Agenda

Planning, Finance, Enterprise, and Economic Development
Oelwein City Hall, 20 Second Avenue SW, Oelwein, Iowa
5:15 PM

April 25, 2022
Oelwein, Iowa

Mayor: Brett DeVore
Mayor Pro Tem: Lynda Payne
Council Members: Karen Seeders, Tom Stewart, Matt Weber, Dave Garrigus, Dave Lenz

Pledge of Allegiance

Discussions

1. Discussion on Security Assessment.

Adjournment

In compliance with the Americans with Disabilities Act, those requiring accommodation for Council meetings should notify the City Clerk's Office at least 24 hours prior to the meeting at 319-283-5440

berganKDV

We have prepared a quote for you

Security Assessment

Quote # 068514
Version 2

Prepared for:

City of Oelwein

Dylan Mulfinger
DMulfinger@cityofoelwein.org

100 E Park Ave Ste 200
Waterloo, IA 50703
www.BerganKDV.com
888-356-2295

berganKDV

Item 1.

Down Payment

Description	Price	Qty	Ext. Price
A down payment of 50% will be required on all purchases with a total of $10,000 or greater. After approval of quote, an invoice for the down payment amount will be sent, orders will be placed after invoice is paid.			

Services

Description	Price	Qty	Ext. Price
Security Assessment Project Fee - Annual for 3 Years	$10,800.00	1	$10,800.00

Subtotal: **$10,800.00**

100 E Park Ave Ste 200
Waterloo, IA 50703
www.BerganKDV.com
888-356-2295

berganKDV

Item 1.

Security Assessment

Prepared by:	Prepared for:	Quote Information:
Cedar Valley	**City of Oelwein**	**Quote #: 068514**
Susan	20 2nd Ave SW	Version: 2
(319) 433-3743	Oelwein, IA 50662	Delivery Date: 04/11/2022
susan.perkins@bergankdv.com	Dylan Mulfinger	Expiration Date: 05/31/2022
	DMulfinger@cityofoelwein.org	
	(712) 870-0617	

Quote Summary

Description	Amount
Services	$10,800.00

Please DO NOT pay from quote. An invoice will be generated after authorization.   Total: **$10,800.00**

Taxes, shipping, handling and other fees may apply. We reserve the right to cancel orders arising from pricing or other errors.

_____   _____
Signature   Date

100 E Park Ave Ste 200
Waterloo, IA 50703
www.BerganKDV.com
888-356-2295

berganKDV

Item 1.

Terms and Approval

By signing and returning this Quotation, I authorize BerganKDV to order the above products. I also agree, upon delivery of the above products, to pay BerganKDV any and all amounts due. Unless explicitly specified in the above quotation details, labor hours required to deliver, install, configure, and/or support the above products is not included in the quoted price. In some cases, an amount will be due prior to ordering. Additional shipping charges may apply. Prices are subject to change without notice.

WARRANTIES AND DISCLAIMERS

A) Limitation of liability. BerganKDV shall not be liable to client under any circumstances for client's loss of the use of it's network or related systems. In no event shall vendor be liable to customer for any indirect, special or consequential damages or loss profits arising out of or related to this agreement or the performance of services hereunder or any breach thereof even if vendor has been advised of the possibility thereof. Vendor's liability to customer hereunder, if any, shall in no event exceed the total amount paid to the vendor hereunder. In no event shall vendor be liable to customer for any damages resulting from or relate to any failure or delay of vendor in the performance of services hereunder.

B) Negation of Warranty. Vendor does not warrant the services performed hereunder or the accuracy or correctness of the results of the services, and there are no warranties, express or implied, including, but limited to warranties of the merchantability or fitness for any particular purpose.

INDEMNIFICATION

City of Oelwein hereby agrees to indemnify and defend at its sole expense: BerganKDV, its employees, agents, representatives, directors and shareholders, from and against any and all claims arising out of or based upon City of Oelwein use of all services, software or hardware provided or serviced hereunder, including, but not limited to, claims based on software licensing violations, copyright infringement, trademark infringement and patent infringement. In addition, City of Oelwein agrees to pay any judgment and costs associated with such claim.

