| Prepared For: Sample Entity

S2ORG

Powered by S2SCORE

Management Summary Report

| Date: December 14, 2020

Table of Contents

Sample Entity Overall Results

The overall S2SCORE (or risk rating) is **610.77.**

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 **610.77** translates to "**Fair**". 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 Sample Entity.

S2SCORE Scale

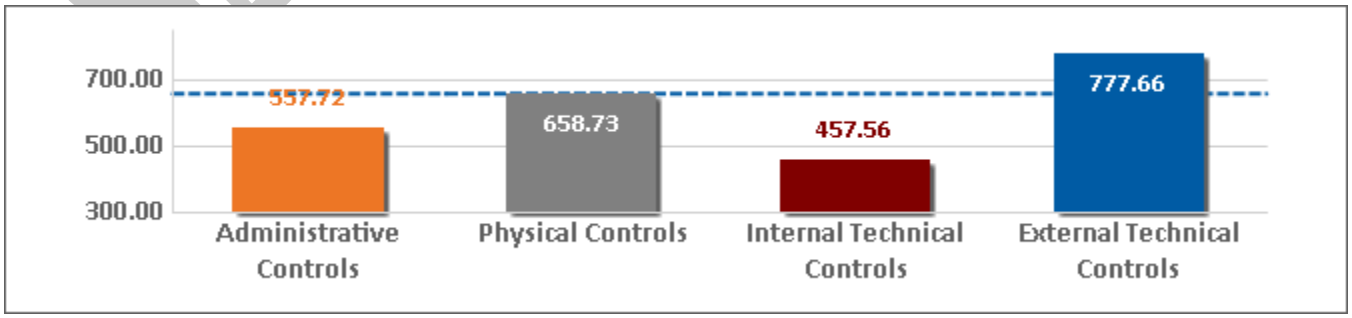
S2SCORE Average Across Industries

Industry: All Industries

The average S2SCORE is **776.50** across all industries. According to our calculations, there is roughly 21.3% more risk in the Sample Entity information security program than other programs in similar organizations.

S2SCORE phase-by-phase Comparison

There are four phases in a Full S2SCORE : . An "acceptable" level of security is 660.



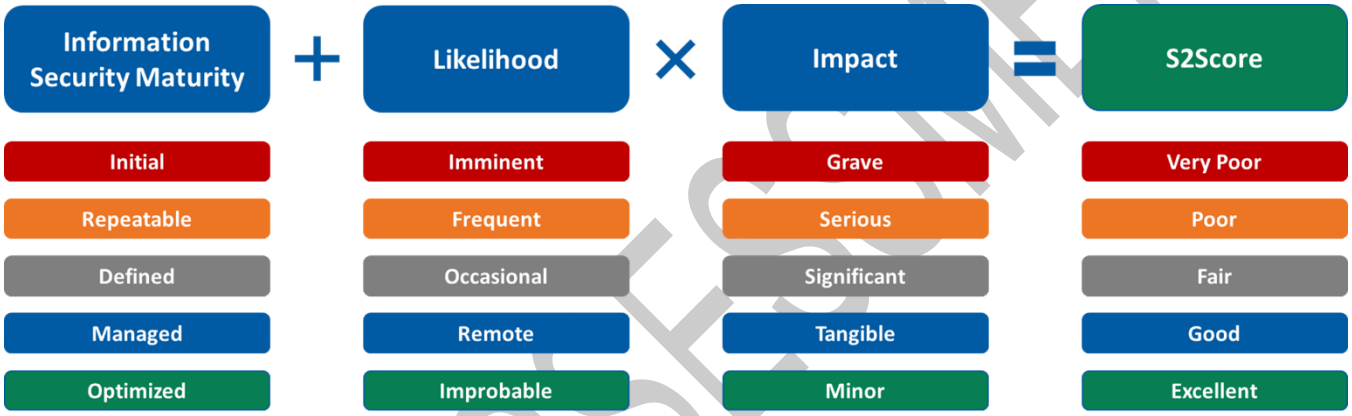
S2SCORE Explained

In simple terms, the S2SCORE is a representation of the risks assigned to Administrative, Physical, Internal Technical, and External Technical information security controls that were in scope for this assessment.

The S2SCORE can and should be used as a definitive measurement of risk and as a comparison with other entities.

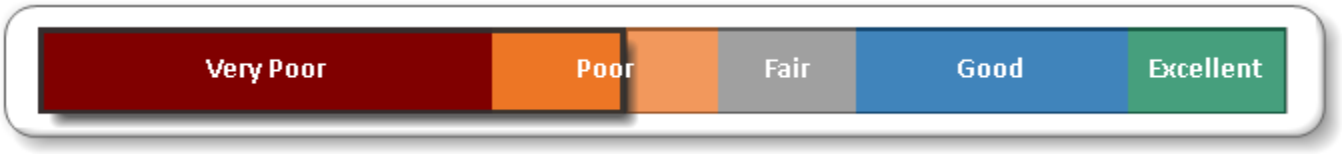
The key to the S2SCORE is "risk" and risk ratings are assigned by generating three values for each of the thousands of controls that were assessed. The three values are:

- **Information Security Maturity**, a translation of how effective a current control is in addressing its objective.
- **Likelihood**, an estimation of how likely an adverse event is given a lack of adequate control.
- **Impact**, an estimation of how impactful an adverse event could be given a lack of adequate control.



