DECEMBER 5, 2024

VILLAGE OF NORTH AURORA
Crossroads on the Fox

CYBER RISK EVALUATION

Contact for RFP Response:

Shawn Johnson
Proposal Manager
SJohnson@securanceconsulting.com
877.578.0215 ext. 115

www.securanceconsulting.com

SECURANCE CONSULTING
the advantage of insight

SECTION 1: EXECUTIVE SUMMARY

December 5, 2024

David Arndt | Information Technology Manager
North Aurora Village Hall
25 E. State Street
North Aurora, IL 60542

Dear David:

Thank you for considering Securance Consulting for the Village of North Aurora's (Village's) upcoming cyber risk evaluation. Securance is a firm of risk management experts with more than 22 years' experience conducting comprehensive risk assessments for more than 400 government municipalities, including multiple villages in Illinois. Our team of seasoned professionals has the breadth of expertise needed to optimize the Village's security controls, mitigate and prioritize network vulnerabilities, and improve the Village's alignment with security frameworks and regulatory compliance requirements. **We want to partner with you!** With Securance as a partner, the Village will benefit from our:

- **Extensive Experience with Similar Scopes of Work:** Securance has completed more than 3,000 cybersecurity risk assessments, on time and on budget, for more than 400 government municipalities during our two decades of service. Our assessments comprehensively evaluate security risks, including those associated with inadequate security controls, network vulnerabilities, Active Directory (AD) weaknesses, and noncompliance with frameworks and regulatory requirements.
- **Senior Cybersecurity Consultants:** The consultants proposed for the Village's engagement have a combined 100+ years' experience managing cybersecurity risk — 18 or more years each. Our team are experts in best practice frameworks including the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), and regulatory compliance including the Criminal Justice Information Services (CJIS) requirements.
- **Proven Methodologies Backed by AI:** Securance is the first and only cybersecurity firm harnessing the power of generative artificial intelligence (GenAI) and large language models (LLMs) to focus our assessments on the most pertinent risks to our clients' technologies and IT processes. Securance will leverage our methodologies to provide highly customized, actionable, and easy-to-understand reporting and remediation recommendations.
- **Value Adds to Enhance Project Efficiency:** To demonstrate Securance's commitment to the Village's near- and long-term security, Securance is offering six free value adds: project management, knowledge transfer sessions, weekly status reporting, project planning and design, an external network vulnerability assessment, and 24 hours of remediation consulting to be used at the Village's discretion.
- **Knowledge of Similar Client IT Environments:** Securance has provided cybersecurity risk assessments to numerous clients similar to the Village, including the Villages of Oak Park, Schaumburg, and Orland Park. Please see the following page for a short description of these projects.

Client	Project	Contract Value	Description	Performance Period
Village of Oak Park	Cybersecurity Risk Assessment	$53,816	Evaluated IT governance; assessed internal, external, and wireless networks; conducted social engineering exercises; assessed Active Directory (AD); assessed CJIS, PCI DSS, and HIPAA compliance	Two Months in 2023
Village of Schaumburg	Network Security Assessment	Total for Four Projects: $120,838	Reviewed IT governance; conducted external, internal, and wireless network vulnerability assessments; assessed patch management, network architecture, and security operations; reviewed the configurations of routers, switches, and firewalls	Multiple Projects in 2015, 2016, 2018, and 2023
Village of Orland Park	Cybersecurity Risk Assessment	$50,344	Conducted NIST CSF gap analysis; conducted internal, external, and wireless network vulnerability assessments and penetration testing; assessed firewall, router, and endpoint configurations; reviewed mobile device security management; reviewed data communications; assessed the police department's CJIS compliance	January - December 2023

We acknowledge that Securance may not be the lowest-priced bidder of the services required by the Village. However, our services represent a superior value when compared to those offered at a lower cost by our competitors. From the detailed nature of our assessment to the comprehensiveness of our deliverables and the in-depth knowledge transfer we will conduct post-assessment, the Village will not find a firm whose analyses and results are more accurate and exhaustive than ours. Discussions with our clients over the past 22 years have confirmed that our slightly higher upfront costs represent significant long-term savings.

Thank you again for including Securance in your evaluation process. If you have any questions after reviewing our proposal, please do not hesitate to contact me.

Professional regards,

Paul Ashe, CPA, CISA, CISSP, CMMC-AB RP, HCISPP

President

We want to partner with you!