RETURNS

Eligible returns must be made with 15 days in the original packaging in like new condition. There may be shipping costs as well as 20% restocking fee on items that can be returned. BerganKDV reserves the right to deny any returns or exchanges. Check with your account manager for details.

berganKDV

Schedule S
Version 2022

CLIENT	City of Oelwein
SCHEDULE NAME	Security Assessment (3 years)
START DATE	May1 , 2022
DELIVERABLES	BerganKDV will provide the following Security Assessment service (collectively, the "Services"): • Pre-project planning meeting. • Perform onsite assessment at agreed upon locations. • Vulnerability assessment is performed on 4 sites (1 subnet or multiple routed subnets) and 1 Active Directory. • Employee interviews will only be conducted at the main location identified in "Client Locations". • Employee interviews will be a minimum of 2 members. • Development of executive summary with 4 categories of risk. • Presentation and discussion of assessment which includes best practices and • Recommendations for corrective actions. • Meetings and interviews may be held virtually or in person. It is important to note that security related issues of IT equipment and processes change daily. No security test or tests can ever guarantee 100% protection from all possible security attacks on the client's system. BerganKDV provides no guarantee in relation to the relevance of the testing methods used or the finding of any vulnerability assessment for any amount of time other than the exact time that any given specific test or procedure is executed.
CLIENT LOCATION (S)	This agreement covers the following CLIENT location(s): City Hall/Fire station Public Works Campus Wastewater Department Police Department
FEES & PAYMENT	CLIENT is purchasing an annual Security Assessment service in exchange for a base fee of **$10,500.00** per year for 3 years. In addition to the agreed upon fee, CLIENT agrees to pay for any requested service performed that is not listed under DELIVERABLES. Security Consultant time is billed at $275/hour. Excluded Services may not be exchanged for the removal or non-performance of Included Services.

The contents of this document are confidential and are only to be viewed by Client.

This Schedule is governed by the terms of the Professional Services Agreement:

For and on behalf of BerganKDV	For and on behalf of Client
Signature:	Signature:
Contact Name: Dan Roling	Contact Name:
Title: Technology Solutions Leader	Title:
Date:	Date:

S2ORG

Powered by S2SCORE

Management Summary Report

| Date: December 14, 2020

Table of Contents

Item 1.

Sample Entity Overall Results

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

610.77 Fair

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

Very Poor 300 - 500	Poor 500 - 600	Fair 600 - 660	Good 660 - 780	Excellent 780 - 850

S2SCORE Average Across Industries

Industry: All Industries
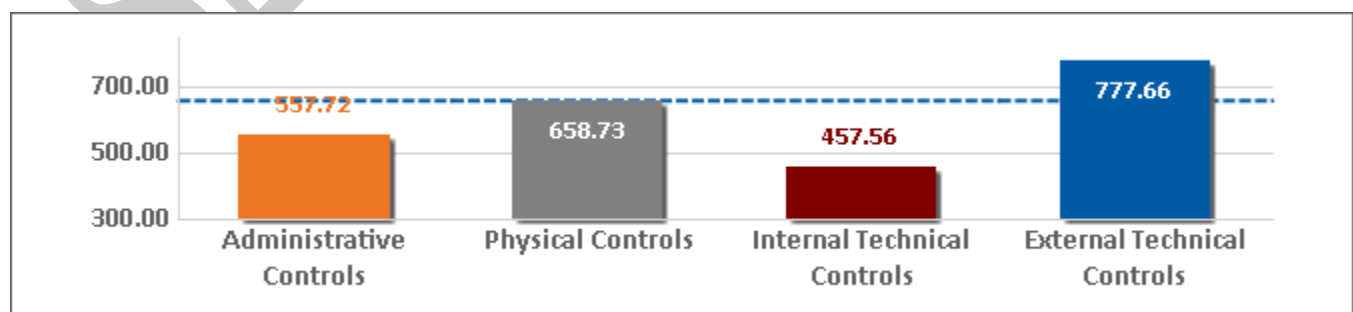
Very Poor	Poor	Fair	Good	Excellent

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.

	Administrative Controls	Physical Controls	Internal Technical Controls	External Technical Controls
Score	557.72	658.73	457.56	777.66

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.

Information Security Maturity	+	Likelihood	×	Impact	=	S2Score
Initial		Imminent		Grave		Very Poor
Repeatable		Frequent		Serious		Poor
Defined		Occasional		Significant		Fair
Managed		Remote		Tangible		Good
Optimized		Improbable		Minor		Excellent

