TO: **HONORABLE MAYOR AND CITY COUNCIL**

FROM: **Aaron S. Reeves, City Administrator** AR

SUBJECT: **IT Security Assessment**

DATE: **January 7, 2014**

BACKGROUND

One of the anti-fraud recommendations from our Auditor was to evaluate the security of our IT systems. In addition, it just makes sense to review our information security and identify areas we need to address as we handle larger amounts of non-public data every year. Staff recommends approving the attached proposal for $11,890 from FRSECURE to conduct the study. The project will be paid from the IT budget.

STAFF RECOMMENDATION

Staff recommends that the City Council approve the proposal as presented to conduct an Information Security Assessment.

REQUESTED COUNCIL ACTION

I respectfully request a motion to approve the proposal as presented to conduct an Information Security Assessment.

FRSECURE
Information Security Management

Your Security. Our Passion.

City of Cannon Falls

Information Security Assessment Proposal

A proposal for an independent, objective review of the City of Cannon Falls information security program, including technical, physical and administrative security controls.

Dated 12/13/2013

A112020131342

Project Overview

Client name	City of Cannon Falls
Client's administrator	Aaron Reeves
Project name	City of Cannon Falls Information Security Assessment Project
Engagement duration	Estimated 6 weeks
Begin date	TBD
End date	TBD

This proposal and SOW is valid for 30 days

FRSecure Profile

The information contained within this section of the proposal provides background information and context about FRSecure.

Contact Information

- Full legal name: FRSecure LLC
- Headquarters address: 150 Pioneer Trail #125, Chaska, MN 55318
- Type of ownership: Limited Liability Corporation ("LLC")
- FRSecure LLC is not a subsidiary or affiliate with any other organization
- FRSecure is incorporated and organized in the State of Minnesota
- Person authorized by FRSecure LLC to field questions and provide answers for clarification regarding this proposal response:
    - Name: Evan Francen
    - Title: President
    - Telephone number: 952-467-6384
    - Email address: evan@frsecure.com

Organizational Overview

About FRSecure

FRSecure LLC is a full-service information security management company. As an information security firm, FRSecure protects sensitive, confidential business information from unauthorized access, disclosure, distribution and destruction. We assess existing information security systems and develop, implement and manage plans tailored to each client's specific security needs and overall business objectives. These plans spare clients from the irreparable financial and reputational costs that invariably accompany the breach of sensitive business and personal information.

FRSecure works with businesses of all sizes, in all industries. We understand that our clients are in business to make money, so we design secure solutions that drive business, protect sensitive information assets, and improve their bottom line.

Achievements, experience and continuous referrals separate FRSecure as reliable information security experts.

Description of Professionals

All information security professionals working for FRSecure have, at a minimum:

- Valid and active information security industry certifications (Certified Information Security Systems Professional - "CISSP", Certified Information Security Manager - "CISM", et al.)
- Real-world information security experience; building, managing, and improving information security programs for which they have been directly responsible for, and;
- An average of 15+ years of information security practitioner experience

Statement of Work

Project Summary

This information security assessment has been developed for City of Cannon Falls in order to satisfy the following requirements:

- Provide City of Cannon Falls with an objective assessment of information security risks within their environment
- Satisfy current requirements for a comprehensive assessment
- Provide City of Cannon Falls with a strategic information security plan to align information security objectives with business objectives

There may be other objectives and requirements that are satisfied as a result of meeting the requirements outlines above. In essence, the following questions should be answered during this project:

- What are City of Cannon Falls's most significant information security risks?
- What are City of Cannon Falls's information security requirements?
- How should City of Cannon Falls best satisfy their own internal information security requirements and those of its customers?
- What is the strategic plan for information security at City of Cannon Falls?
- In order for information security to be effective, what involvement should there be from management?
- Can we demonstrate value in City of Cannon Falls's information security investments?
- If City of Cannon Falls had one information security dollar, where would it be best spent?
- Where do we begin in improving City of Cannon Falls's information security?
- And others.

This assessment will follow FRSecure's Information Security Assessment Methodology. FRSecure's methodology is available upon request.

Assumptions

FRSecure LLC will provide all of the materials required for the completion of this information security assessment project. FRSecure will rely upon experience, observation, and interviews with City of Cannon Falls employees to assess the current risks of unauthorized disclosure, modification, or destruction of information under the custodial care of City of Cannon Falls. The FRSecure information security assessment will follow the standards as noted in the ISO 17799:2005 (ISO 27002) international standard.

The FRSecure information security analyst will review a variety of information including, but not necessarily limited to prior reviews and current City of Cannon Falls policies, processes, and procedures.

