

Phones and Tablets:

Implement a mobile device management solution to ensure that all mobile devices are consistently managed according to defined organizational requirements. Keep corporate data on corporate-managed devices by restricting access for BYOD to “Internet only.”

Aggregation and Correlation:

Consider implementing centralized logging for all systems, that will aggregate and correlate logs across multiple systems to alert on technical system issues or security events and protect log files from destruction or loss. Create documented procedures around formal review of all logs generated, including summary logs. Critical events should alert administrators, and formal procedures should provide steps on remediation, including an organic flow into Incident Response procedures that have been approved by management. Review NIST best practices for Log Management: https://csrc.nist.gov/publications/detail/sp/800-92/final.

Backup Storage:

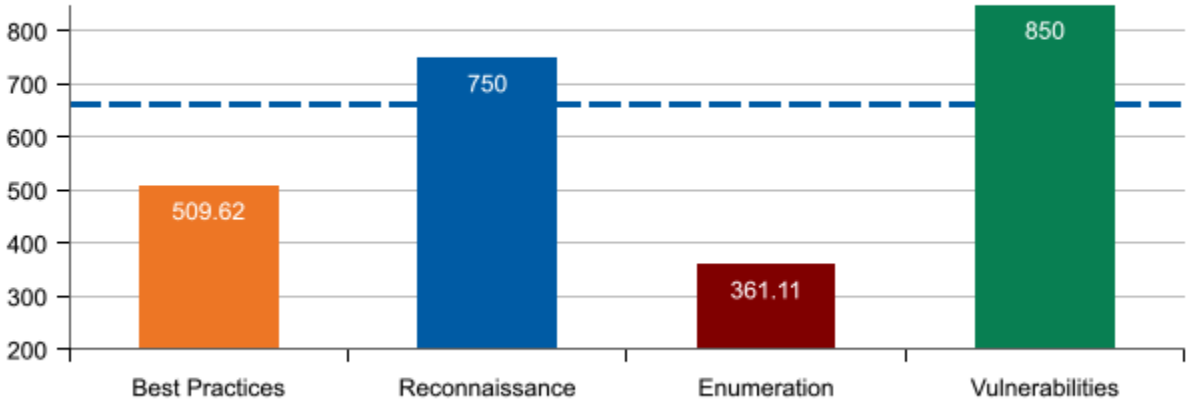
Conduct a business impact analysis (BIA) to help identify critical systems, processes, and their respective dependencies. Determine how long the organization can tolerate any downtime for critical systems.

External Technical Controls Summary

External technical controls are technical in nature and are used to protect outside access to your organization's technical domain (outside the gateways or firewalls). External technical controls consist of search engine indexes, social media, DNS, port scanning, and vulnerability scanning. For more information about the City of Saint Paul Alaska External Technical Controls S2SCORE, see the section titled "External Technical Controls" in the full report.

The overall External Technical Controls S2SCORE is **589.03** or "**Poor**".

There are four (4) sections within the external technical controls assessment and are summarized in the following chart.



Top External Technical Controls Recommendations

Monitoring:

Implement perimeter traffic security that monitors and alerts on malicious or abnormal ingress and egress traffic to DMZ or DNS servers. Implement additional security at the perimeter of the network to detect and block malicious traffic. Perform periodic and regular testing of the effectiveness of perimeter network controls.

Validation and Testing:

Conduct external penetration testing on a regular basis. Penetration testing is more in-depth and involved than simple vulnerability scanning and should give the organization additional insight into the ways that Internet-accessible systems could be compromised by a bad actor. Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts. Web applications should be tested for security on a regular basis and each time a change is made.

You have reached the end of the report.

Please contact FRSecure LLC with any questions or concerns about the content of this report.