Wayzata City Council Workshop Meeting Agenda
Wayzata City Hall Community Room, 600 Rice Street
TUESDAY, MARCH 8, 2022

WORKSHOP TOPICS FOR DISCUSSION:

1. Review of Proposal from FRSecure to Conduct a Cyber Security Assessment (5:20-5:50 p.m.)
2. Update of Preferred Platform Tennis Facility Location and Discussion of Next Steps (5:50-6:20 p.m.)
3. Discussion of Volunteer Coordination Structure (6:20-6:30 p.m.)

City Council Workshop
City Council Agenda Report

MEETING DATE: March 8, 2022	**WORKSHOP AGENDA ITEM:** 1
TITLE: Review of Proposal from FRSecure to Conduct a Cyber Security Assessment (5:20-5:50 p.m.)	
PREPARED BY: Aurora Yager, Administrative Services Director	
REVIEWED BY: Jeffrey Dahl, City Manager	

DISCUSSION OBJECTIVE:

To review the proposal from FRScure for a cyber security assessment and ask questions.

BACKGROUND:

At the February 22, 2022 Council Meeting, staff submitted a proposal for FRSecure to perform a cyber security assessment. Given the increase in cyber attacks, it is important for the City of Wayzata to have a cybersecurity assessment completed to identify and then minimize the risk to the City as much as possible. This assessment has been planned and budgeted for several years and is identified as an initiative in the Strategic Plan.

The proposal from FRSecure includes an S2Org assessment which will include interviews with staff and evaluation of our administrative, physical, and technical controls. FRSecure has worked with a number of Minnesota cities on this issue and comes highly recommended. Findings from this study will be given to select staff and the City's IT provider, Loffler, to review and create an implementation plan. Given the highly technical and specialized nature of this work, FRSecure will be present at the meeting to give an overview of their company, their process, the proposal, and to answer any questions from the Council.

ATTACHMENTS:

1. FR Secure Proposal - Cybersecurity Risk Assessment

FRSECURE®

A Proposal For

Risk Assessment with Roadmap and IR Retainer

Prepared For

City of Wayzata

Prepared for:

Jeff Dahl
City Manager
City of Wayzata

Prepared By:

John Williams
jmwilliams@frsecure.com
(651) 728-6825

Date: Feb 4, 2022

Feb 4, 2022

Jeff Dahl, City Manager
City of Wayzata
600 Rice St E Wayzata MN 55391

Thank you for your time and consideration of this proposal.

At FRSecure, we are called to a mission of fixing the broken security industry. Our focus resides in helping our peers and clients master the fundamentals of information security through establishing a common language, providing low or no cost training and resources and by building the very best security professionals in the industry. Our objectivity in guiding you rests in our product agnostic stance and the core values shared by each and every member of our team.

Whether or not we formally engage, please count on us to be a resource and help us keep you informed as we make our training and expertise available to the community. Our passion for information security as our sole focus is the driving force to our current and future success.

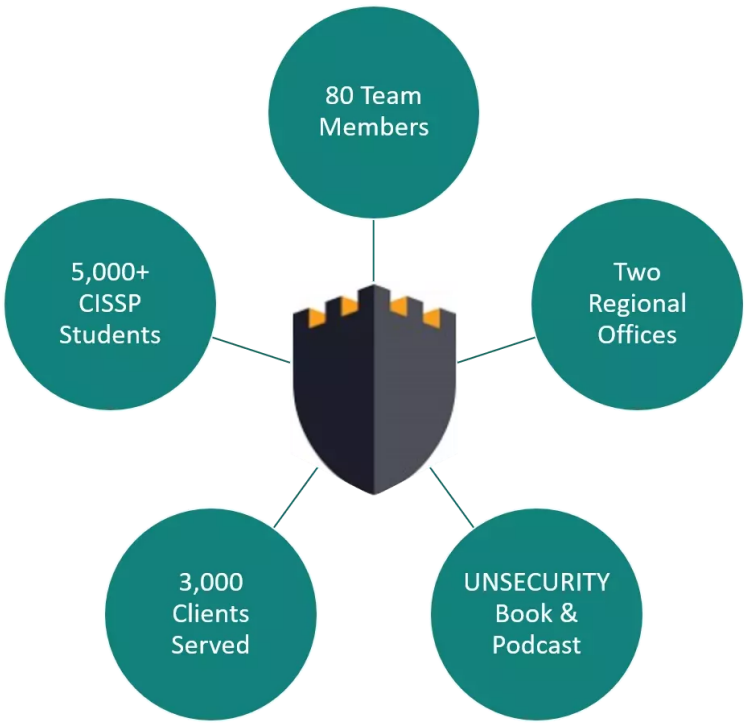
We hope our proposal today adds to our already positive relationship, where our mission is put to work meeting your information security objectives.

Respectfully yours,

Evan Francen
FRSecure Founder & CEO

FRSECURE® Security Experts on a Mission

The information security industry is broken. We are on a mission to fix it. By staying true to our mission, our commitment to product agnostic services and living our core values, we've developed a community of like-minded individuals, clients and partners. All we do is information security.



Consulting & Compliance Services

- Security Risk Assessment
- Virtual CISO
- Remediation Planning & Support
- PCI DSS Compliance & Audit
- HIPAA Compliance
- GDPR & CCPA Compliance
- SOC 2 Readiness
- NIST & CMMC Compliance
- ISO Audit Readiness

Technical Services

- Network Penetration Testing
- Web Application Penetration Testing
- Wireless Network Penetration Testing
- Physical Penetration Testing
- Vulnerability Testing
- Social Engineering
- Digital Forensics
- Incident Response

Additional Information Available on FRSecure.com

- Team Certifications
- Team Profiles
- Industry Expertise
- Free Tools
- Blogs & Security Advice
- CISSP Mentor Program Details

Statement of Work

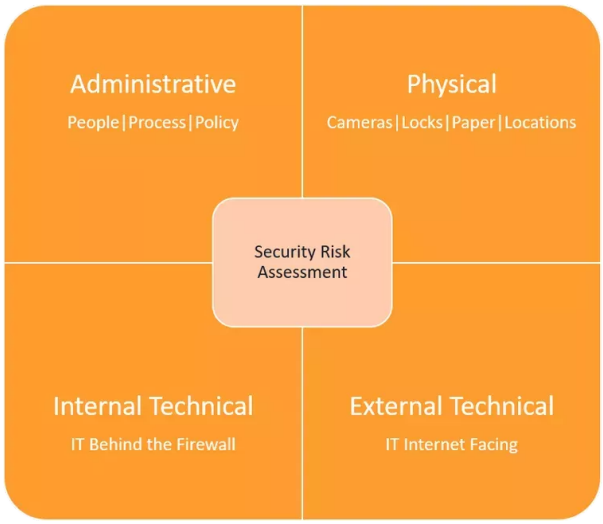
The information contained within this document is a proposal and formal statement of work, if accepted by City of Wayzata by execution of this document.

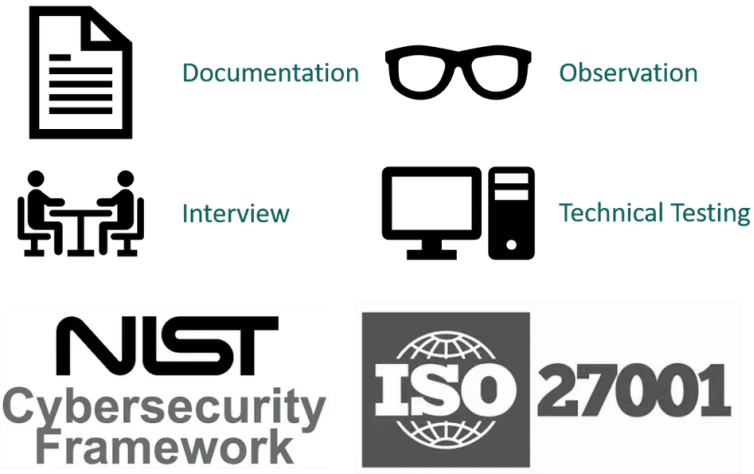
Engagement Overview

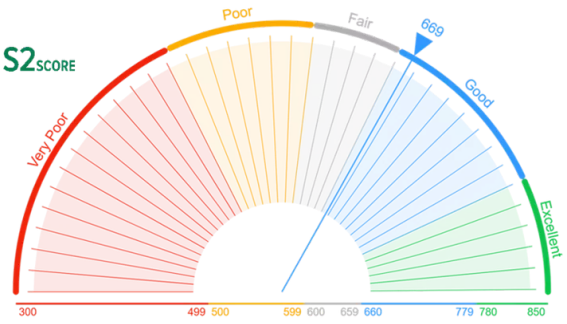
Purpose and Objective	Proposed Solution	Timing
A comprehensive assessment of the organization's information security posture	Information Security Risk Assessment • Administrative Controls • Physical Controls • Technical Controls • S2Score & Reporting	4-6 weeks
Determine the Who, What and When for addressing identified risks.	Roadmap	1-2 weeks
Reserve resources for help with a cyber incident	IR Retainer	12 months

Information Security Risk Assessment

FRSecure's information security risk assessment is meant to find the measurable baseline for your security posture and prioritize remediation efforts for the most impactful items. A security assessment is always the first step to building a functioning, measurable security strategy.