City of Cannon Falls will provide FRSecure with access to information and answers required to complete the information security assessment. City of Cannon Falls will provide access to personnel and documentation (if it exists) as required.

This project and Statement of Work is for information security assessment and recommendation services only. FRSecure will not implement or change anything as part of this engagement. Design, implementation and management work are outside of the scope of this project.

Project Phases

This Information Security Assessment is comprised of the following phases:

- Phase 1 – Administrative Security Controls Assessment,
- Phase 2 – Physical Security Controls Assessment,
- Phase 3 – Internal Network Security Assessment, and;
- Phase 4 – External Network Security Assessment

Phase 1 – Administrative Security Controls Assessment

The administrative security controls assessment includes a comprehensive and objective review of all documentation, processes, and practices used in the management and governance of information security at City of Cannon Falls. FRSecure's analyst will use the controls found in ISO 27002 (17799:2005), NIST, and others for comparison, gap analysis, and risk rating.

Where there are gaps, the analyst will assign three metrics in an attempt to provide a qualitative risk rating:

- Level of Effectiveness ("LOE") - a measure of control quality and maturity,
- Likelihood of an adverse event or threat, and
- The potential Impact suffered by the organization

FRSecure expects to review between 3,000 – 3,500 administrative control characteristics during this assessment.

Phase 2 - Physical Security Controls Assessment

Phase 2 of the FRSecure Information Security Assessment is a review of physical security controls and associated risks. Focus for the Phase 2 of the assessment will be on where critical City of Cannon Falls information resources are physically located.

Physical security controls review is comprised of physical site tours and risk analysis of the following:

- Facility construction,
- External security,
- Access to the facility,
- Visitor access,
- Surveillance cameras,
- Security guards,
- Loading and delivery areas,
- Office areas,
- Datacenter/restricted areas,
- Environmental controls,
- Property removal,
- Destruction practices, and;
- Housekeeping

Phase 3 – Internal Network Security Assessment

The Internal Network Assessment phase of the FRSecure information security assessment is comprised of the analysis of risk with the following two sub-phases:

- **Network architecture and practices review:**
  - Network Connectivity
  - Remote Access
  - Directory Services
  - Servers and Storage
  - Workstations
  - Mobile Devices
  - Logging and Alerting
  - Vulnerability Management
  - Backup and Disaster Recovery

- **Vulnerability scanning and analysis**
  - Vulnerability scanning of all internal subnets
  - Analysis of the vulnerability scan data
  - Vulnerability scoring and comparisons.

Phase 4 – External Network Security Assessment

The primary objective of the External Network 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.

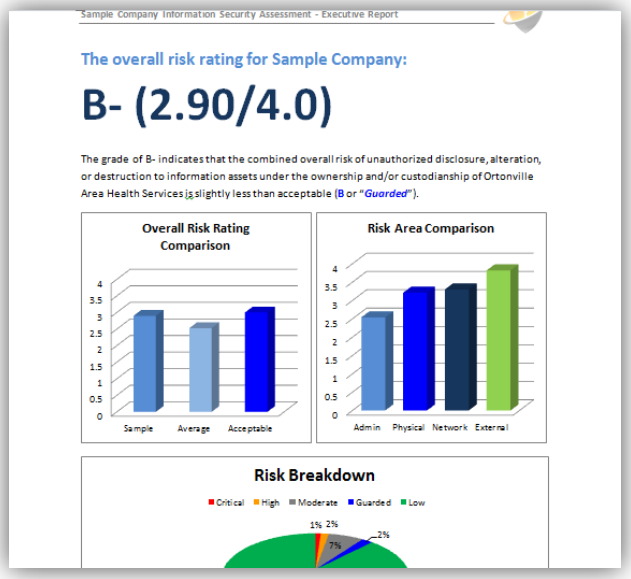
The External Network Assessment consists of a six phase process; reconnaissance/discovery, enumeration, vulnerability identification, vulnerability verification, analysis, and reporting.