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 Sample Entity Administrative Controls S2SCORE, see the section titled "Administrative Controls" in the full report.



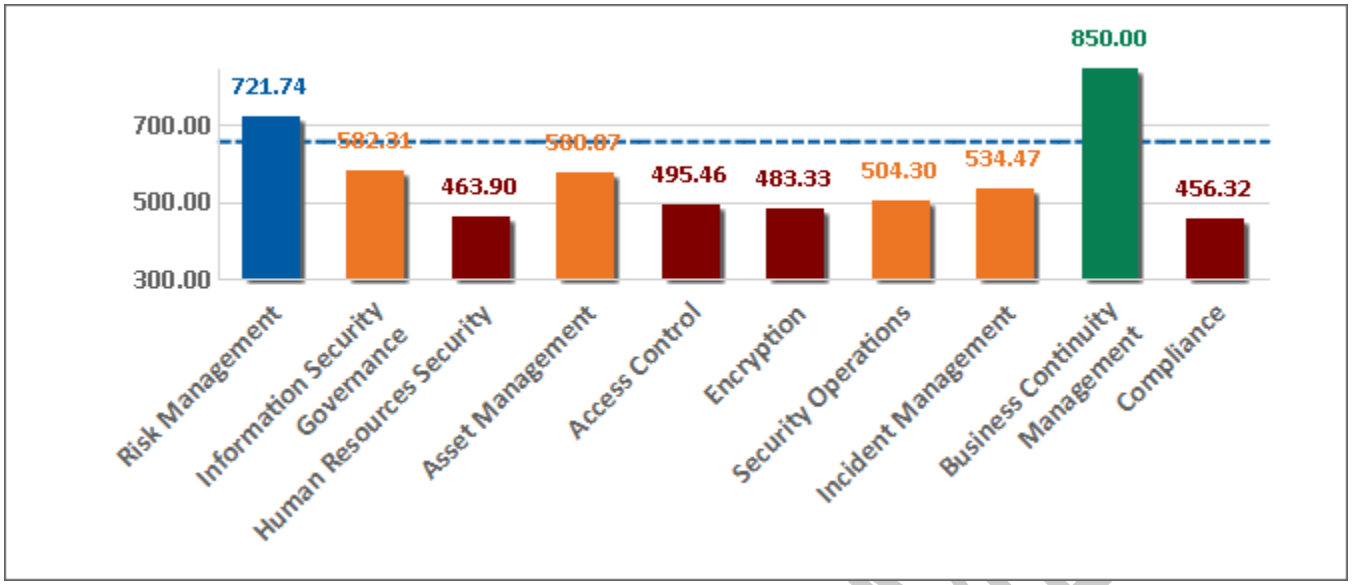
The overall Administrative Controls S2SCORE is **557.72** or "**Poor**".

There are ten (10) sections within the Administrative Controls assessment.

- **Risk Management** - To ensure that risk management practices are formalized, and executive management is enabled to make sound risk-based information security decisions.
- **Information Security Governance** - To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
- **Human Resources Security** - To ensure that personnel are adequately screened, qualified, and trained to perform their job functions in accordance with information security requirements.
- **Asset Management** - To maintain and manage a comprehensive asset inventory that enables the effective application of information security controls.
- **Access Control** - To limit access to information, information processing facilities, and sensitive organizational information.
- **Encryption** - To provide the required additional levels of protection for data-at-rest and data-in-transit.
- **Security Operations** - To ensure that the information security structure is properly implemented in practice.
- **Incident Management** - To ensure that responses to information security incidents are effective in minimizing the incident's effect to the organization.
- **Business Continuity Management** - To ensure that the organization can recover as quickly and effectively as possible from outages and severe degradation of service.
- **Compliance** - To ensure that the organization maintains compliance with applicable information security laws, regulations, and contractual language.