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.
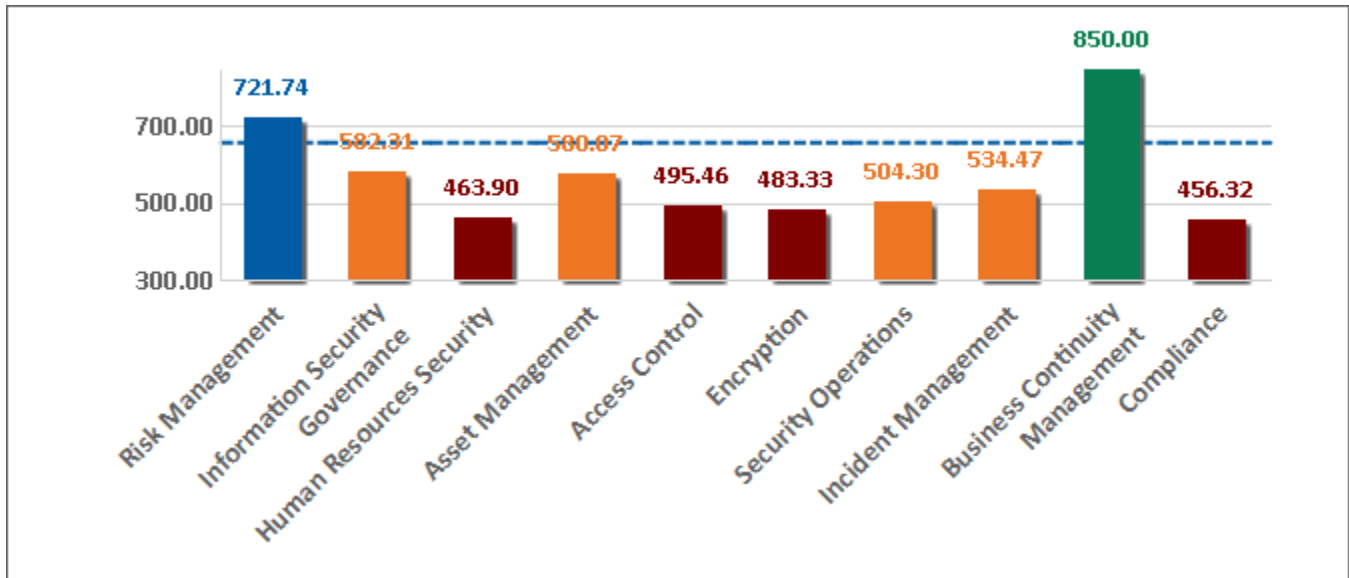

The overall Administrative Controls S2SCORE is **557.72** or "**Poor**".

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.
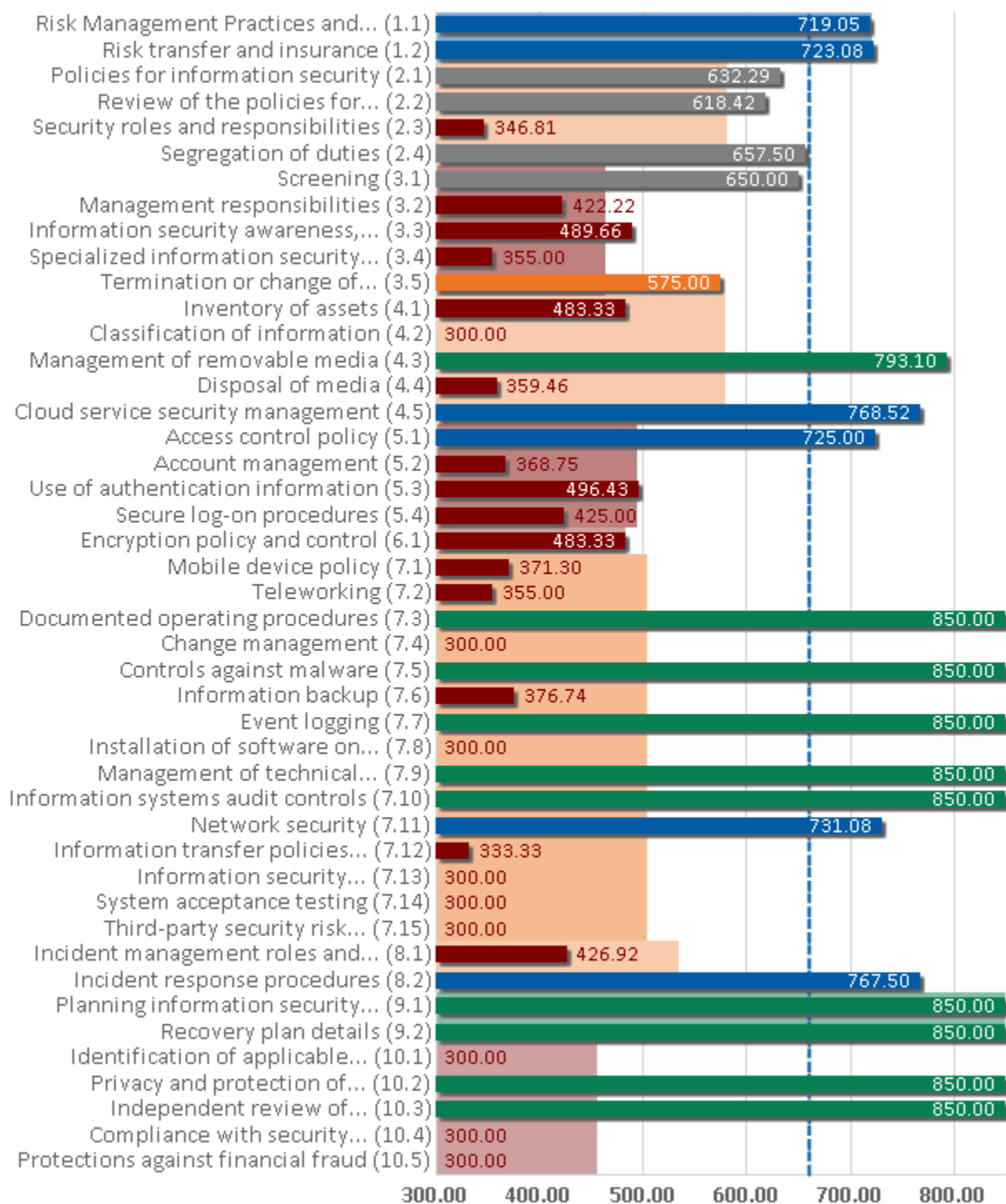
Control Section Summary