Deliverables

City of Cannon Falls will be provided with the following deliverables from FRSecure:

Information Security Assessment Executive Summary

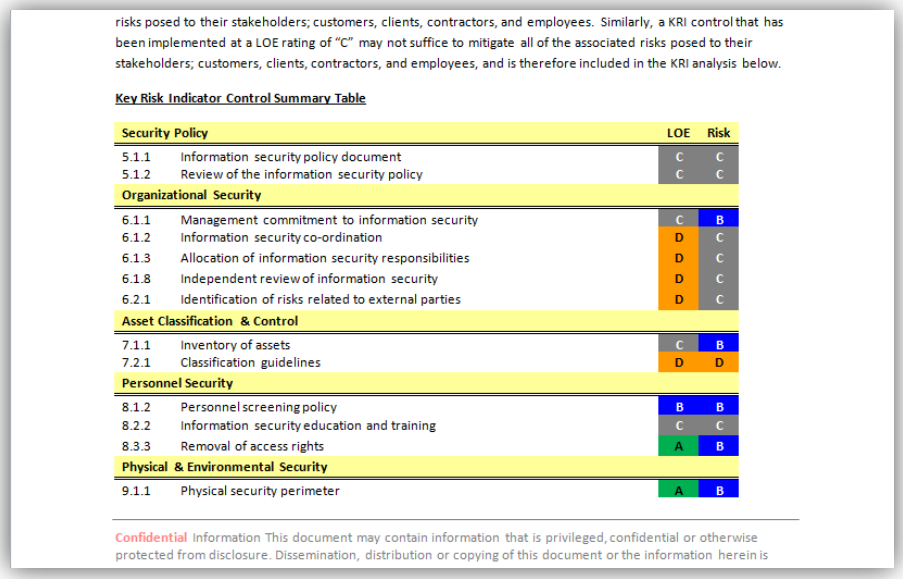
A high level summary of the information security assessment findings; including the top 5 security recommendations in each assessment area.



Information Security Assessment Final Report

A detailed report of all risk findings for controls which lack a general level of effectiveness (3 or less on a scale of 1-5), including:

- Overview
- Organization profile
- Overall risk and summary of findings
- Network security and encryption analysis
- Level of Effectiveness (LOE)
- Average risk level
- Assigned risk rating
- Organizational responsibility matrix
- Documents reviewed
- Key risk indicators
- Key risk indicator analysis
- Justifications
- Recommendations



risks posed to their stakeholders; customers, clients, contractors, and employees. Similarly, a KRI control that has been implemented at a LOE rating of "C" may not suffice to mitigate all of the associated risks posed to their stakeholders; customers, clients, contractors, and employees, and is therefore included in the KRI analysis below.

Key Risk Indicator Control Summary Table

Security Policy		LOE	Risk
5.1.1	Information security policy document	C	C
5.1.2	Review of the information security policy	C	C
Organizational Security			
6.1.1	Management commitment to information security	C	B
6.1.2	Information security co-ordination	D	C
6.1.3	Allocation of information security responsibilities	D	C
6.1.8	Independent review of information security	D	C
6.2.1	Identification of risks related to external parties	D	C
Asset Classification & Control			
7.1.1	Inventory of assets	C	B
7.2.1	Classification guidelines	D	D
Personnel Security			
8.1.2	Personnel screening policy	B	B
8.2.2	Information security education and training	C	C
8.3.3	Removal of access rights	A	B
Physical & Environmental Security			
9.1.1	Physical security perimeter	A	B

Confidential Information This document may contain information that is privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this document or the information herein is

Information Security Action Plan

A detailed plan of action created from the information security assessment findings and City of Cannon Falls risk acceptance criteria. The action plan is created after the assessment reports have been created and are included within one or both of the above mentioned reports.

Process

On a high-level, the assessment process is comprised of the following steps:

1. **Planning and Coordination** – planning timelines, resource constraints, and activities.
2. **Information Gathering** – a combination of remote and onsite information gathering used to justify risk findings and ratings.
3. **Organization and Comparison** – pairing thousands of pages of information into manageable "chunks" and comparing against well-known industry standards/practices*.
4. **Analysis and Quantification** – analysis of control gaps (coverage, quality, functionality, etc.) and quantification of associated risks
5. **Translation and Communication** – translation of risks into grading, risk prioritization, generate recommendations, and produce reports.
6. **Next Steps** – once your assessment is complete, we'll discuss how to move forward.

*Information gathered during the assessment is compared against well-known industry standards such as those found in ISO 27002 (17799:2005), NIST, and others.

Change management process

Changes can be made to the scope of this project 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 project-related expenses may be itemized and billed to City of Cannon Falls separately.