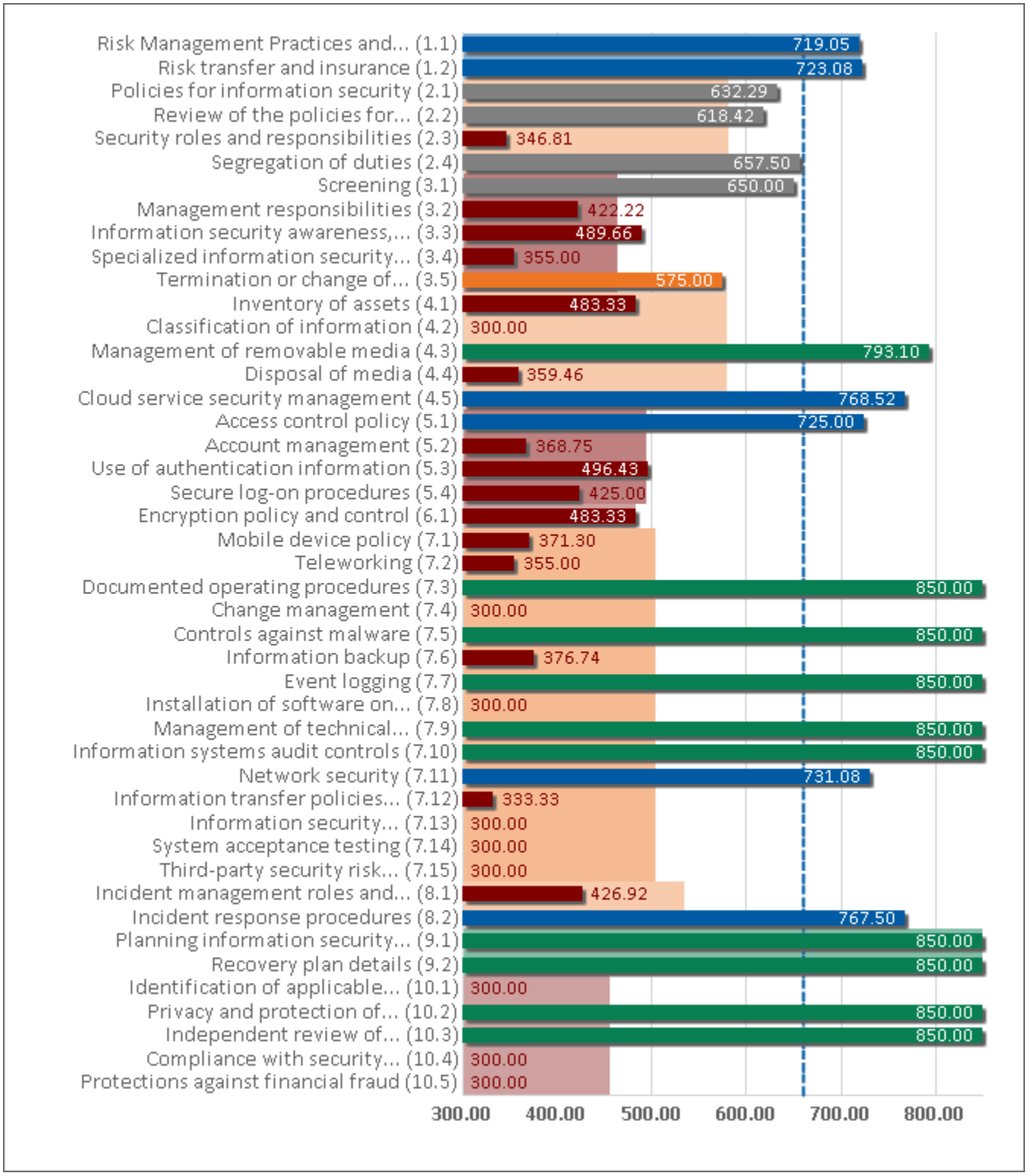
Control Section Summary

The S2SCORE for each section is summarized in the following chart.



Control Summary

Each of the ten (10) sections within the Administrative Controls assessment are further divided into forty-five (45) controls. The S2SCORE for each control within each section is summarized in the following table.



Top Administrative Controls Recommendations

Formalize your organization's approach for using encryption to protect data at rest and data in transit. Document and adopt a formal policy and support the policy with additional documentation and practices. Refer to the S2SCORE Full Report for more information.

Improve your incident management capabilities through more thorough, formalized planning and execution. Refer to the S2SCORE Full Report for more information.

Document all relevant information security roles and responsibilities in accordance with your organization's information security governance requirements. Refer to the S2SCORE Full Report for more information.

Formalize all account management practices in policy and procedure. Account management practices must account for the creation, approval, registration, and deregistration of all accounts, and practices should be audited on a periodic basis. Refer to the S2SCORE Full Report for more information.

Improve your compliance with your own policies and procedures through formalized audits. Make adjustments to policy and practices as necessary. Refer to the S2SCORE Full Report for more information.

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 Sample Entity Physical Controls S2SCORE, see the section titled "Physical Controls" in the full report.

The overall Physical Controls S2SCORE is **658.73** or "**Fair**".

There are four (4) sections that make up the S2SCORE for a given physical location:

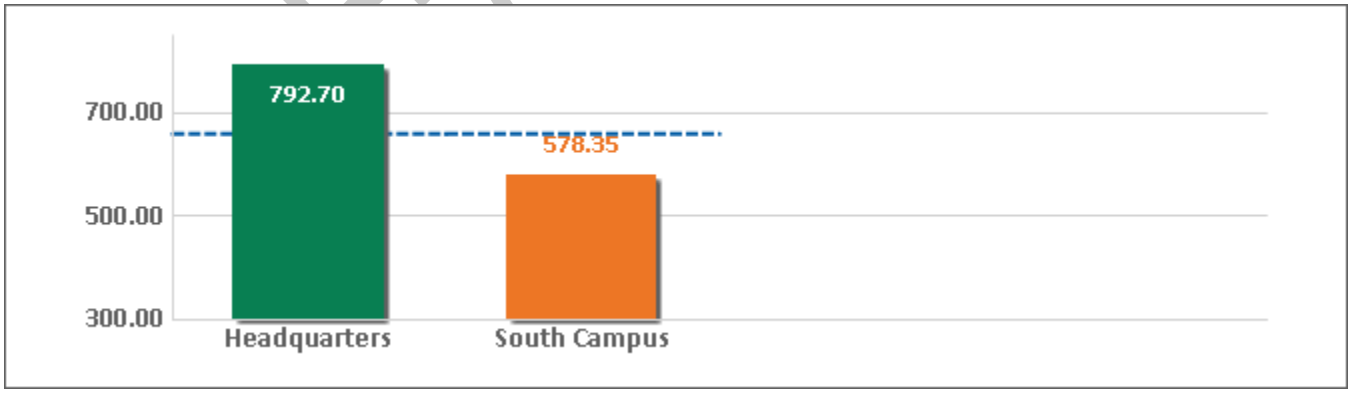
- **Crime Index** - To determine the amount of crime reported in the physical location of the facility. Data is gathered from publicly available sources such as the Federal Bureau of Investigation (FBI) publications.
- **Natural Disasters** - The number and severity of natural threats in the surrounding area.
- **Facility Security** - Primarily focused on facility security practices around physical access, damage, and interference to the organization's information and information processing facilities.
- **Equipment and Information** - Primarily focused on the security practices used to protect equipment and operations.