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.

Control	Score
Risk Management Practices and... (1.1)	719.05
Risk transfer and insurance (1.2)	723.08
Policies for information security (2.1)	632.29
Review of the policies for... (2.2)	618.42
Security roles and responsibilities (2.3)	346.81
Segregation of duties (2.4)	657.50
Screening (3.1)	650.00
Management responsibilities (3.2)	422.22
Information security awareness,... (3.3)	489.66
Specialized information security... (3.4)	355.00
Termination or change of... (3.5)	575.00
Inventory of assets (4.1)	483.33
Classification of information (4.2)	300.00
Management of removable media (4.3)	793.10
Disposal of media (4.4)	359.46
Cloud service security management (4.5)	768.52
Access control policy (5.1)	725.00
Account management (5.2)	368.75
Use of authentication information (5.3)	496.43
Secure log-on procedures (5.4)	425.00
Encryption policy and control (6.1)	483.33
Mobile device policy (7.1)	371.30
Teleworking (7.2)	355.00
Documented operating procedures (7.3)	850.00
Change management (7.4)	300.00
Controls against malware (7.5)	850.00
Information backup (7.6)	376.74
Event logging (7.7)	850.00
Installation of software on... (7.8)	300.00
Management of technical... (7.9)	850.00
Information systems audit controls (7.10)	850.00
Network security (7.11)	731.08
Information transfer policies... (7.12)	333.33
Information security... (7.13)	300.00
System acceptance testing (7.14)	300.00
Third-party security risk... (7.15)	300.00
Incident management roles and... (8.1)	426.92
Incident response procedures (8.2)	767.50
Planning information security... (9.1)	850.00
Recovery plan details (9.2)	850.00
Identification of applicable... (10.1)	300.00
Privacy and protection of... (10.2)	850.00
Independent review of... (10.3)	850.00
Compliance with security... (10.4)	300.00
Protections against financial fraud (10.5)	300.00

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.

Very Poor	Poor	Fair	Good	Excellent

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

Headquarters	South Campus
792.70	578.35
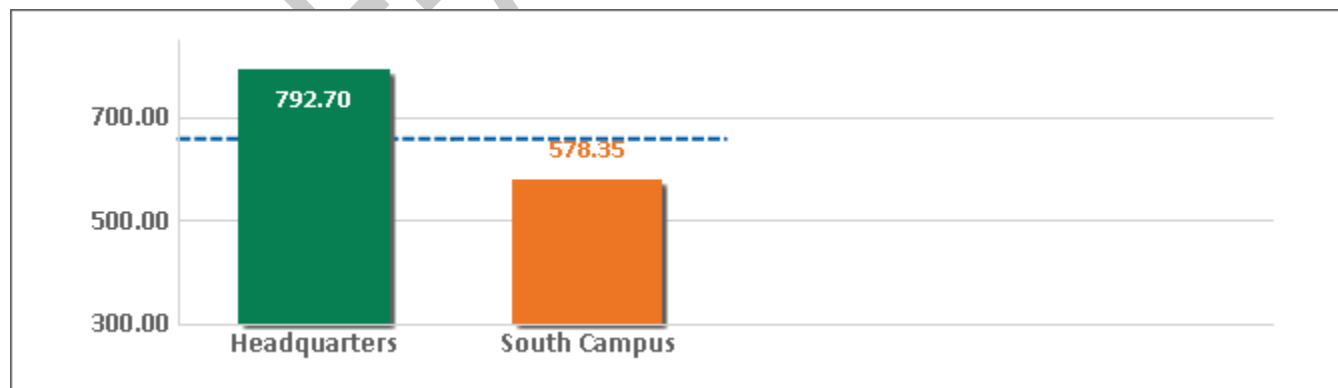
Physical Location (Headquarters)