Estimated expenses for this project include:

- Travel – Billed at actual cost and/or based upon 2013 IRS Standard Rates (est. $200)
- Printing – Billed at actual cost (est. $150)

Payment Terms

Total Project Investment • Administrative Controls Assessment • Physical Controls Assessment • External Network Vulnerability Assessment • Internal Network Vulnerability Assessment	$11,890

Phase	Completion date	Payments due
Prior to project initiation	TBD	$5,945 US
Project completion, all deliverables complete and accepted	TBD, est. 6 weeks after project initiation	$5,945 US

A la carte Options

Check Any That Apply	Description	Unit Price
	Administrative Controls Assessment	$5,370
	External Network Vulnerability Assessment	$2,890
	Internal Network Vulnerability Assessment	$4,340

Value Proposition

There are many significant value propositions that would be realized by City of Cannon Falls in selecting FRSecure. Examples include:

- **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 Contact Information

Steve Marsden
952-467-6388
smarsden@frsecure.com

Customer Acceptance

FRSecure is excited about the opportunity to serve you on this important engagement.

Please indicate your acceptance of the terms outlined in this agreement by signing it and returning it to:

FRSecure
Attn Kevin Orth
150 Pioneer Trail #125
Chaska MN 55318
Fax 952-467-6381
Email korth@frsecure.com

Acceptance for Customer:

City of Cannon Falls

_____ (authorized agent)
Name

_____
Title

_____
Signature

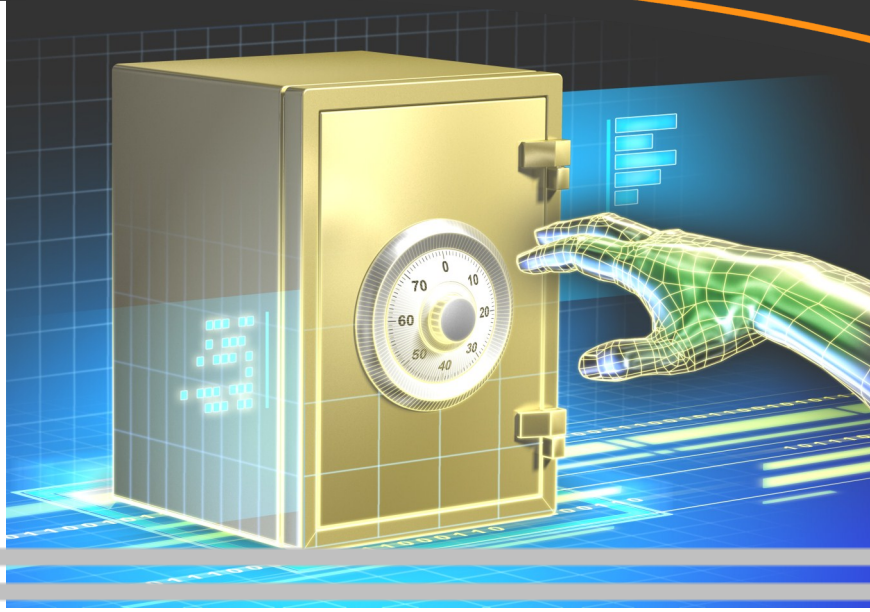
_____
Date

FRSecure

Your Security Partner

"We offer sound, strategic information security expertise, gained through 20 years of experience building information security programs."

- Evan Francen, President



Best Practices

The inspection body shall be independent of the parties involved.

The personnel of the inspection body shall be free from any commercial, financial and other pressures which might affect their judgment.

The inspection body shall be capable of performing an inspection of processes that include personnel, facilities, technology and methodology.

The inspection body shall have documentation which describes its functions and the technical scope of activity for which it is competent.

The inspection body shall have a technical manager who is qualified and experienced.

The inspection body shall perform periodic assessments of its own security and processes.

FRSecure Fits The Bill

- We are completely independent and objective. We are not your IT company or your CPA firm.
- We do not sell hardware. We have no ulterior motives in our recommendations. In fact, our recommendations are written so that you can implement them internally.
- Our standard assessment reviews security in all areas of your organization, including Internal IT, External IT, Physical, and Administrative security controls.
- Our assessment methodology has been tested and proven hundreds of times. Ask us for a copy.
- All projects are performed and supervised by information security professionals with a minimum 10 years of industry experience.
- Ask us about our own security practices.

Companies that seek the best choose FRSecure.

www.FRSecure.com
info@frsecure.com
952-467-6381

FRSECURE
Information Security Experts

(888) 676-8657 www.frsecure.com

FRSecure will help clearly define your information security requirements and guide you to the *right* level of security specific to your needs.

Get an objective, measurable assessment of your risks.

1. Where are you vulnerable?
2. How likely are your vulnerabilities to be exploited?
3. How impactful are the consequences?

Build a strategy to address your risks.

1. Start with the most impactful risks.
2. Mitigate, transfer or accept risks as appropriate.
3. Account for regulatory compliance influences.

Execute the plan.