Metrics are assigned for multiple controls within each section as part of the overall Physical Controls S2SCORE.

There are two (2) physical locations that are in scope for this assessment. The in-scope physical locations are:

- **Physical Location 1** - Headquarters
- **Physical Location 2** - South Campus

Physical Location by Physical Location Comparison

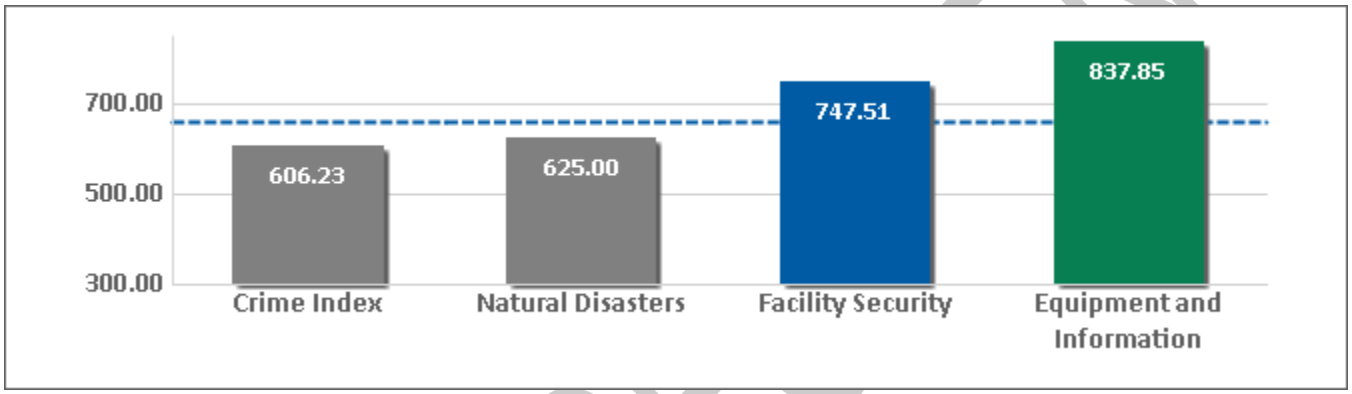


Physical Location (Headquarters)

The overall Headquarters S2SCORE is **792.70** or "**Excellent**".

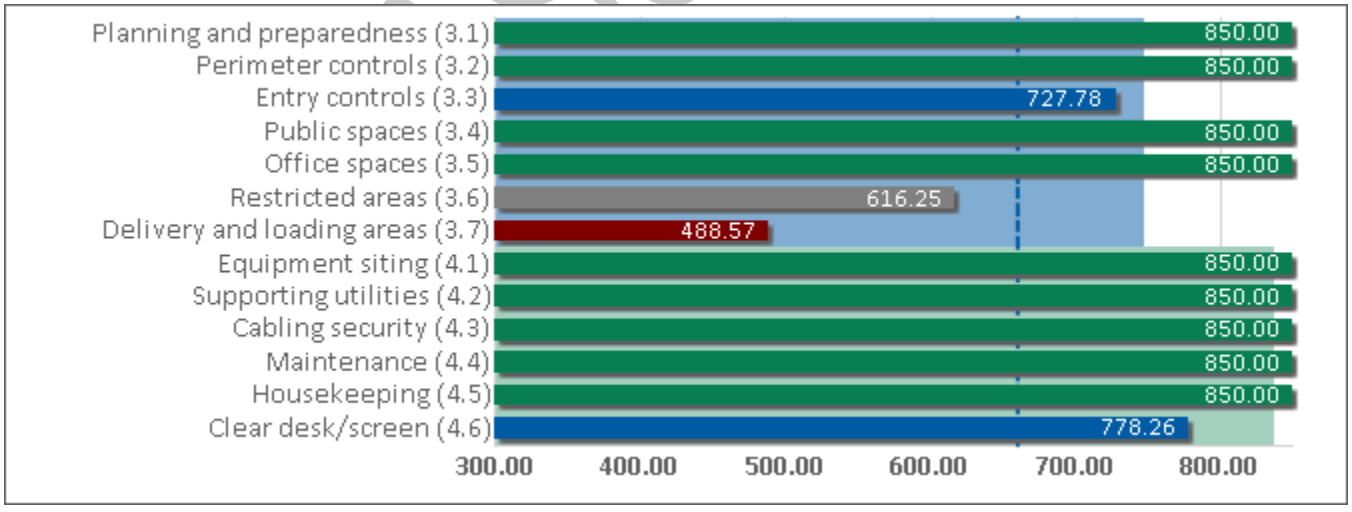
Control Section Summary (Headquarters)

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



Control Summary (Headquarters)

Each of the four (4) sections within the Physical Controls assessment are further divided into fifteen (15) controls. The S2SCORE for each control within each section is summarized in the following table.