13916 Monroes Business Park, Suite 102 • Tampa, Florida 33635
877.578.0215
www.securanceconsulting.com

SECTION 2: TABLE OF CONTENTS

22+ YEARS

Securance has more than 22 years of experience providing cyber risk evaluation services similar in scope to those sought by the Village of North Aurora (Village).

EXECUTIVE-LEVEL CONSULTANTS

Our executive-level consultants have provided comprehensive risk assessments for clients such as the Villages of Schaumburg, Oak Park, and Orland Park.

EXTRA VALUE

Few firms are as dedicated to their clients as Securance will be to you. We will invest the time and effort necessary to learn the Village's IT environment and organizational objectives. Then, we will use that understanding to prioritize risks and develop customized, actionable recommendations for a robust security posture.

SECTION 2: TABLE OF CONTENTS

Requirements Matrix

Securance has formatted our proposal according to the Village's requirements. Below, we summarize the contents of our proposal:

RFP Section	Requirement	Page No.
Contents of Proposal	SECTION 1 – EXECUTIVE SUMMARY Provide a letter of introduction signed by an authorized representative of the firm (2 pages maximum) that provides an executive summary of the firm's experience relevant to the scope of work described in the RFP and describes why the firm would be of service to the Village of North Aurora on this project.	2
	SECTION 2 – TABLE OF CONTENTS	4
	SECTION 3 – STATE OF QUALIFICATIONS A statement of qualifications shall summarize key elements of the proposal and highlight your firm's qualifications as they relate to this project and these services requested. The Statement of Qualifications should demonstrate to the Village that your firm fully understands the Scope of Services, has industry knowledge and possesses the qualifications to provide the services requested.	6
	SECTION 4 – ORGANIZATIONAL INFORMATION Identify key personnel from your firm, including specific personnel that would be assigned to this Project, if any. Any and all primary contractor and subcontractor relationships and responsibilities must be detailed. Identify the Village's primary point(s) of contact for service requests, if your firm is retained for this Project. How many potential different people will the Village have to contact for service?	13
	SECTION 5 - VENDOR REQUIREMENTS/REFERENCES Respondents shall have at least 5 years' experience in information technology security services. Provide at least three (3) references for which your firm has performed similar services. Provide a brief synopsis of the services performed and contact information.	23
	SECTION 6 – PROJECT APPROACH/METHODOLOGY What is your firm's process leading to service delivery? How much time does it take your firm to mobilize and deploy after a request is received? Provide a description of the equipment, software, and personnel your firm possesses that can adequately address this project.	24
	SECTION 7 – COST OF PROPOSAL Provide a cost breakdown of the proposed solution showing the cost for each part of the scope of work and any additional costs. This information shall be followed by narrative which shall describe and justify the proposed costs, and include an estimate of staff allocations, estimated hours, rates per assigned staff and an estimate of total billable hours (and project hours for each item and total). Also identify any assumptions you have built into your costs. The cost proposal must provide a guarantee that no additional fees beyond those proposed will be charged to the Village of North Aurora without the Village's prior written consent.	48
	SECTION 8 – ACKNOWLEDGMENTS, ADDITIONS AND EXCEPTIONS a) Acknowledge your ability to meet or not meet all of the requirements as stated in the scope of work b) Compile and include all other information you deem pertinent, but not specifically requested elsewhere (5 pages maximum). c) Indicate any exceptions to the terms and conditions of this request for proposal, or any qualifications/clarifications regarding the proposal response.	51
	SECTION 9 – CERTIFICATE OF INSURANCE Proof of insurance is not required to be submitted with your proposal but will be required prior to the Village's award of the contract.	55

SECTION 3: STATEMENT OF QUALIFICATIONS

More Than Two Decades of Cybersecurity Risk Assessment Services

Securance is a 100-percent minority-owned limited liability company, certified as an 8(a), Small Disadvantaged Business (SDB), and Minority Business Enterprise (MBE). Paul Ashe, the Village's proposed engagement manager (EM), founded Securance in March 2002. Since then, we have performed more than 3,000 risk assessments for clients in nearly every industry, including more than 400 government agencies.