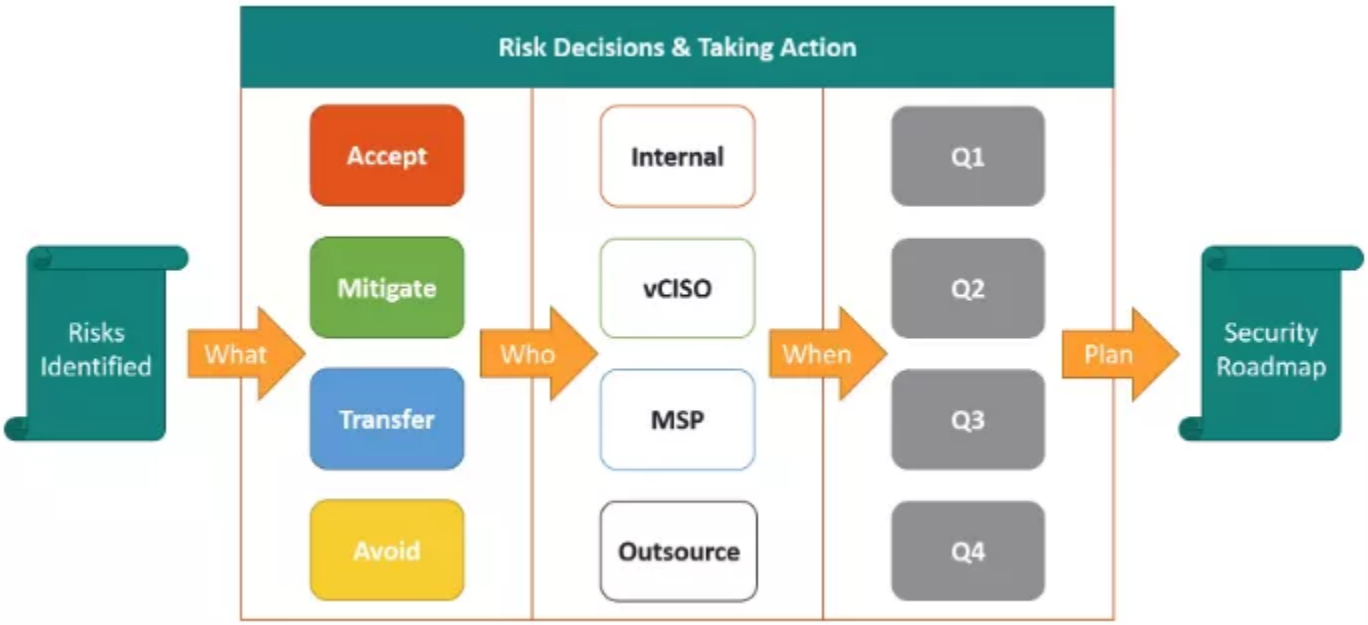




Detailed information available in the Approach and Process section at the end of the proposal.

Security Program Roadmap

Building a functioning, successful security strategy lies in planning and preparation. Once risk is measured and recommendations are identified, the next step is to determine how to address the identified risks, determine who will own the execution of those decisions and when to act. The security program roadmap is designed to facilitate and document each step.



Cyber Security Incident Response Services Program Overview

1. Cyber Security Incident Response Managed Service
2. Cyber Security Incident Response Retainer Services
3. Cyber Security Incident Response Registration Service
4. Emergency Cyber Security Incident Response Service

IR Managed Service

This offering will provide our customers with a designated Incident Response Manager who familiarizes themselves with the client environment upon contract signature.This designated resource will spend time with you to understand your environment, provide policy guidance, as well as training of in-house staff of how to properly respond and manage an identified incident.

Prepaid hours will be utilized for all incident containment, eradication, forensic services, reporting, and other services as required. Managed Service includes weekly call, ongoing email support, annual Cyber Security Incident Response capabilities assessment, as well as assisting customers in creation and maturation of their CSIRP. Managed services customers will be prioritized in the unfortunate event of a security incident.

Emergency Cyber Security Incident Response Service & Cyber Security Incident Response Retainer Services

FRSecure Emergency Cyber Security Incident Response service provides our clients with a comprehensive approach for security incident response. When an incident arises, and you need immediate response, FRSecure will be there to assist! This service will provide expert response, support, and triage in the event of a suspected security incident. You will be assigned an experienced incident response expert within the FRSecure Incident Response Team to ensure that your incident is properly handled.

IR Registration Service

Setup and registration with FRSecure's IR Registration Service ensures that your organization has a completed Master Services Agreement (MSA) on file, and has provided the FRSecure CSIRT with basic IR plan documents and network configuration in the event its needed by our IR Response team in an emergency situation. This saves valuable triage time and cost, as well as provides an assurance to your insurance provider that FRSecure's team of information security experts can respond without delay.

Engagement Scope Details

Scope Information	Scope Details
Security Risk Assessment - L2 - Number of users - Number of physical locations - Number of internal IP addresses Laptops/Workstations/Servers/Network Devices - Number of active external IP addresses	 - Approximately 55 - 1 Location (City Hall & Police Department - Approximately 100 - 10

Engagement Planning

Engagement	Begin Date - End Date
Security Risk Assessment - L2	October 2021

The success of this engagement will be assured by your Client Success Manager in partnership with our Information Security Experts and Project Management Team.

We encourage you to include the entire team in relevant communications, but please consider your Client Success Manager as your go-to for anything you need.
Every engagement begins with formal initiation procedures.

1. Introductions to respective teams and their roles in the engagement
2. Establishment of communication preferences
3. Confirmation of scope and service levels expectation
4. Confirmation of timing and constraints
5. Engagement completion expectations and due date for deliverables

Support Team

Name	Title	Contact
John Williams	Senior Account Executive	jmwilliams@frsecure.com
Caleb Phillips	Client Success Manager	cphillips@frsecure.com
Chad Spoden	Sr. Security Analyst & Solution Architect	cspoden@frsecure.com
Executive Leadership Team		
John Harmon	President	jharmon@frsecure.com
Renay Rutter	Chief Operating Officer	rrutter@frsecure.com
Vanae Pearson	Chief Financial Officer	vpearson@frsecure.com

Engagement Investment

Name	Price	QTY	Subtotal
☑ Risk Assessment - L2	$12,500.00	1	$12,500.00
☐ Roadmap	$3,500.00	1	$3,500.00
☑ IR Registration Service - A $1,000 value	$0.00	1	$0.00
☐ IR Retainer Service prepaid hours (25) Bundle of 25 hours (Invoiced at acceptance of agreement)	$400.00	25	$10,000.00

Total (USD) **$12,500.00**

This proposal expires in 60 days

Please note that multi-year options typically amortize the 1st and/or 2nd year costs. If City of Wayzata cancels this agreement prior to the completion of the term selected, City of Wayzata agrees to pay the full amount of services pursuant to Section 2.E of the Master Services Agreement between City of Wayzata and FRSecure.

Customer Acceptance

City of Wayzata

_____

_____

Signature of Authorized Agent Date

Contact Information

FRSecure LLC
Attn Vanae Pearson
5909 Baker Road Suite 500
Minnetonka, MN 55345
Phone 612-230-0427
Email vpearson@frsecure.com

Assumptions

FRSecure will provide all of the materials required for the completion of this engagement. FRSecure will rely upon experience, testing, observation, and interviews with City of Wayzata employees to assess the completeness and effectiveness of City of Wayzata's information security program. FRSecure will follow all guidance provided by the previously referenced standards for the completion of the work.

The FRSecure information security analyst will review a variety of information including, but not necessarily limited to prior working papers, reviews and current City of Wayzata diagrams, policies, processes, and procedures.
Assessments that have been conducted follow the standards as noted in the National Institute of Standards in Technology Cybersecurity Framework (NIST CSF), ISO/IEC 27002:2013 international standard, Center for Internet Security (CIS) Controls, & NIST Special Publication 800-53 (NIST SP 800-53).

Change Management Process

Changes can be made to the scope of this engagement and Statement of Work. Any changes requested by either party should be in writing and signed by both parties indicating acceptance.

Engagement Related Expenses

All engagement related expenses will be billed to the client following FRSecure Client Project Travel And Expense Policy.

Invoicing Details

For one-time project agreements (i.e. assessments), a down payment invoice of 50% will be sent upon acceptance of this proposal and statement of work. The balance is due upon engagement completion of all deliverables to City of Wayzata. For multi-year or multi-project agreements, a down payment invoice of 50% will be sent at the beginning of the year in each year or term in which the project is performed. The balance is due upon engagement completion of all deliverables to City of Wayzata. Monthly or quarterly recurring consulting agreements, or projects with an amortized payment schedule, will be invoiced quarterly starting on the 1st day of the first month services begin.
City of Wayzata may cancel this engagement at any time pursuant to Section 2.E of the Master Services Agreement between City of Wayzata and FRSecure. Cancellation or rescheduling of an engagement by City of Wayzata may result in additional fees.
City of Wayzata may reschedule this engagement at any time and will be invoiced for costs incurred to date including an additional 20% rescheduling fee.
Meetings cancelled by City of Wayzata less than 5 business days prior to a FRSecure resource commitment of four or more hours, will result in a reschedule fee for time and expenses lost.
Failure to return a workbook from FRSecure within 9 business days will result in a late fee of up to 10% of the project cost.
Note: Prices shown do not include sales tax, if applicable.
Please note, failure by City of Wayzata to respond to repeated attempts at communications by FRSecure within 90 days of initial communication of project initiation will result in project engagement closeout and City of Wayzata will be invoiced for full remaining balance due as described in this statement of work. For payments made by credit card, a 3% convenience fee will be added.