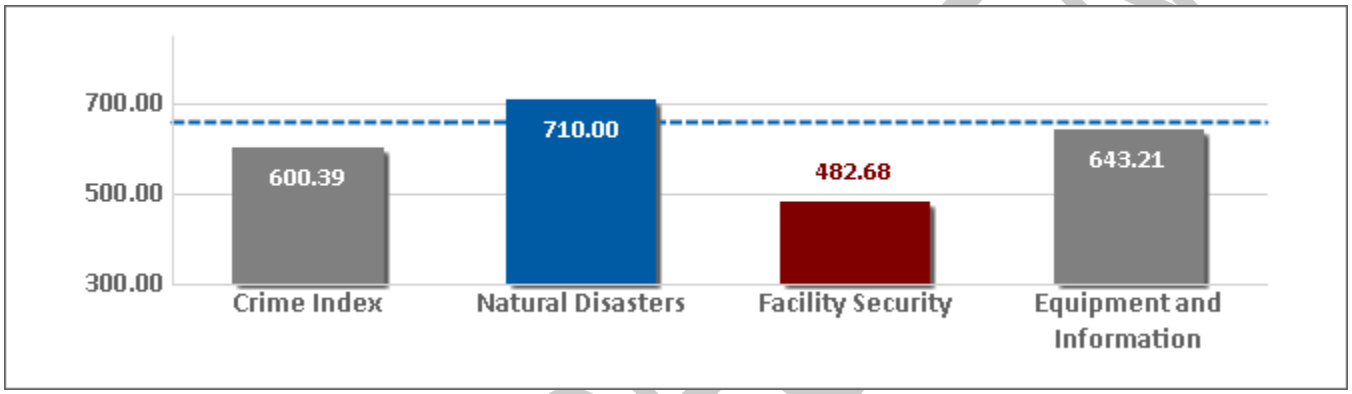


Physical Location (South Campus)

The overall South Campus S2SCORE is **578.35** or "**Poor**".

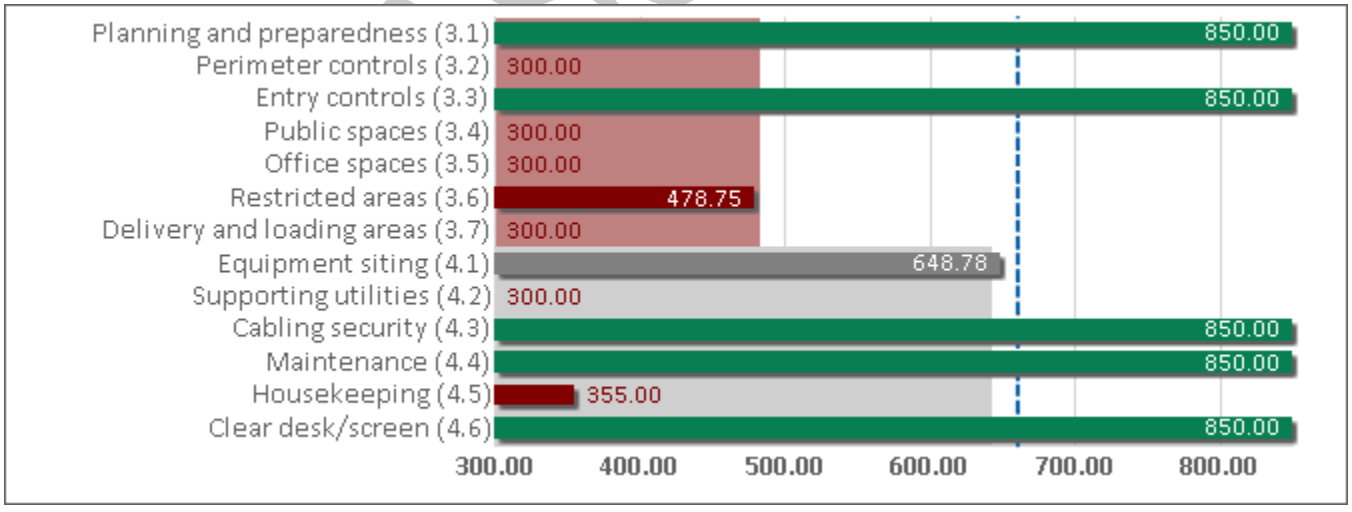
Control Section Summary (South Campus)

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



Control Summary (South Campus)

Each of the four (4) sections within the Physical Controls assessment are further divided into fifteen (15) controls. The S2SCORE for each control within each section is summarized in the following table.



Top Physical Controls Recommendations

Improve clear desk and/or clear screen practices to protect sensitive information. Refer to the S2SCORE Full Report for more information.

Improve the physical security and safety of delivery and loading areas in and around the organization's facilities. Refer to the S2SCORE Full Report for more information.

Formally define the organization's physical security perimeter and follow best practices (better) to ensure information, and more importantly, people remain safe. Refer to the S2SCORE Full Report for more information.

Formalize and improve the segregation of public facility spaces from non-public spaces. Once completed, improve security controls between them. Refer to the S2SCORE Full Report for more information.

Improve the physical security of office spaces within the organization's facilities. Refer to the S2SCORE Full Report for more information.

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 Sample Entity Internal Technical Controls S2SCORE, see the section titled "Internal Technical Controls" in the full report.