Exclusively Staffed with Senior-Level Cybersecurity Professionals

To provide the highest quality services, Securance only hires cybersecurity consultants with more than 15 years of professional experience. Their expertise in risk evaluation, network security, and best practice and compliance standards is our foundation, and our consultants hold prestigious certifications, including:

- C | CISO - Certified Chief Information Security Officer
- CCNA - Cisco Certified Network Associate
- CCSP - Certified Cloud Security Professional
- CCNP - Cisco Certified Network Professional
- CDPSE- Certified Data Privacy Solutions Engineer
- CEH - Certified Ethical Hacker
- CISA - Certified Information Systems Auditor
- CISM - Certified Information Security Manager
- CISSP - Certified Information Systems Security Professional
- CompTIA A+, Network+, Linux +, Security+ Certification
- RHCE - Red Hat Certified Engineer
- RHCSA - Red Hat Certified System Administrator

Our team is committed to clear and proactive communication and will work with all relevant Village staff to develop detailed, actionable recommendations that improve security controls, address network vulnerabilities, and optimize alignment with security best practices and regulatory compliance requirements.

Understanding of the Village's Scope of Work

Securance understands that the Village is seeking a comprehensive evaluation of its risks and security controls against the NIST CSF and CJIS compliance requirements, vulnerability assessments of its internal and external network, and an evaluation of its Active Directory (AD) environment. Securance will thoroughly complete each of these scope items for the Village, and provides specific examples of our experience with these services on pages 9-12.

The Securance Difference

HANDS-ON EXECUTIVE LEADERSHIP ON EVERY PROJECT

A niche cybersecurity firm, Securance was founded more than two decades ago by a group of executives from Big 4 accounting firms. Their vision was to provide highly specialized IT consulting services to clients in a wide range of industries, with unique advantages that only a small business could offer. Among these benefits are the caliber of our professional staff and the hands-on involvement of our executive team in client projects.

Larger firms use senior resources to lead their businesses but often turn much of the fieldwork on client projects over to less experienced consultants. This is not the case with Securance. **Our professional staff is limited to senior IT consultants with at least 15 — and, often, 30 or more — years of experience. Senior staff members do not just lead our projects; they execute them from cradle to grave.** Our firm's executives, such as founder and president Paul Ashe and security lead Ray Resnick, work alongside our staff consultants on every project.

CYBERSECURITY RISK TRANSLATED TO BUSINESS RISK

We have worked with hundreds of clients over the years and understand the disconnect that can occur when IT speaks one language and business another. An assessment report filled with technical jargon may be useful to a system administrator or engineer, but it provides little, if any, value to the C-suite. **Securance's reports are written in plain English that both technical and non-technical executives can understand.** We explain the potential adverse effect of each finding on business operations. This approach extends the value of our analysis beyond IT staff, helping senior management understand the risks and making our recommendations truly actionable.

Securance is the *only* cybersecurity firm that uses generative artificial intelligence (GenAI) and large language models (LLMs) to enhance its approach to identifying and assessing technology risks. Our proprietary GenAI technology uses OpenAI's GPT-4 model, an LLM with 1 trillion parameters, to analyze large amounts of multimodal data, identify patterns and potential risks in a client's technology environment, and, even, predict security breaches and failures. Armed with this insight, Securance tailors its assessment approach to fit each client's organization, address industry concerns, and target technology-specific threats.

SECTION 3: STATEMENT OF QUALIFICATIONS

We Understand Governments

Government agencies have unique needs when it comes to cybersecurity. Not only do they have to protect their networks from bad actors and internal threats, but they are also responsible for safeguarding sensitive citizen and employee data, updating and maintaining robust security controls, and monitoring compliance with regulatory requirements and best practice frameworks. Inadequate controls, outdated IT processes, and inadequate security awareness can leave governments vulnerable to cyber attacks and data breaches. For this reason, agencies need a cybersecurity partner who understands evolving cybersecurity threats and the best practices needed to defend against them. Securance is that partner, and our expertise and past experience proves this.

Government at a Glance

- **22+** years serving small, medium, and large government agencies.
- **400+** clients.
- **3,000+** projects completed.
- Agencies served: local | city | state governments, healthcare organizations, transportation authorities, education | higher education institutions, financial | insurance organizations, utilities.