Practice Lead

Director of Professional Services & Innovation

BRAD NIGH
5909 Baker Road, Suite 500, Minnetonka, MN 55345
linkedin.com/in/bradnigh
bnigh@frsecure.com
(952) 467-8849

PROFILE

Brad is a passionate information security expert with 20+ years of overall IT experience, including 10+ years of IT management and leadership experience working in 24/7 environments that required top tier technical skills, and efficient project management. In addition, Brad has several years of experience working in highly regulated industries that are required to comply with PCI-DSS, HIPAA, HITECH, Sarbanes-Oxley, OCC, and various state regulatory requirements.

At FRSecure Brad leads the Professional Services practice, serving businesses of all sizes and in all industries by cooperatively solving the complex issues surrounding information security. Brad's goals are ensuring consistent methodology, improving our existing programs, and innovating and continual development of new offerings.

EDUCATIONAL & COMMUNITY SERVICE ENGAGEMENTS

- CISSP Mentorship Program
- FRSecure Workshop Series
- ISC2 Safe & Secure Online Volunteer
- Wayzata Public Schools COMPASS Mentor (Cybersecurity)

CERTIFICATIONS

- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Certified Security Studio Analyst (CSSA)
- MCSA: Windows Server 2012
- ITIL v.3 Foundations
- Certified Incident Handler (ECIHv2)
- CMMC Certified Registered Practioner (CMMC-RP)

Value Proposition

Based on the conversations between FRSecure and City of Wayzata to date, we believe we are an excellent fit for your engagement.

Here are some additional reasons we believe you should select FRSecure:

- **FRSecure's Methodology** – FRSecure has developed a proprietary approach to assessing information security risks. It's more than a checklist of questions and recorded answers. Our approach gives you a full picture of your risks - prioritized and rated - with recommended solutions, so you know which security investments will have the greatest impact.
- **FRSecure's Project Leader** – All of our project leaders have more than 15 years of information security experience as a leader in, and consultant for hundreds of companies ranging from the Fortune 100 to SMBs. BIO's for our project leaders are available upon request.
- **Full Transparency** – FRSecure strongly believes in empowering our customers. The more knowledge transfer that occurs during our engagement, the more value our customers recognize. FRSecure fully discloses the methods, tools, and configurations used to perform analysis work for our customers in the hope that they can easily adopt our processes for their future benefit.
- **Product Agnostic** – FRSecure does not represent any third-party products or services; on purpose. Our projects and recommendations stand on their own, with no ulterior motive to sell you things you don't really need.

FRSecure Information Security Principles

Our Information Security Principles are fundamental to our everyday work and help us to stay focused on our mission to "Fix the Broken Industry". All our Principles are able to stand by themselves, but they are also solidly interrelated.

1. **A business is in business to make money**
   Information security must align with business objectives.
2. **Information Security is a business issue**
   Information security is NOT an IT issue.
3. **Information Security is fun**
   That's right, we said "FUN"!
4. **People are the biggest risk**
   Not technology.
5. **"Compliant" and "secure" are different**
   We shouldn't confuse the two.
6. **There is no common sense in Information Security**
   If there were, we would have better information security.
7. **"Secure" is relative**
   One of many reasons for ongoing measurements and comparisons.
8. **Information Security should drive business**
   Identify and focus on information security benefits. Information security shouldn't just be a cost-center.
9. **Information Security is not one size fits all**
   No two businesses are exactly alike.
10. **There is no "easy button"**
    So stop looking for one.

Client references available upon request

Approach and Process

Information Security Risk Assessment with S2Org® and S2Score®

The S2Score®, available through the SecurityStudio® software platform is the most objective and comprehensive measurement of information security risk available in the market. It was designed by engineers at FRSecure, who average more than 15 years of information security experience, with these specific objectives in mind:

- Serve as the **foundational** risk score and measurement.
- **Based on risk**. The most effective way to manage information security is based on risk, not on specific controls that may or may not fit for your organization.
- **Easy to understand**. *Easy to understand* and *effective* are not mutually exclusive. In fact, they usually go hand in hand. The most effective information security programs are typically simple and effective. Complexity is often the enemy to good security.
- **Comprehensive**. Information security is not an IT issue; it is a business issue.
- **Objective**. Scoring is as objective as is possible given what we know about threats, vulnerabilities, exploits and risk in general. Each assessed control is given a risk metric based on professional opinions, best practices, and real-life data.
- **Clear and free from technical jargon**. Terms like "NextGen", "Internet of Things" (IoT), "Advanced Persistent Threats" (APT), etc. are all avoided as much as possible.
- **Industry accepted and credible**. The assessment leverages and references current security frameworks and standards such as ISO/IEC 27001:2013 and the NIST Cybersecurity Framework (CSF). This is very good news for organizations that have built their information security programs per one or more of these frameworks and helps to lend to the credibility of the assessment.
- **One-stop.** The type of assessment that can be used to measure the effectiveness of the security program, provide high-quality next steps (or recommendations), demonstrate regulatory compliance (HIPAA, GLBA, and others), and allow for effective cyber insurance underwriting*

*NOTE: The S2Score® is **approved for cyber insurance underwriting** submission through Node International and Lloyd's of London.

The S2Org® Assessment is built to be the definitive and best information security risk assessment methodology available with reporting designed to be easy to manage and actionable.

Each phase, control category, control subcategory, and the overall S2Org® assessment is calculated based upon

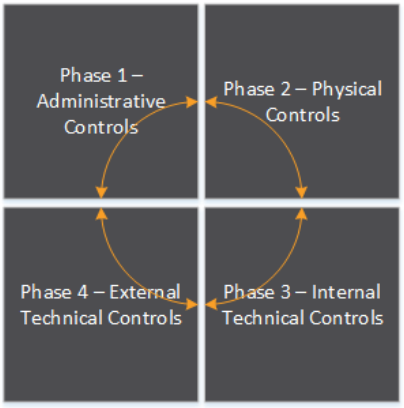
1. The size of the organization
2. The industry in which the organization operates
3. Historical threat and incident data obtained from a variety of source.

Scope

The intended scope for the S2Org® is the entire organization. Information security is a very broad topic so to ensure a comprehensive assessment, that is still easy to understand, the S2Org® assessment is segmented into four (4) phases.

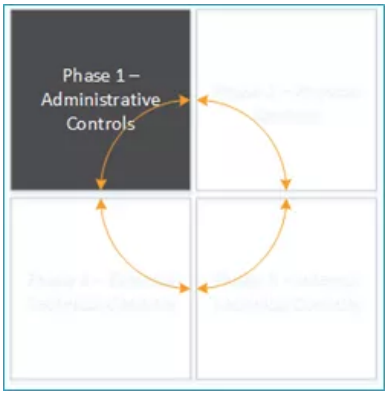
The four phases of a S2Org® assessment are:

- **Phase 1: Administrative Controls** – The "people" part of security, including risk management, security governance, policies, standards, training and employee awareness.
- **Phase 2: Physical Controls** – Physical controls are an essential and often overlooked part of your security strategy. How much does your anti-virus protection mean to you if someone steals your server?
- **Phase 3: Technical Controls (Internal)** – We affectionately call this "the gooey center". Most organizations do a pretty good job at securing the technical perimeter (firewalls, intrusion detection, etc.), but sometime neglect the controls that are essential for an effective defense-in-depth strategy.
- **Phase 4: Technical Controls (External)** – This category covers how effective your organization is at securing the perimeter of your network.



The S2Org™ process and simple and efficient. We understand that our clients have other work to do, so the process needs to be focused and time-sensitive. Each phase of the S2Org® assessment is slightly different in the manner that information is gathered and assessed.

Phase 1 – Administrative Security Controls Assessment



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.

Administrative Controls are derived from the NIST Cybersecurity Framework (CSF), ISO/IEC 27001:2013, NIST SP 800-53, and the CIS Critical Security Controls for reference, comparison, gap analysis, and risk rating.

Where there are *applicable* gaps, the following metrics are applied using the S2Org® proprietary algorithm:

- Information Security **Maturity** ("ISM") - a measure of control quality and maturity,
- **Likelihood** of an adverse event or realized threat, and the potential **Impact** suffered by the organization; resulting in a **Risk Rating**.

Phase 1 – Administrative Security Controls is further segmented into the following 10 control categories which contain a total of 42 subcategories:

Control	Risk Management
1.1	Risk Management Practices and Integration
1.2	Risk transfer and insurance
Control	**Information Security Governance**
2.1	Policies for information security
2.2	Review of the policies for information security
2.3	Security roles and responsibilities
2.4	Segregation of duties
Control	**Human Resources Security**
3.1	Screening
3.2	Management responsibilities
3.3	Information security awareness, education, and training
3.4	Specialized information security education and training
3.5	Termination or change of employment responsibilities
Control	**Asset Management**
4.1	Inventory of assets
4.2	Classification of information
4.3	Management of removable media
4.4	Disposal of media
4.5	Cloud service security management
Control	**Access Control**
5.1	Access control policy
5.2	Account management
5.3	Use of authentication information
5.4	Secure log-on procedures
Control	**Encryption**
6.1	Encryption policy and control

Control	Security Operations
7.1	Mobile device policy
7.2	Teleworking
7.3	Documented operating procedures
7.4	Change management
7.5	Controls against malware
7.6	Information backup
7.7	Event logging
7.8	Installation of software on operational systems
7.9	Management of technical vulnerabilities
7.10	Information systems audit controls
7.11	Network security
7.12	Information transfer policies and procedures
7.13	Information security requirements analysis and specification
7.14	System acceptance testing
7.15	Third-party security risk management
Control	**Incident Management**
8.1	Incident management roles and responsibilities
8.2	Incident response procedures
Control	**Business Continuity Management**
9.1	Planning information security continuity
9.2	Recovery plan details
Control	**Compliance**
10.1	Identification of applicable legislation and contractual requirements
10.2	Privacy and protection of personally identifiable information
10.3	Independent review of information security
10.4	Compliance with security policies and standards
10.5	Protections against financial fraud

The Administrative Controls are assessed through:

1. Documentation review
2. Interviews with the FRSecure Analyst
3. Observations made by the FRSecure Analyst

Phase 2 – Physical Security Controls Assessment

Physical Controls are the security controls that can often be touched and provide physical security to protect your information assets. Common physical controls include doors, locks, camera surveillance, and alarm systems.