The overall Internal Technical Controls S2SCORE is **457.56** or "**Very Poor**".

The Internal Technical Controls Assessment is divided into two (2) areas:

- **Network Architecture Overview** - A thorough review of the technologies and practices employed by Sample Entity to protect information resources and assets. The details for the Network Architecture Overview assessment are presented in the next section of this report.
- **Vulnerability Scanning** - Vulnerability scanning is used to identify the technical vulnerabilities present in the Sample Entity technical environment. The details for the Vulnerability Scanning Overview assessment are presented in the Vulnerability Scanning Overview section of this report.

Network Architecture Overview

The overall Network Architecture Overview S2SCORE is **660.57** or "**Good**".

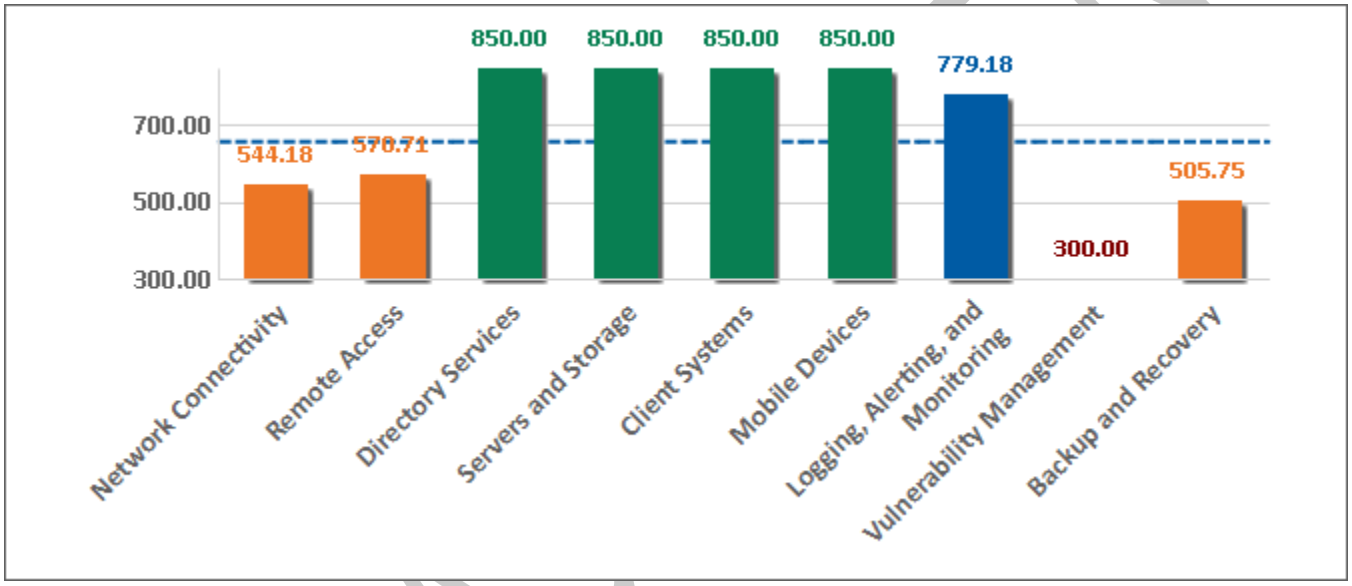
There are nine (9) sections within the Internal Technical Controls assessment.

- **Network Connectivity** - The analysis of the current network (Internet Connectivity, WAN connections, LAN design and configuration, and Wireless networking use) to qualify and quantify how risks have been managed and where potential gaps still exist.
- **Remote Access** - The analysis of any current remote access functionality and vendor connectivity to identify any potential risks.
- **Directory Services** - The analysis of the existing directory services design and configuration in order to identify any risks.
- **Servers and Storage** - The analysis of the server and storage environment and the methods used to mitigate risks in the unique context of the organization’s requirements.
- **Client Systems** - The analysis of the client systems to identify any risks that should be addressed.
- **Mobile Devices** - The analysis of the implementation and use of mobile devices inside and outside the environment to identify any risks that should be addressed.

- **Logging, Alerting, and Monitoring** - The analysis of the implementation, key components, and nonrepudiation strength (integrity) of the current logging, alerting, and monitoring within the environment.
- **Vulnerability Management** - The analysis of the current vulnerability management process (vulnerability patching, tracking, monitoring, and validation).
- **Backup and Recovery** - The analysis of the key component's backup and recovery processes and methods in place to protect the organization from the loss of information resources (partial or complete).