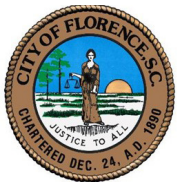
Given our experience and expertise, we will bring specific value to the Village's project, including:

- The knowledge of senior cybersecurity consultants who have a combined 100+ years of experience conducting comprehensive risk evaluations for similar organizations, such as the Villages of Oak Park, Orland Park, and Schaumburg and the Cities of Highland Park and St. Charles.
- An expert understanding of and extensive experience helping organizations align their processes with cybersecurity frameworks, including the NIST CSF, and regulatory compliance standards, including those issued by the CJIS.
- Awareness of cybersecurity threats facing government agencies, including ransomware attacks, denial of service (DoS) attacks, and techniques that exploit end-user knowledge of sensitive information.
- Heightened consideration of recent cyber attacks on local governments, including the ransomware attack on Henry County, Illinois, in March by the Medusa ransomware gang.

SECTION 3: STATEMENT OF QUALIFICATIONS

Similar Clients

Below is a sample of clients that have engaged Securance for similar work to the Village's project.



Case Studies

CLIENT NAME: Village of Oak Park (Village)

SECURANCE TEAM: Paul Ashe, Ray Resnick, Jerry Bruggeman

PROJECT DURATION: 2 Months, 2023

CLIENT SINCE: 2023

PROJECT OUTCOMES

Provided actionable remediation recommendations to reduce compliance risks within environment

Improved cybersecurity posture by reducing technical risks associated with vulnerabilities and external networks

CYBERSECURITY ASSESSMENT

CLIENT OBJECTIVES

The Village sought a vendor to:

- Review IT processes and governance.
- Identify vulnerabilities in select technologies.
- Assess compliance with identified standards.

SECURANCE SOLUTION

The Securance team conducted a cybersecurity assessment that included:

- Reviewing IT policies, procedures, and standards.
- Vulnerability assessments and penetration tests of the external, internal, and wireless network.
- Testing user security awareness via email phishing and other social engineering activities.
- Assessing the AD environment.
- Assessing compliance with CJIS, PCI DSS, and HIPAA.

Case Studies

CLIENT NAME: Village of Schaumburg (Village)

SECURANCE TEAM: Paul Ashe, Ray Resnick, Jerry Bruggeman

PROJECT DURATION: Multiple Projects in 2015, 2016, 2018, and 2023

CLIENT SINCE: 2015

PROJECT OUTCOMES

Facilitated a sustainable reduction in vulnerabilities

Addressed urgent-, high-, and medium-risk vulnerabilities to decrease technical threats in the environment

NETWORK SECURITY ASSESSMENT

CLIENT OBJECTIVES

The Village sought a vendor to:

- Review its IT processes and operations.
- Assess technical configurations and network security.

SECURANCE SOLUTION

The Securance team conducted a cybersecurity assessment that included:

- Reviewing IT policies, procedures and standards.
- Conducting external, internal, and wireless network vulnerability assessments.
- Assessing patch management, network architecture, and security operations.
- Reviewing the configurations of its routers, switches, and firewalls.

Case Studies

CLIENT NAME: Village of Orland Park (Village)

SECURANCE TEAM: Paul Ashe, Ray Resnick

PROJECT DURATION: January-December 2023

CLIENT SINCE: 2023

PROJECT OUTCOMES

Developed a customized remediation roadmap based on the NIST CSF

Addressed high-priority risks to the internal network and router | switch configurations

Provided recommendations to implement formal IT governance documents, including an IT strategic plan, an IT risk assessment program, IT policies and procedures, data flow diagrams, a disaster recovery plan, and an incident response plan

CYBERSECURITY RISK ASSESSMENT

CLIENT OBJECTIVES

The Village sought a vendor to:

- Use the NIST CSF to assess Orland Park's IT processes and identify vulnerabilities in select technologies.

SECURANCE SOLUTION

The Securance team conducted a cybersecurity assessment that included:

- Conducting a NIST CSF gap analysis to identify risks.
- Conducting internal, external, and wireless network vulnerability assessments and penetration testing.
- Assessing firewall, router, and endpoint configurations.
- Reviewing mobile device security management.
- Reviewed data communications (e.g., communications between the Village and its software as a service (SaaS) providers).
- Assessed the Village police department's CJIS compliance.