Phase 2 of the S2Org® assessment is a review of these, and other, physical security controls and associated risks. Focus for the Phase 2 of the assessment will be on where critical information resources are physically located.

Phase 2 takes the following into consideration to generate a definitive risk score:

Control	Crime Index
1.1	Crime Index
Control	**Natural Disasters**
2.1	Natural Disasters
Control	**Facility Security**
3.1	Planning and preparedness
3.2	Perimeter controls
3.3	Entry controls
3.4	Public spaces
3.5	Office spaces
3.6	Restricted areas
3.7	Delivery and loading areas
Control	**Equipment and Information**
4.1	Equipment siting
4.2	Supporting utilities
4.3	Cabling security
4.4	Maintenance
4.5	Housekeeping
4.6	Clear desk/screen

The Physical Controls are assessed through:

1. Documentation review
2. Interviews with the FRSecure Analyst
3. Observations made by the FRSecure Analyst

Phase 3 – Internal Technical Controls Assessment

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).

Phase 3 reviews these controls using a combination of interviews with staff and use of tools to perform:

- Vulnerability scanning on the internal network(s),
- Tests for password policies, system permissions, required auditing and system settings that are common in all networks.
- Tests for user auditing settings, such as their password complexity and logging access failures and logons that are common in all networks.
- Tests against known good configurations

Phase 3 of the S2Org® assessment consists of the following control sections:

Control	Network Connectivity
1.1	Internet
1.2	Wide Area Network (WAN)
1.3	Local Area Network (LAN)
1.4	Wireless Local Area Network (WLAN)
Control	**Remote Access**
2.1	User remote access
2.2	Third-party remote access
Control	**Directory Services**
3.1	Directory security
3.2	Directory policy
3.3	Directory resilience
Control	**Servers and Storage**
4.1	Server software
4.2	Server hardware
4.3	Storage

Control	Client Systems
5.1	Client software
5.2	Client hardware
Control	**Mobile Devices**
6.1	Phones and tablets
6.2	Laptops
Control	**Logging, Alerting, and Monitoring**
7.1	Performance
7.2	Events and incidents
7.3	Aggregation and correlation
7.4	Trust
Control	**Vulnerability Management**
8.1	Microsoft software and applications
8.2	Non-Microsoft operating systems
8.3	Validation
Control	**Backup and Recovery**
9.1	Backups
9.2	Backup storage
9.3	Disaster recovery and business continuity
9.4	Backup validation

FRSecure discloses the tools, methods, and configurations employed during testing to enable your personnel to conduct future testing on a regular basis.

The Internal Technical Controls are assessed through:

1. Documentation review
2. Interviews with the FRSecure Analyst
3. Observations made by the FRSecure Analyst
4. Tools run by FRSecure or your personnel

Phase 4 – External Technical Controls Assessment

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.

The primary objective of the External Technical Controls Assessment and testing exercise is to identify significant vulnerabilities that pose a risk of unauthorized information disclosure, alteration, and/or destruction through publicly accessible* information resources.

*Publicly accessible is defined as those resources which are purposefully or accidentally made available through the Internet.

Phase 4 of the S2Org® assessment consists of the following control sections:

Control	Best Practices
1.1	Perimeter control
1.2	Monitoring
1.3	Validation and testing
Control	**Reconnaissance**
2.1	Reconnaissance testing
Control	**Enumeration**
3.1	Enumeration testing
Control	**Vulnerabilities**
4.1	Vulnerability testing

The External Technical Controls are assessed through:

1. Documentation review
2. Interviews with the FRSecure Analyst
3. Tool and manual testing conducted by the FRSecure Analyst

Assessment Deliverables

City of Wayzata will be provided with the following deliverables as part of this engagement:

S2Score®

One of the most important end results from the S2Org® assessment engagement is your S2Score®. You will be provided with your overall S2Score® as well as a S2Score® for each Phase, control category, and individual control sub-category. This is important for your organization as you identify your most significant risks and prioritize remediation.

The S2Score® can be used to communicate your "risk score" to interested parties and is a definitive risk calculation.

The overall S2SCORE (or risk rating) is **678.72.**

The S2Score® is represented on a scale of 300 – 850.

- 300 – 500 is generally considered to be **"Very Poor"**
- 501 – 599 is generally considered to be **"Poor"**
- 600 – 659 is generally considered to be **"Fair"**
- 660 – 779 is generally considered to be **"Good"**
- A score equal to or higher than 780 is generally considered to be **"Excellent"**

Most organizations should be striving to attain and maintain a score of 660 or higher.

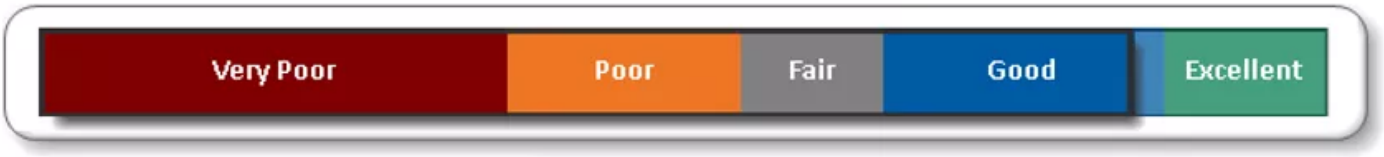
S2Org® Executive Summary Report

The S2Org® Executive Summary report is written in plain English with comparisons to other organizations; with a similar profile. It provides the necessary information to quickly understand where your organization's information security program excels and where it is deficient. The snapshot views allow solid decision-making now (tactically) and into the future (strategically).

S2SCORE Scale

S2SCORE Average Across Industries

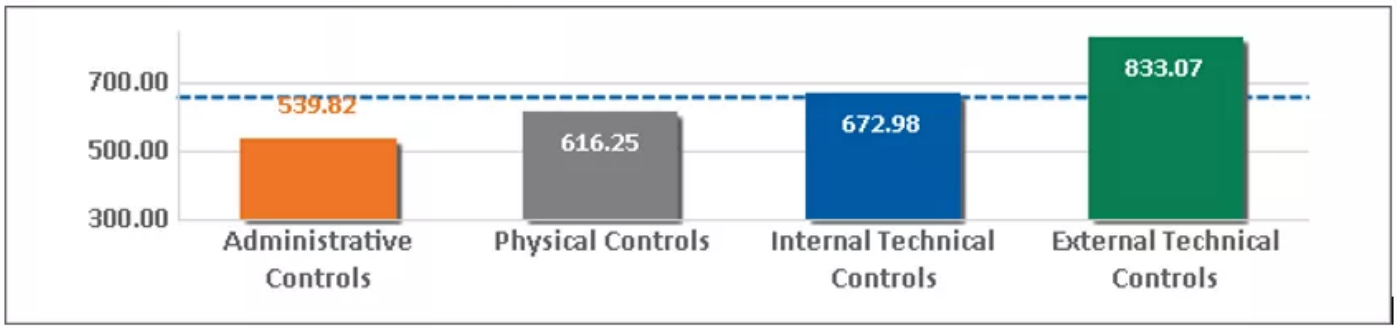
Industry: All Industries



The average S2SCORE is **766.05** across all industries. According to our calculations, there is roughly 11.4% more risk in the Fossa University 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.



S2Org® Information Security Assessment Full Report

The S2Org® Full Report is written with information security professionals in mind. All the details involved with what was assessed, how it was assessed (including tools and logic), findings, and recommendations are provided. The S2Org® Full Report is also supported with numerous other documents, technical testing results, and raw data. All supporting information is referenced and provided.