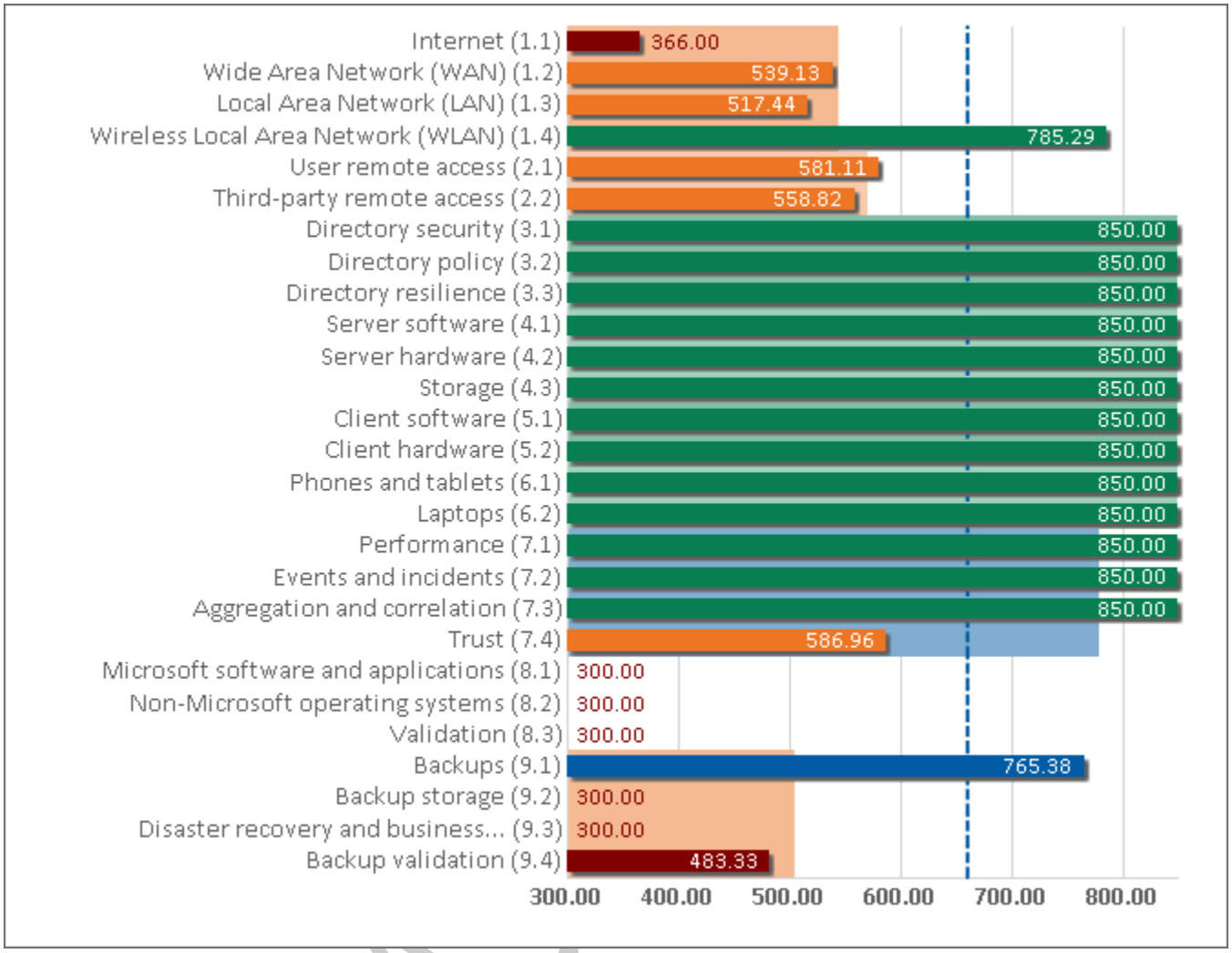
Control Section Summary

The S2SCORE for each section is summarized in the following chart.



Control Summary

Each of the nine (9) sections within the Internal Technical Controls assessment are further divided into twenty-seven (27) controls. The S2SCORE for each control within each section is summarized in the following table.



Vulnerability Scanning

The Vulnerability Scanning S2SCORE is **322.22** or "**Very Poor**".

Summary

"Good" is the acceptable threshold for systems. Of the total hosts, 50.0% (3) were at or exceeded this threshold and 50.0% (3) **did not meet** this threshold.

The single largest population of systems in the Sample Entity environment is rated "Excellent".

<-- Above	Below -->
50.0%	50.0%
50.0% (3) Hosts	50.0% (3) Hosts

Systems BELOW the acceptable threshold:

- 0.0% (0) of the total hosts in the environment were rated **"Very Poor"**
- 50.0% (3) of the total hosts in the environment were rated **"Poor"**
- 0.0% (0) of the total hosts in the environment were rated **"Fair"**

Systems AT or ABOVE the acceptable threshold:

- 0.0% (0) of the total hosts in the environment were rated **"Good"**
- 50.0% (3) of the total hosts in the environment were rated **"Excellent"**

The vulnerabilities noted are significant and have a great impact on the Sample Entity overall risk rating.

- Of all places to start remediation, the first should be in attending to the critical-severity and high-severity vulnerabilities identified during this assessment. This should be done as soon as possible.
- Review the details of the scanning exercise and remediate all vulnerabilities that are unacceptable to the organization.

Top Internal Technical Controls Recommendations

Improve vulnerability management practices. Ensure formality, repeatability, objectivity, and adequate scope. Vulnerability management must include patch management and configuration management in order to be most effective. Refer to the S2SCORE Full Report for more information.

Improve third-party remote access security. Remote access must only be provided to third-parties who specifically require it, and only when they specifically require it. Security must be provided with multi-factor authentication (MFA), consistent monitoring, encryption, etc. Refer to the S2SCORE Full Report for more information.

Improve user/employee remote access security. Remote access must only be provided to those personnel who specifically require it, and security must be provided with multi-factor authentication (MFA), consistent monitoring, encryption, etc. Refer to the S2SCORE Full Report for more information.

Improve the trust level of evidentiary information though log strategy, access control, time synchronization, and other means. Refer to the S2SCORE Full Report for more information.