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

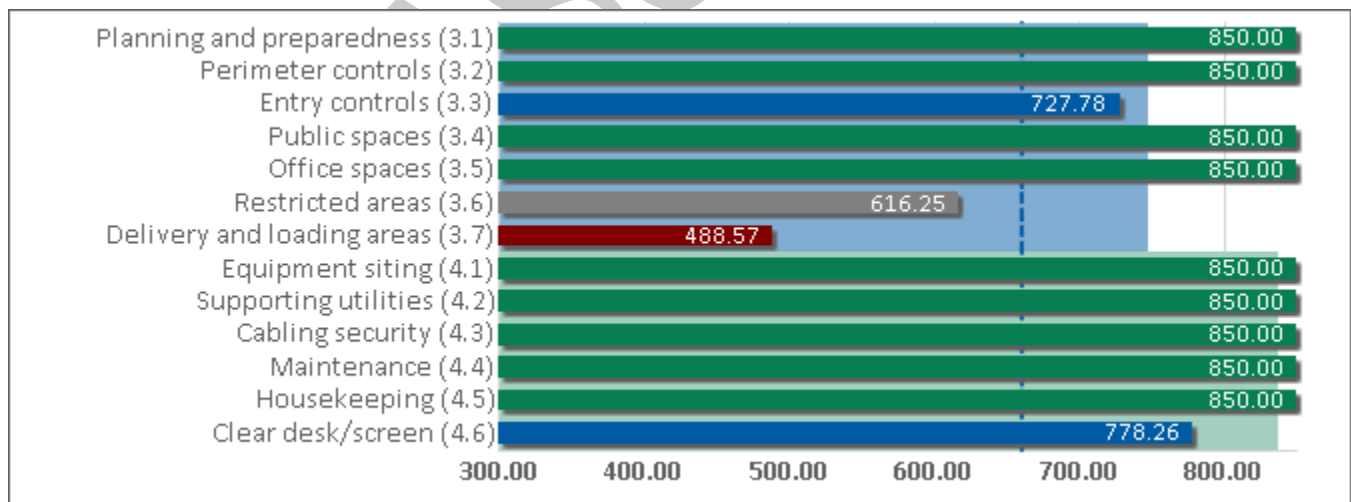| Very Poor	Poor	Fair	Good	Excellent

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.
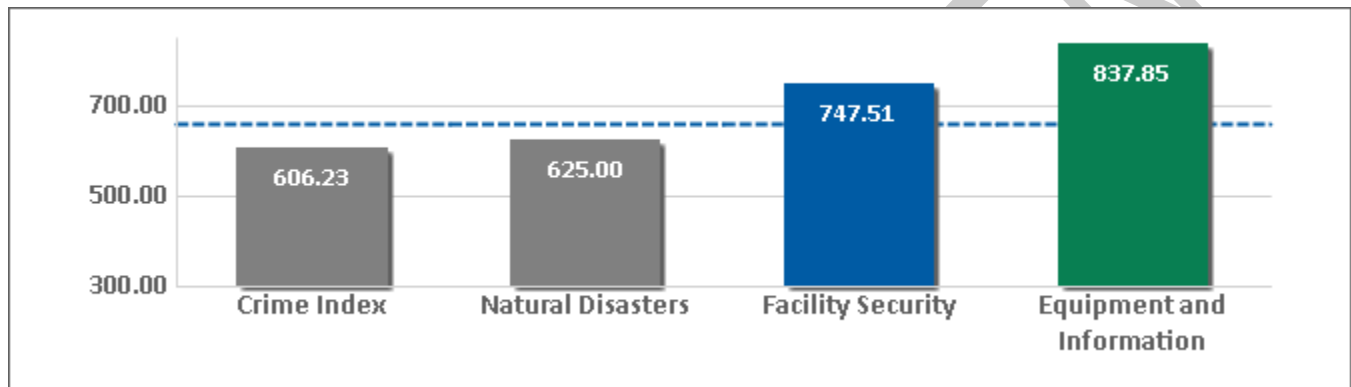
Control Summary (Headquarters)