1. Get the right people involved.
2. Follow your road map.
3. Improvise, adjust and adapt as business needs change.

"We help organizations align security with strategic business objectives, creating an information security program that is integrated into the business."

- Evan Francen, President

Assessment Services

- HIPAA/Meaningful Use Risk Assessments
- PCI-DSS QSA
- GLBA Security Assessments
- NCUA Security Assessments
- Information Security Risk Assessments
- Customer Required Security Assessments
- Penetration Testing
- IT Vulnerability Assessments
- Cyber Security Assessments
- General Controls Assessments
- SSAE16 Readiness Assessments
- ISO 27002 Gap Analysis
- NIST Gap Analysis
- COBIT Gap Analysis

Program & Strategy Development

- Information Security Risk Remediation
- Social Engineering
- DR Planning and Testing
- Incident Response and Management
- Security Training & Awareness
- Outsourced CISO
- Vendor Risk Management
- Information Security Policy Development
- Information Security Guidance

FRSECURE
Information Security Management

FRSecure
150 Pioneer Trail #125
Chaska MN 55318

FRSecure.com | 888-676-8657

Meet FRSecure

Information Security Experts

Your Security. Our Passion.

We've been helping organizations in all industries solve complex security issues since 2008.

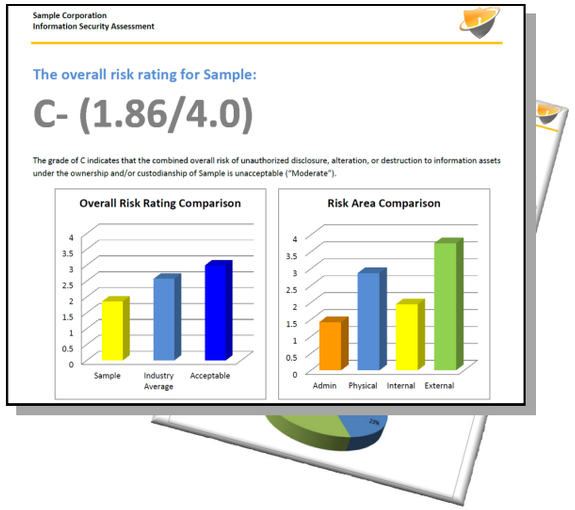
FRSECURE
Information Security Management

Meet FRSecure: Information Security Experts

In most organizations, information security is a subset of IT. But consider this, Information Security touches all aspects of your organization from HR, to Finance, to IT. And you have information in all types of forms; electronic, paper, knowledge, etc.

The challenge for those responsible for information security is to build a security program that allows for access to information while keeping it confidential and accurate, all while staying in compliance with regulations, customer requirements, or the organization's objectives.

Information security is bigger than IT. It's an organizational issue that should be measurable, strategic, and help drive the organization forward, not slow it down.



More than 90% of successful breaches require only the most basic techniques

The average time to discover a breach is five months

75% of attacks use publicly known vulnerabilities in commercial software

A recent survey showed that 45% of companies believe their security program is doing well. The study also showed that only 10% were taking adequate steps or taking a proactive approach.

The best security programs are risk based, strategic, measurable and align with the objectives of the organization.

If an effective, organizational information security program is the goal, FRSecure is the answer.

Information security programs are very complex and impact your entire organization. Having FRSecure as your security partner means you immediately gain 20 years of experience assessing and building security programs.

We specialize in helping organizations get to the right level of security. Not too locked down, but also not too many security gaps.

These days, breaches happen all the time, affecting not only the bottom line, but the reputation of the organization. Our sole purpose is to help our clients avoid information losses.

"Everyone I worked with left me with the feeling that they were here to teach me and help me improve my security program. And they all did it in such a relaxed manner that I felt like we were just friends having a conversation about security."

- CISO of a MN Bank

You have security challenges. We have the expertise and the answers.

FRSecure is the ideal choice for organizations that need an information security partner that understands the challenges, understands compliance, understands business, and knows how to balance the right amount of security with the need for access to information.

Assessments

FRSecure performs many types of independent security assessments, including: general information security, GLBA, HIPAA including Meaningful Use, Customer Requirements, PCI-DSS, and more.

Program Development

Our team is here to help with any security challenges or projects you have, including: security guidance, security leadership, participation on security teams or committees, vendor risk management, policy, and much more.

Partner with FRSecure

Invest 20 minutes to find out how FRSecure can help make sense of your information security puzzle.

Our approach to security truly is different, and our clients appreciate our ability to make security efficient, effective, and fun!

Visit FRSecure.com or call 888-676-8657 today.