How to Use This Report

There are four primary purposes for this report:

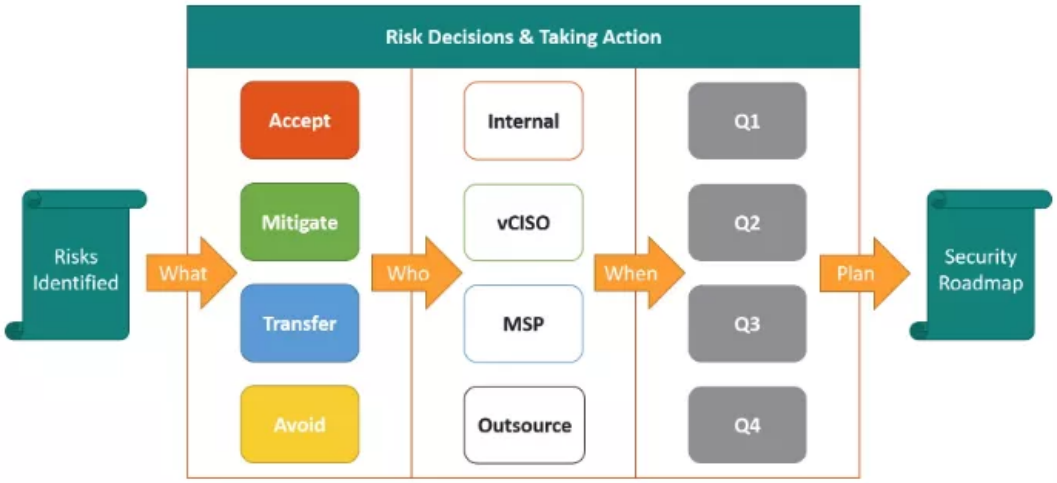
1. To understand how mature your organization's information security program is.
2. To understand where your organization's information security risks are.
3. To build a plan of action on how you should address your most significant unacceptable risks.
4. To demonstrate compliance with industry regulations (HIPAA, GLBA, and others) and customers/business partner requirements

In order to gain the most benefit from the contents of this report, it is recommended that you read the report in its entirety and develop a plan of action. Information security is a lifecycle discipline that requires a long-term commitment. In order to get the most benefit from this report, create an action plan for your organization.

Control	Risk Management	Maturity	S2SCORE	
1.1	Risk Management Practices and Integration	3.33	721.74	719.05
1.2	Risk transfer and insurance	4.00		723.08
Control	**Information Security Governance**	**Maturity**	**S2SCORE**	
2.1	Policies for information security	1.00	450.99	437.50
2.2	Review of the policies for information security	1.88		618.42
2.3	Security roles and responsibilities	0.62		346.81
2.4	Segregation of duties	0.00		300.00
Control	**Human Resources Security**	**Maturity**	**S2SCORE**	
3.1	Screening	0.00	438.44	300.00
3.2	Management responsibilities	0.71		422.22
3.3	Information security awareness, education, and training	1.88		489.66
3.4	Specialized information security education and training	1.00		355.00
3.5	Termination or change of employment responsibilities	2.78		575.00
Control	**Asset Management**	**Maturity**	**S2SCORE**	
4.1	Inventory of assets	1.67	580.07	483.33
4.2	Classification of information	0.00		300.00
4.3	Management of removable media	4.25		793.10
4.4	Disposal of media	0.71		359.46
4.5	Cloud service security management	4.44		768.52

S2Org® Roadmap

The primary purpose of the Security Program Roadmap is to empower you to be able to choose which tasks you want to take on and which tasks you want to assign to external resources, and provide a strategic Roadmap for completion of all tasks. All actions are measurable and easily communicated.



Improvement comes through putting the recommendations from the assessment into practice by:

1. Making risk-based decisions about what to do with each recommendation.
2. Assigning responsibility for actions that must be taken.
3. Determining the priority for such actions and assigning deadlines/timelines.

Activities for the Roadmap are driven from the S2Org® assessment.
The FRSecure Analyst creates the initial roadmap (or plan) for your information security program over the next 12, 24, and 36 months

The Security Program Roadmap tackles the planning of "what", "who", and "when" for information security improvement:

- What are we going to do with each of the findings and recommendations from the S2Org®? There are four viable options for decision-making:
  - *Accept* – the risk "as-is" and take no corrective actions but continue to monitor the risk
  - *Mitigate* – the risk and do what the recommendation says (or similar)
  - *Transfer* – the risk and/or defer it for insurance (or similar)
  - *Avoid* – the risk and stop doing the actions that led to the risk in the first place
- Who is going to do the actions and carry out the decisions that were made? Decisions such as "Mitigate" and "Avoid" made in the previous step will require somebody to do something. Some of the tasks and/or projects can be done internally with your own resources and some of the tasks and/or projects will require outside assistance. Those tasks and/or projects that require outside assistance can be assigned to the vCISO (Step 4) and some of the tasks and/or projects can be assigned to another party.
- When will the actions need to be taken to achieve your goals? It's best to assign the tasks and/or projects to a timeline based on quarters to accommodate day-to-day operational challenges along the way.

The information from S2Org® and the Roadmap can be easily communicated to stakeholders (Board of Directors, executive management, examiners/regulators, customers, etc.) includes:

- What our current S2Score® is.
- What our S2Score® goal is.
- What tasks and/or projects are necessary to meet objectives.

Cyber Security Incident Response Services Program Overview

1. Cyber Security Incident Response Managed Service
2. Cyber Security Incident Response Retainer Services
3. Cyber Security Incident Response Registration Service
4. Emergency Cyber Security Incident Response Service

IR Managed Service

This offering will provide our customers with a designated Incident Response Manager who familiarizes themselves with the client environment upon contract signature.This designated resource will spend time with you to understand your environment, provide policy guidance, as well as training of in-house staff of how to properly respond and manage an identified incident.Your dedicated resource will be there to help you work through any incidents that may arise in your environment. Beginning with containment and assisting you all the way through the triage process to ensure complete containment, eradication, and recovery from the threat.

Your designated Manager will assist you through all Cyber Security Incident Response planning and management as well as engage in ongoing communications and cyber threat intelligence sharing to ensure you are properly prepared to respond to a Cyber Security Incident.Your Manager will be there to support you in audit and regulatory compliance as needed.

Prepaid hours will be utilized for all incident containment, eradication, forensic services, reporting, and other services as required. Managed Service includes weekly call, ongoing email support, annual Cyber Security Incident Response capabilities assessment, as well as assisting customers in creation and maturation of their CSIRP. Managed services customers will be prioritized in the unfortunate event of a security incident.

Emergency Cyber Security Incident Response Service & Cyber Security Incident Response Retainer Services

FRSecure Emergency Cyber Security Incident Response service provides our clients with a comprehensive approach for security incident response. When an incident arises, and you need immediate response, FRSecure will be there to assist! This service will provide expert response, support, and triage in the event of a suspected security incident. You will be assigned an experienced incident response expert within the FRSecure Incident Response Team to ensure that your incident is properly handled.
FRSecure Emergency Incident Response service & Cyber Security Incident Response Retainer Services are delivered as detailed in the table below. For customers looking for ongoing support, we recommend you review our Incident Response Managed service capability.

IR Registration Service

Setup and registration with FRSecure's IR Registration Service ensures that your organization has a completed Master Services Agreement (MSA) on file, and has provided the FRSecure CSIRT with basic IR plan documents and network configuration in the event its needed by our IR Response team in an emergency situation. This saves valuable triage time and cost, as well as provides an assurance to your insurance provider that FRSecure's team of information security experts can respond without delay.

Cyber Security Incident Response Services Comparison - SLA

	IR Emergency Response	IR Registration Service	IR Retainer Services	IR Managed Service
Incident Response Program Development	-	-	• Monthly Checkpoints • External Vulnerability Scan (10 IPs) • Dedicated CSIRT Hotline	• Dedicated Liaison • 30 Hour Readiness Assessment • IR Report/Roadmap • External Vulnerability Scan (25 IPs) • 24/7/365 Phone and Email support • Weekly Checkpoints • Threat Intelligence • Incident Response Tabletop • Dedicated CSIRT Hotline
IR hours expiration from purchase date	-	-	• Under 200 hours - 1 year • 200+ hours - 2 years	• Under 200 hours - 1 year • 200+ hours - 2 years
Dedicated CSIRT Hotline	-	-	Yes	Yes
Response Time* - Email/Telephone - Business Hours	Best Effort	Best Effort	4 hours	2 hours
Response Time* - Email/Telephone - Non-Business hours	Best Effort	Best Effort	8 hours	6 hours
Response Time* - On-site, Continental U.S.	Best Effort	Best Effort	24 hours En Route	24 hours En Route
Remote Containment Phase activity response	Varies by Severity Level	Varies by Severity Level	Varies by Severity Level	Varies by Severity Level
Unused Hours can be applied to other services	-	-	Yes	Yes
IR Registration Service	-	$1,000	Included	Included

Cyber Security Incident Response Services Comparison - Additional Services

IR Services Available*	IR Retainer Service	IR Managed Service
External Vulnerability Scan with Recon	✔	✔
Incident Response Plan Review	Available	✔
Incident Response Readiness Assessment	Available	✔
Ransomware Readiness Assessment	Available	✔
Incident Response Tabletop	Available	✔
Cyber Threat Intel	Available	✔
Executive and Management Preparation (Board Included)	Available	✔
Red Team Assessment	Available	Available
Penetration Testing	Available	Available
Social Engineering (Spear, Voice, Physical)	Available	Available
Digital Forensics	Available	Available
Malware Analysis	Available	Available
Incident Response Plan Drafting	Available	Available
Security Operations Center Development Exercise	Available	Available
Threat Hunting	Available	Available