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.
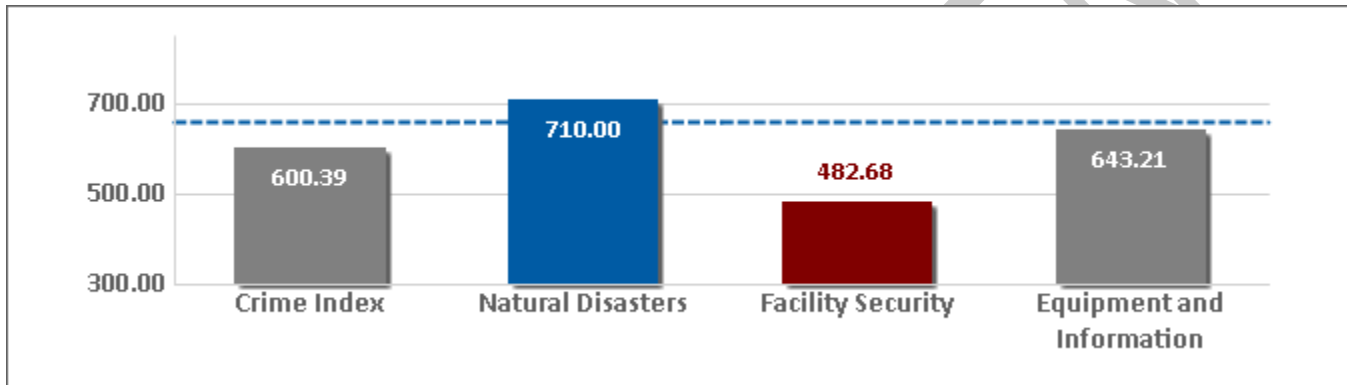
Control Summary (South Campus)

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.
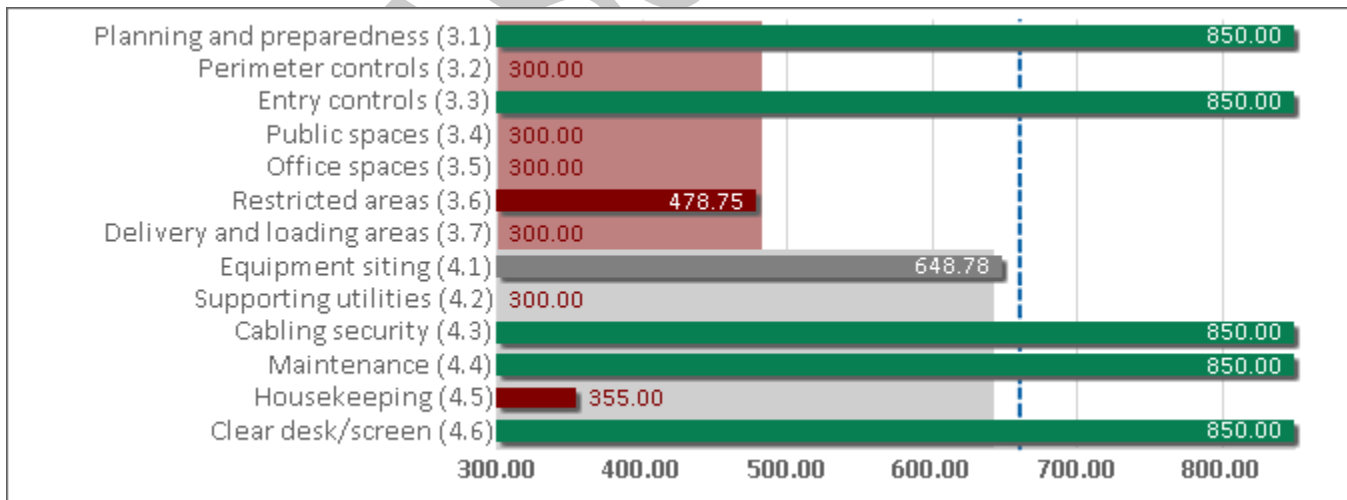
Top Physical Controls Recommendations

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.

| Very Poor		Poor	Fair	Good	Excellent

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**".

Very Poor	Poor	Fair	Good	Excellent
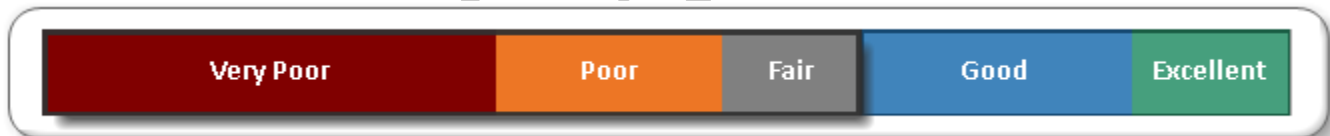
There are nine (9) sections within the Internal Technical Controls assessment.