Formalize vulnerability management for all operating systems and define specific SLAs for remediation thoughout the enterprise. Refer to the S2SCORE Full Report for more information.

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 Sample Entity External Technical Controls S2SCORE, see the section titled "External Technical Controls" in the full report.

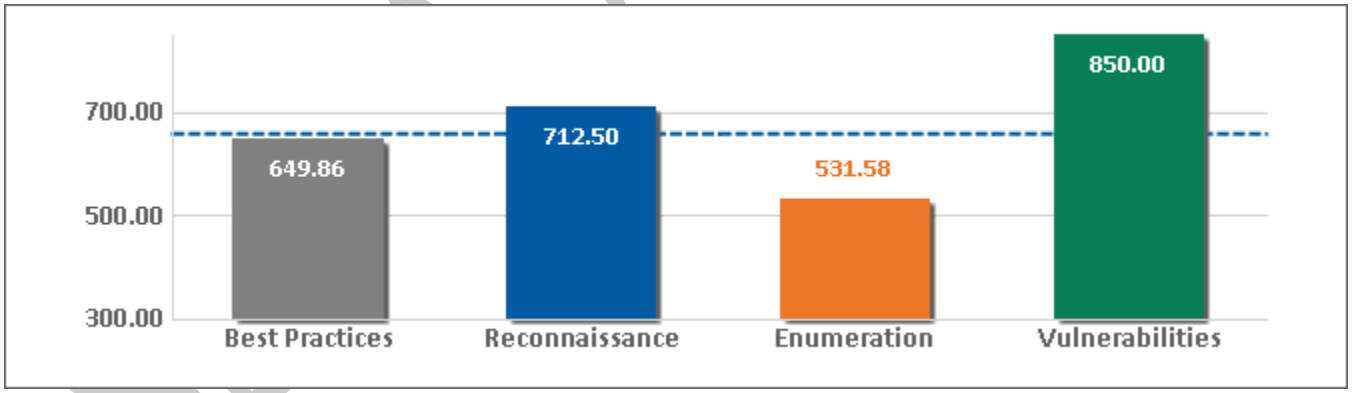
The overall External Technical Controls S2SCORE is **777.66** or "**Good**".

There are four (4) sections within the External Technical Controls assessment.

- **Best Practices** - Generally-accepted best practices for securing publicly (or Internet) accessible systems and information resources.
- **Reconnaissance** - To discover information about the organization's information resources from sources outside of the organization's control.
- **Enumeration** - Identification and qualification of information resources made available by the organization, some intentionally and others unintentionally.
- **Vulnerabilities** - Armed with information from Enumeration, technical vulnerabilities are identified in the organization's information resources.

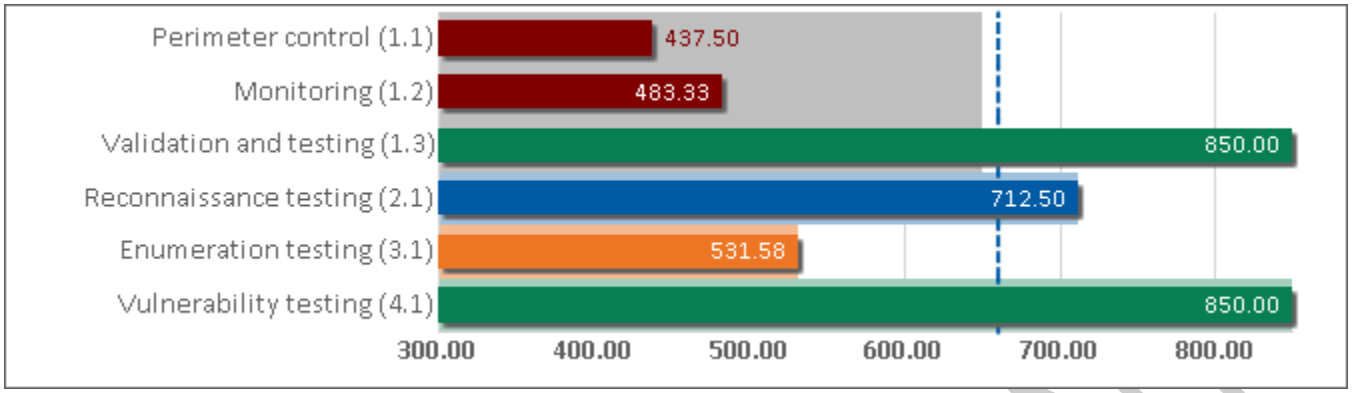
Control Section Summary

The S2SCORE for each section is summarized in the following chart.



Control Summary

Each of the four (4) sections within the External Technical Controls assessment are further divided into six (6) controls. The S2SCORE for each control within each section is summarized in the following table.



Top External Technical Controls Recommendations

Follow perimeter security best practices more closely. Refer to the S2SCORE Full Report for more information.

Improve the ingress and egress traffic monitoring technologies and processes related to the perimeter of the organization's network(s). Refer to the S2SCORE Full Report for more information.

Regularly and formally enumerate all externally exposed information assets to ensure your organization is only exposing that which is absolutely necessary for business operations. Refer to the S2SCORE Full Report for more information.

Formalize and improve your organization's testing related to the reconnaissance techniques commonly used by attackers. Refer to the S2SCORE Full Report for more information.

You have reached the end of the report.

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