IR Services Available*	Description	IR Retainer Service	IR Managed Service
External Vulnerability Scan with Recon	A vulnerability scan of public facing hosts along with some evaluation of public source information to determine if an attacker could use that info to build an attack.	✔	✔
Incident Response Plan Review	Detailed review of your current IR plan that will provide feedback and recommendations to increase your maturity level and close identified gaps.	Available	✔
Incident Response Readiness Assessment	Custom developed assessment that will review your current capabilities through the standard IR six step response process. Preparation; Identify; Contain; Eradicate; Recover; Lessons Learned. This assessment will allow us to identify strengths and weaknesses in your current capabilities as well as provide a road map for incident response maturity.	Available	✔
Ransomware Readiness Assessment	A focused assesment of an organizations abilities to property deal with a ransomeware outbreak. Tools, processes and procedures are evaluated to determine how impactful a ransomeware event could be as well as determining how the staff is able to deal with such an event.	Available	✔
Incident Response Tabletop	Custom tailored tabletop exercise that will simulate an active breach. This assessment will allow us to identify strengths and weaknesses in your current capabilities as well as provide a road map for incident response maturity.	Available	✔
Cyber Threat Intel	Custom Cyber Threat Intelligence that is relevant to your organization quickly delivered to your organization enabling you to act fast and remediate potential vulnerabilities before an incident occurs!	Available	✔
Executive and Management Preparation (Board Included)	FRSecure experts have years of experience delivering messages to senior level personnel, we will be there to assist you in communication drafting, preparation, and delivery to ensure all aspects of an incident are communicated in a clear, concise and understandable format.	Available	✔
Red Team Assessment	Comprehensive security assessment that will assess the full spectrum of an organizations security mechanisms. Test will be tailored and designed to meet your organizational needs and can include External, Internal, Social, and Physical exercises.	Available	Available
Penetration Testing	Utilize your pre-purchased hours for any of our penetration testing services. This includes External, Internal, PCI, Physical and Social Engineering.	Available	Available

IR Services Available*	Description	IR Retainer Service	IR Managed Service
Social Engineering (Spear, Voice, Physical)	Test users ability resist human behavior modification by testing various methods of social engineering.	Available	Available
Digital Forensics	The use of technical tools to determine what happened during a cyber security incident. A digital breadcrumb.	Available	Available
Malware Analysis	Analysis of suspected malware to attempt to determine the details of the payload, transmission and behavior.	Available	Available
Incident Response Plan Drafting	Don't have a current Incident Response Plan? We can help! Our experts will work closely with your organization to draft a mature and comprehensive Incident Response plan to ensure you are prepared before an incident occurs.	Available	Available
Security Operations Center Development Exercise	FRSecure will work directly with your Security Operations Center to identify strengths and weakness in your current monitoring and identification process. We custom tailor this engagement to fit your needs, and we can assist in everything form device tuning to identification and response process.	Available	Available
Threat Hunting	Quickly discover and respond to any cyber threat actors that may be on your network. Disrupt threats and stop potential adversaries in their tracks!	Available	Available

* Available utilizing pre-paid IR hours

Cyber Security Incident Response Managed Service - Severity Levels

Incident Severity Types	Definitions	Containment Activity Response Time
Priority One Security Incident (P1) (Critical Incident – Likely Breach)	Incident affecting critical systems or information with potential to be revenue or customer impacting. **Examples include:** Application Compromise System Compromise Denial of Service Exploitation of known vulnerabilities Privileged Account Compromise Sabotage Unauthorized Access to Information Unauthorized Modification of Information Unauthorized wireless access points Unknown Vulnerabilities Worm	Response within **4** hours after Identification phase completed
Priority Two Security Incident (P2) (Serious Incident – Possible Breach)	Incident affecting critical systems, non-critical systems or unregulated information, which is not revenue or customer impacting. **Examples include:** Login attempts (Brute Force) Policy Violations Social Engineering Unprivileged Account Compromise Virus/Malware outbreak	Response within **8** hours after Identification phase completed
Priority Three Security Incident (P3) (Moderate Event – Low likelihood of Breach)	Incident affecting non-critical systems or information, not revenue or customer impacting. Generally, a single user issue. **Examples include:** Spyware Dialer Unauthorized use of resources	Response within **24** hours after Identification phase completed
Priority Four Security Incident (P4) (Security Event – Non-Incident)	No destructive behavior seen. In general, these would be considered to be part of normal support operations. **Examples include:** Spam Inappropriate content Scanning Copyright	Response within **48** hours after Identification phase completed

Rate Details

Name	Rate
IR Emergency Response and IR Registration Service	$425/hour - Initial block of hours determined on triage. A separate Statement of Work will be executed for each incident/engagement.
Cyber Security Incident Response Retainer Services	
IRR 25-99 hours Pre-purchased emergency support hours	$400/hour
IRR 100+ hours Pre-purchased emergency support hours	$380/hour
Cyber Security Incident Response Managed Service	
Cyber Security Incident Response Monthly Retainer	$2,500/month
Prepaid 25-99 hours of Emergency Response Service Pre-purchased emergency support hours	$400/hour
Prepaid 100+ hours of Emergency Response Service Pre-purchased emergency support hours	$380/hour

Project Constraints - IR Services

- Onsite for Emergency response in 24 hours limited to the Minneapolis/St. Paul metro area. Outside the Minneapolis/St. Paul metro area transit plans will be confirmed within 24 hours.
- Travel expenses are not included in any Cyber Security Incident Response Services and will be billed to the client following FRSecure Client Project Travel And Expense Policy.
- Normal business hours are defined as Monday through Friday 8am-5pm Central Time
- All Incident Response hours expire 12 months from Managed Service start date if not used and do not "roll over" to subsequent years.
- All Managed Services engagements require an active prepaid Response Service hour agreement.
- Cyber Security Incident Response Team (CSIRT) Hotline.
    - FRSecure will provide City of Wayzata a toll-free support number to the CSIRT Hotline, which is available 24x7x365. The CSIRT Hotline is to be used by City of Wayzata when City of Wayzata has a request for Incident Response support. Upon calling the CSIRT Hotline, an FRSecure Security Analyst will log the information and reason for the call, and will engage the next level of phone support. Depending on the nature of the issue, City of Wayzata may receive a follow-up call to discuss further details of their request to ensure response efforts are accurate and properly focused. A member of FRSecure's team will return the City of Wayzata’s initial call within the defined SLA to get more information related to the support request
- Pre-paid hours for both IR Retainer services and IR Managed services are available 30 days after contract is agreed to.

City Council Workshop
City Council Agenda Report

MEETING DATE: March 8, 2022	**WORKSHOP AGENDA ITEM:** 2
TITLE: Update of Preferred Platform Tennis Facility Location and Discussion of Next Steps (5:50-6:20 p.m.)	
PREPARED BY: Nick Kieser, Parks Planner	
REVIEWED BY: Jeffrey Dahl, City Manager	

DISCUSSION OBJECTIVE:

To discuss the Parks and Trails Board preferred location of platform tennis location and remaining process.

BACKGROUND:

Two years ago when the Parks and Trails Master Plan was adopted, there was significant discussion about the prioritization of platform tennis and where, if it is built, it should be located. Ultimately, the direction from the Council was that it should not be located in Klapprich Park and the Parks and Trails Board (PTB) should re-evaluate location options. Meanwhile, the City Council pushed its allocation of funds to assist in the capital cost to 2022. Currently, the CIP indicates a $128,750 allocation from the City and private funds contributing $128,750 for a total cost of $257,500 for the platform tennis project.

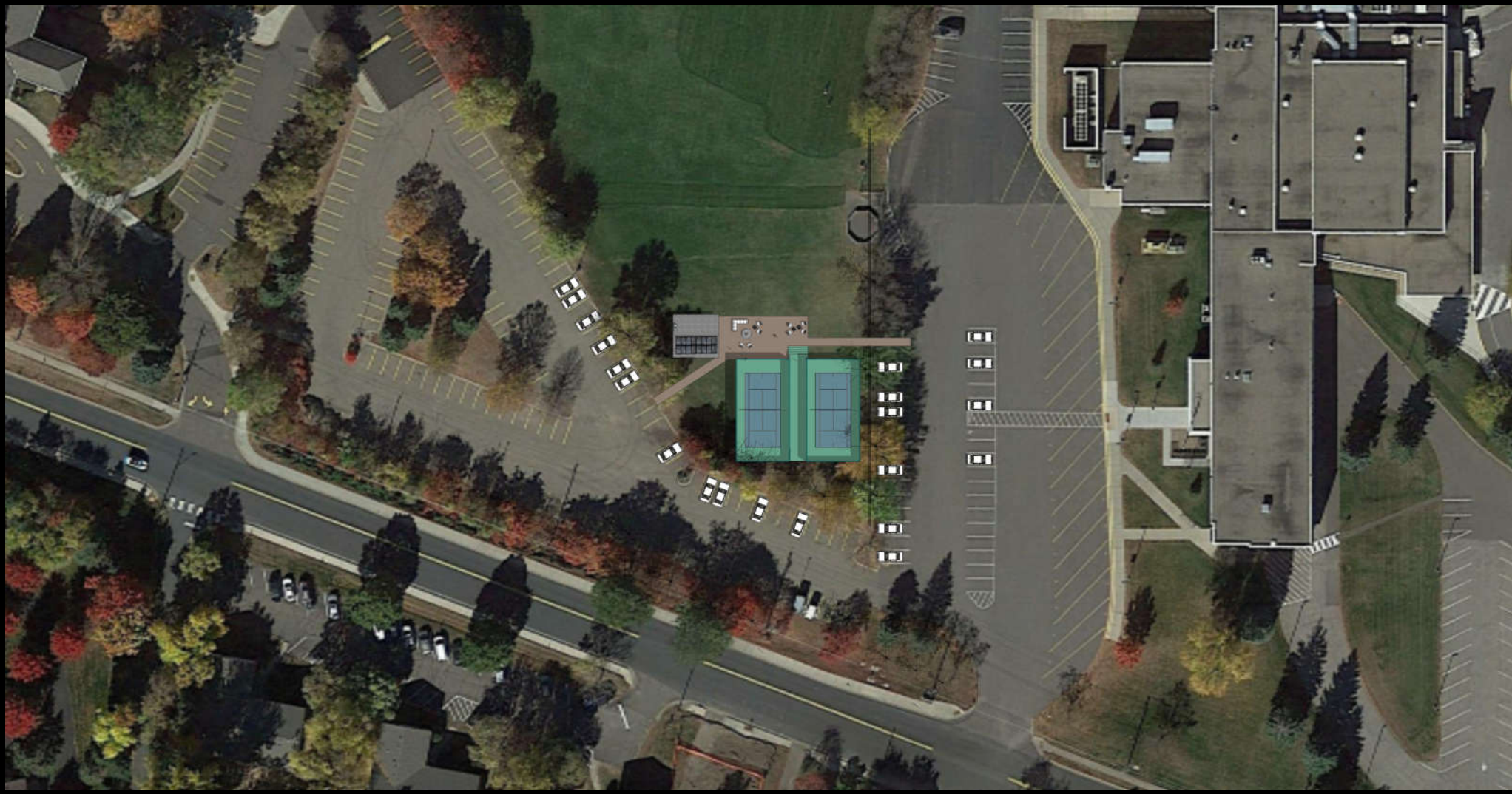
Since then, the PTB has studied locations and ultimately recommends the facility be built at Wayzata West Middle School. CIty staff have been in discussions with School District staff and they gave favorable input to allow the project on their property. They would like to have further discussion about programming, the details of the finalized plans, future needed agreements, and the proposed amenities. The School District Board would also need to be involved in an approval process similar to the City process.