- **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).
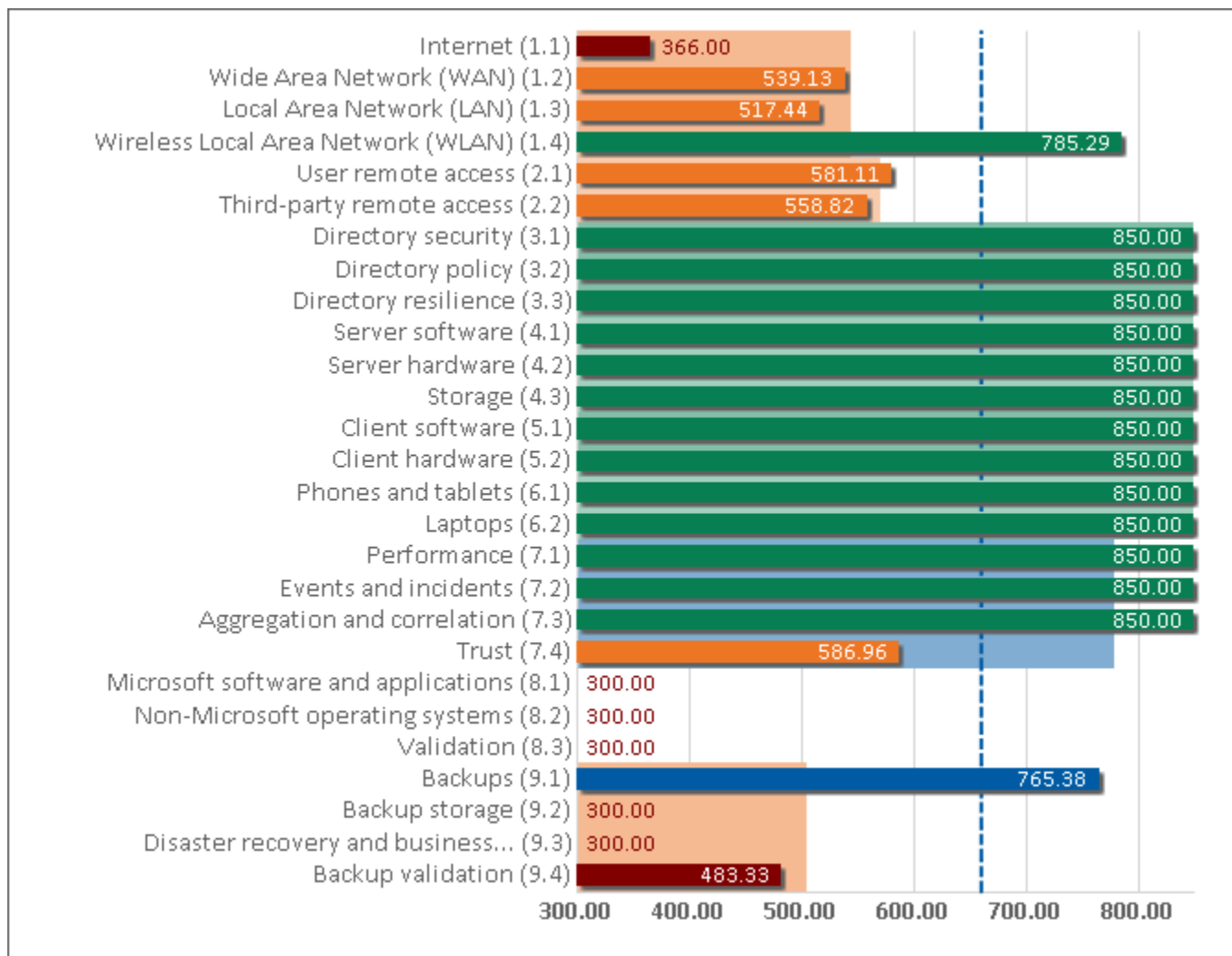
Control Section Summary

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.

| Category	Score
Internet (1.1)	366.00
Wide Area Network (WAN) (1.2)	539.13
Local Area Network (LAN) (1.3)	517.44
Wireless Local Area Network (WLAN) (1.4)	785.29
User remote access (2.1)	581.11
Third-party remote access (2.2)	558.82
Directory security (3.1)	850.00
Directory policy (3.2)	850.00
Directory resilience (3.3)	850.00
Server software (4.1)	850.00
Server hardware (4.2)	850.00
Storage (4.3)	850.00
Client software (5.1)	850.00
Client hardware (5.2)	850.00
Phones and tablets (6.1)	850.00
Laptops (6.2)	850.00
Performance (7.1)	850.00
Events and incidents (7.2)	850.00
Aggregation and correlation (7.3)	850.00
Trust (7.4)	586.96
Microsoft software and applications (8.1)	300.00
Non-Microsoft operating systems (8.2)	300.00
Validation (8.3)	300.00
Backups (9.1)	765.38
Backup storage (9.2)	300.00
Disaster recovery and business... (9.3)	300.00
Backup validation (9.4)	483.33