Renderings of the proposed location are attached to show how the tennis courts and amenities could be constructed. Please note the renderings are concepts so final plans would be reviewed and updated with input from the Council, School District, and surrounding neighbors if Council decides to move forward with this location. The aforementioned total cost is estimated so future refinements and a bidding process would give more accurate estimates. Overall, staff is not anticipating the School District to participate in funding of the project so if the cost is above $257,500, the balance would need to be covered by private funds.

If the Council agrees to move forward with this location and prioritize the platform tennis project for 2022, staff would start a neighborhood engagement process that would result in finalized plans to go through the required bidding procedure. Future approval would be needed from the City Council to go out for bid for the proposed project.

ATTACHMENTS:

1. Platform Tennis Rendering 3-3-2022

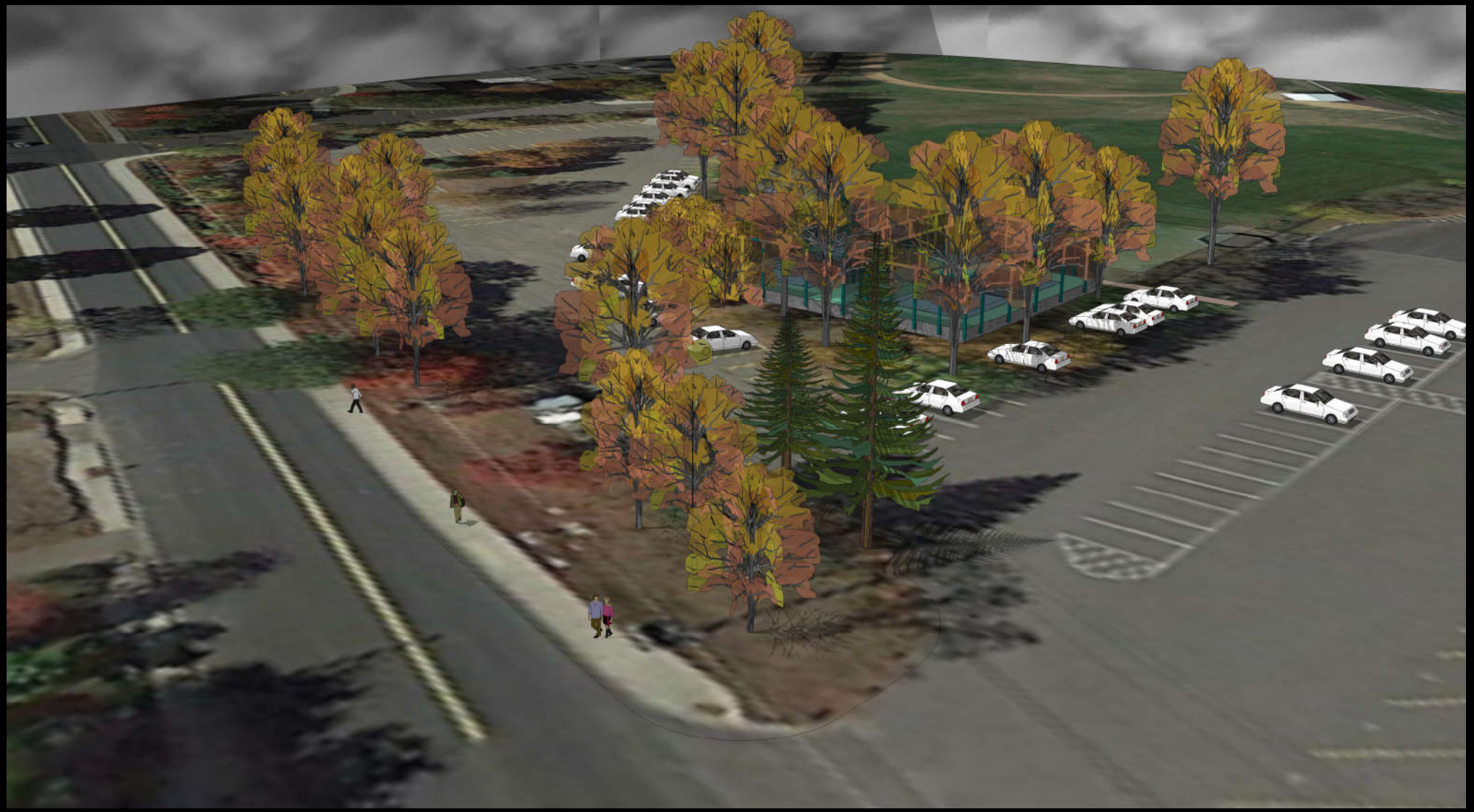


Context Plan

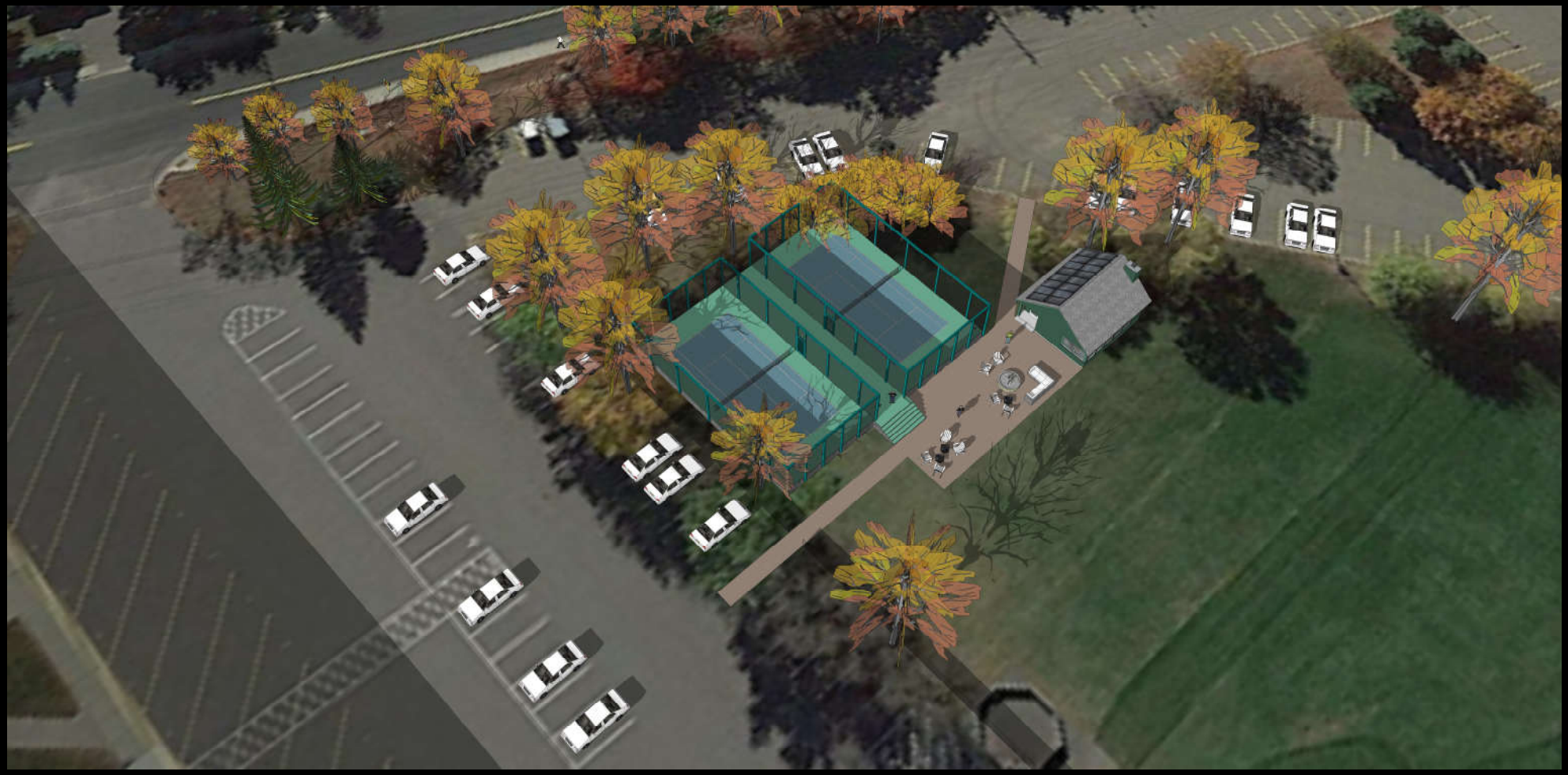
Platform Tennis Wayzata, MN March 2022

Site Organization

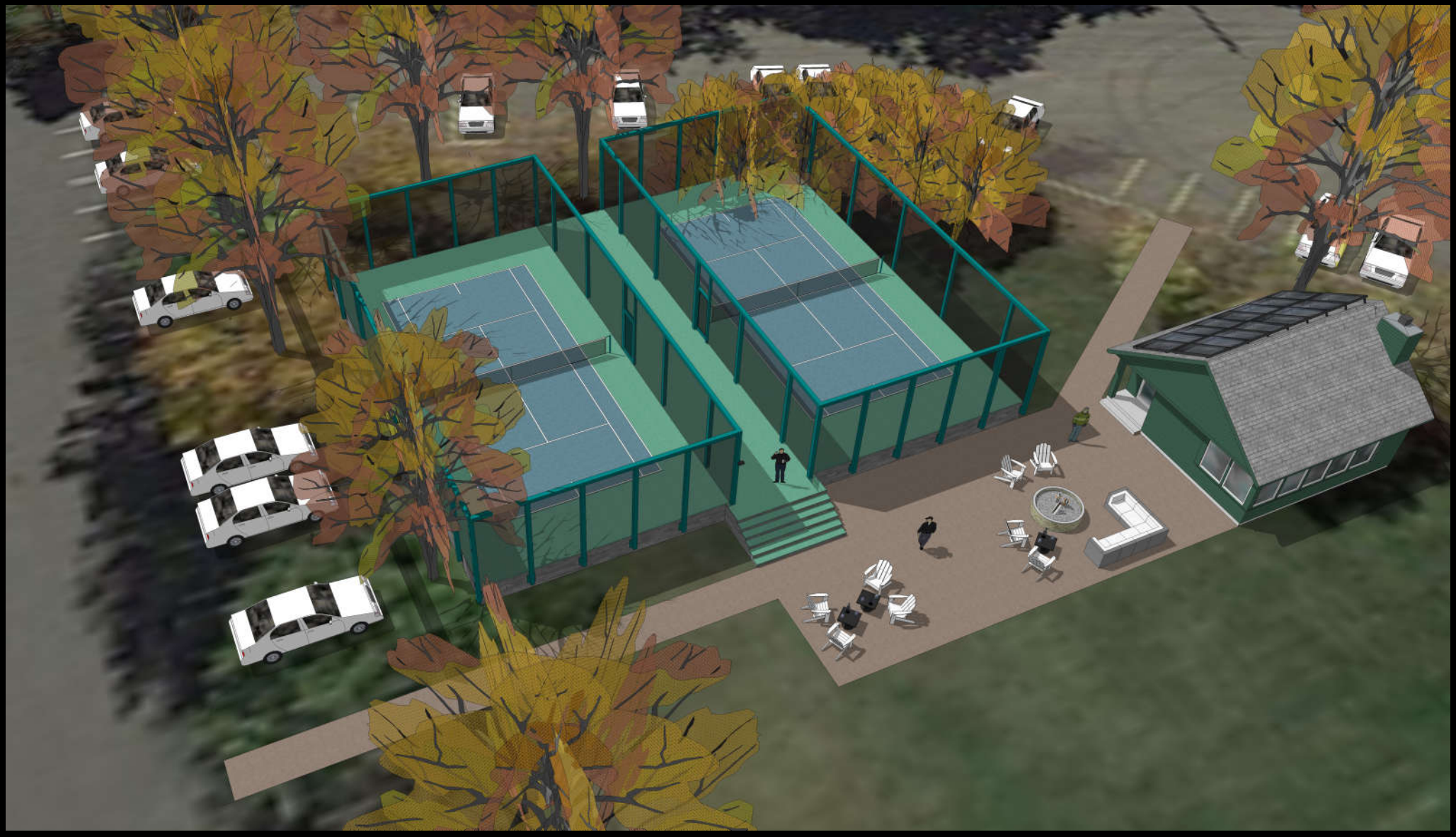
Platform Tennis Wayzata, MN March 2022



Aerial Image from Wayzata Blvd



Aerial Looking Southwest



Aerial image

Parking Lot Access from the East

Parking Lot Access from the West

Platform Tennis Wayzata, MN March 2022

Parking Lot Image

Platform Tennis Wayzata, MN March 2022

City Council Workshop
City Council Agenda Report

MEETING DATE: March 8, 2022	**WORKSHOP AGENDA ITEM:** 3
TITLE: Discussion of Volunteer Coordination Structure (6:20-6:30 p.m.)	
PREPARED BY: Jeffrey Dahl, City Manager	
REVIEWED BY: N/A	

DISCUSSION OBJECTIVE:

To provide a brief update on volunteer coordination options and receive Council feedback.

BACKGROUND:

Based on several reasons (retirement of coordinator, pandemic, Panoway opportunities), staff has put together the attached outline of what a more structured volunteer committee might look like.

Once the outline was drafted, staff met with key volunteers to get their feedback. A summary of that feedback is below:

- *Do not make participation too formal/complicated. Keep projects and structure very simple*
- *Formal applications to be a part of the committee could dissuade potential members from applying*
- *Let members choose the volunteer opportunities based on their own interest*
- *A staff liaison to keep the City-connection and a minimal budget are key to success*
- *Bring in people who are passionate/interested in doing the work and who can work independently*
- *Having an engaged Chair/leader/coordinator is essential*
- *The Committee can bring in other people when needed (i.e. bring in the Chamber for a specific project or the Garden Club, etc.)*
- *Have the Committee pick ~3 projects the first year to really pursue*
- *Try to pick COVID friendly projects/events*
- *Get the Logistics program up and running again or some other communications portal*

After hearing this feedback, staff is looking for discussion/directions on a few options moving forward. Potential options are:

- 1a—Advertise/Solicit to appoint a new Volunteer Coordinator who would work with staff on volunteer initiatives, develop an annual work plan, attend events, recruit new members, and coordinate activities with subcommittees