Vulnerability Scanning

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

Very Poor	Poor	Fair	Good	Excellent

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	
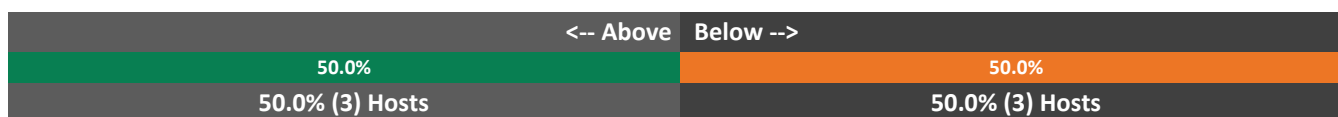
Systems BELOW the acceptable threshold:

- 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.

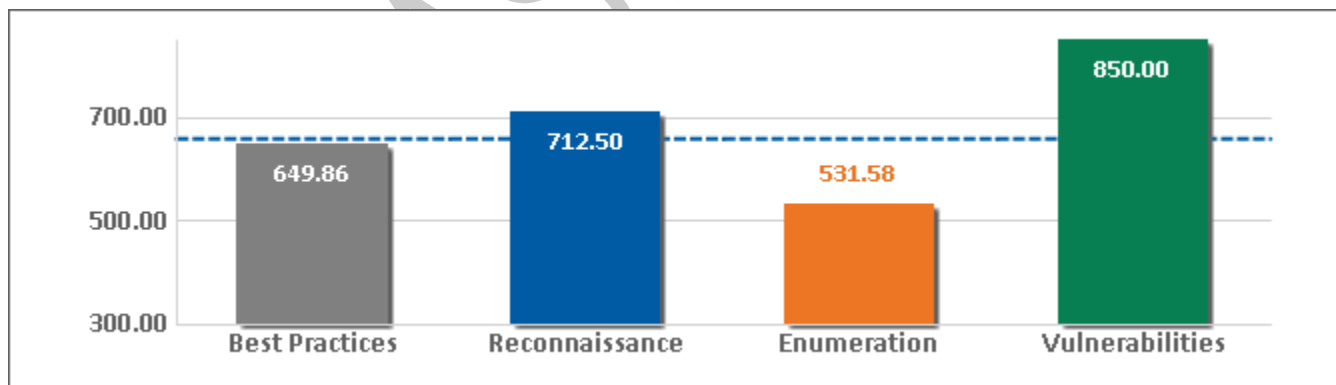| Very Poor	Poor	Fair	Good	Excellent

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.

	Best Practices	Reconnaissance	Enumeration	Vulnerabilities
Score	649.86	712.50	531.58	850.00

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.

Item 1.
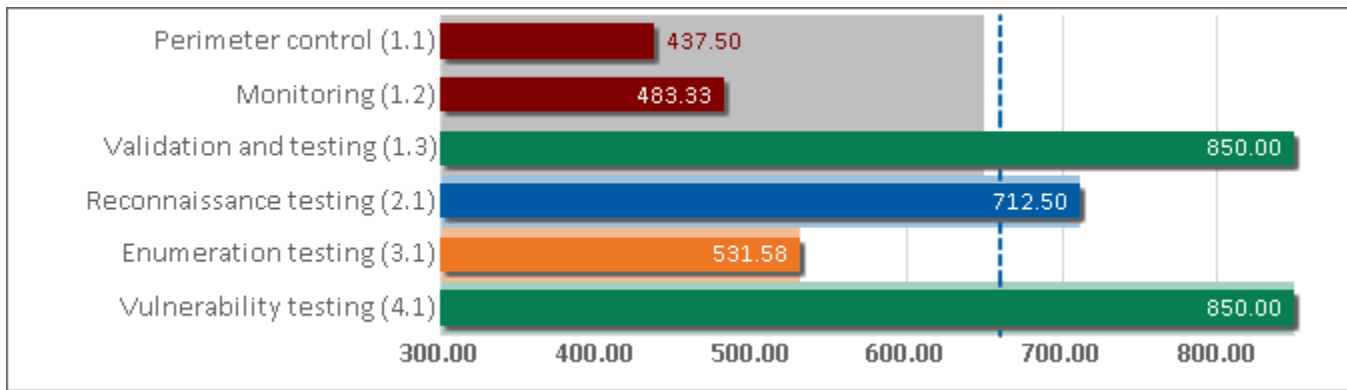
Top External Technical Controls Recommendations

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.