- 1b—Advertise/Solicit to hire (part-time) a new Volunteer Coordinator who would work with staff on volunteer initiatives, develop an annual work plan, attend events, recruit new members, and coordinate activities with subcommittees
- 2—Move forward with creating a Volunteer Committee via resolution

Regardless of the options that are pursued, it is planned that the Parks Planner position would be the volunteer liaison with help from the communications coordinator position for communications/recognition event.

ATTACHMENTS:

1. Volunteer Committee Outline 1.10.21

TITLE: Consider Adoption of Resolution Establishing Volunteer Committee

BACKGROUND:

The City has worked informally with a volunteer committee for over 10 years. The volunteer committee, led by Lynn McCarthy, was a grass roots community response to the 2007-2008 recession, when City services were scaled back, in order to maintain and enhance both the level of service AND increase community building. This effort, because it was grass roots, did not have any formal structure as a City body.

This group led countless volunteer efforts, including:

- Dig it and Pull it Days
- Planting of Bushaway Corridor
- Gateway plantings with MNDOT
- Maple Tree Tapping
- Adopt-A-Garden
- Senior Programs at the Boardwalk Apartments
- Public Works Administrative Duties
- Portal Deliveries
- Garlic Mustard and Buckthorn Pull Events

Over the past two years, four significant dynamics have impacted the existing volunteer structure:

- COVID-19 Pandemic and the ability to gather
- Retirement of core volunteers
- Increased expectation of City services
- Increase of City amenities to maintain

Because of these dynamics, the City will need to be more strategic and offer more resources in order to maintain and enhance City-related volunteers.

Purpose of Volunteer Committee

- Community building
- Achieve goals not able to be completed by city staff
- Save money

Goals of the Committee

- To corral and prioritize volunteer ideas and opportunities
- Manage annual volunteer budget
- To communicate and attract volunteers
- To communicate volunteer activities to community
- Keep Council updated on volunteer events
- To ensure volunteer efforts are aligned with City goals
- Organize volunteer appreciation opportunities

Structure

- Resolution establishing indefinite Volunteer Committee by City Council. Staff would return to Council with bylaws and a more long-term plan within one year.
- Monthly Meetings – held remotely or in person. Open to the public and advertised via City communications.
- Chair, Vice Chair, and Secretary elected by the Committee.
- Chair runs the meeting, develops meeting agendas with staff liaisons.
- Minutes taken each meeting by the Secretary.
- Most items will be a round table discussion in order for City staff to get feedback on City's Maintenance and Operations of downtown.
- Items that have any policy or financial implications will need to be approved via a motion, second, discussion, and vote. The meetings will follow Robert's Rules of Order.

Suggested Community Members/Representatives

- Two Council Member/s
- Chamber Staff
- Business Owner/s
- Residents
- Parks and Trails Board Members
- Wayzata Conservancy Member
- City staff
- Lake Minnetonka Garden Club
- Wayzata Lions
- Wayzata Sailing Center