SECTION 4: ORGANIZATIONAL INFORMATION

Point of Contact

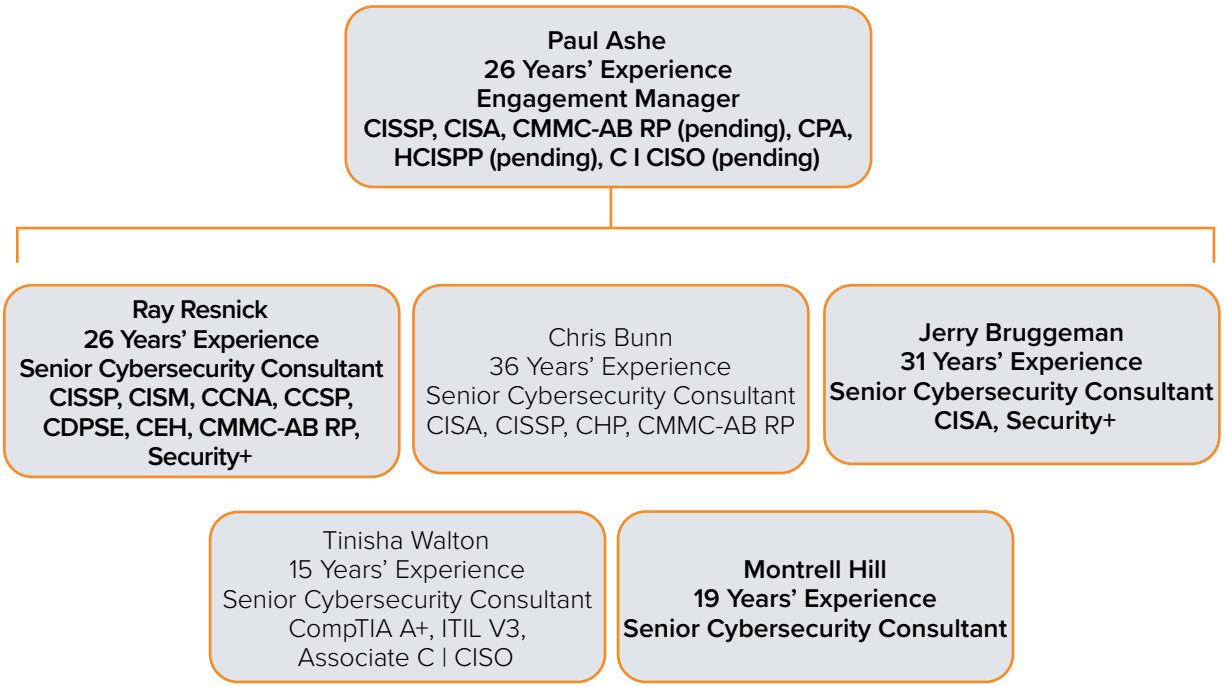
The Village's point of contact for all service requests is Paul Ashe | pashe@securanceconsulting.com | 877.578.0215 ext. 140.

The Village's point of contact for all proposal-related communications is Shawn Johnson | sjohnson@securanceconsulting.com | 877.578.0215 ext. 115.

Key Personnel

Securance's key personnel include president and engagement manager Paul Ashe and senior cybersecurity consultants Chris Bunn, Ray Resnick, Jerry Bruggeman, Tinisha Walton, and Montrell Hill. We provide a summary of their qualifications below.

The staff specifically proposed for the Village's project includes Paul Ashe, Ray Resnick, Jerry Bruggeman, and Montrell Hill (emboldened below). We provide full resumes for these four proposed consultants on the following pages. If any of these consultants are unavailable when the project starts, Securance will propose an equally experienced substitute for approval. Securance only employs senior-level consultants; no junior-level consultants will be assigned to the Village's project.



Consultant Resumes — Key Personnel

PAUL ASHE

26 YEARS OF CYBERSECURITY EXPERIENCE

President and Engagement Manager | Securance Consulting

EDUCATION

Master of Science
Accounting Information Systems

Bachelor of Science
Accounting and Management Information Systems

PROFESSIONAL CREDENTIALS

- Certified Public Accountant (CPA)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Healthcare Information Security and Privacy Practitioner (HCISPP) (pending)
- Cybersecurity Maturity Model Certification Registered Practitioner (CMMC RP) (pending)
- Certified Chief Information Security Officer (C | CISO) (pending)

Paul has provided hands-on project management to lead Securance engagements over the past 22 years. A former IT consultant for Ernst & Young, he translates his knowledge and experience into an effective, time- and budget-conscious project management style. Paul conducts risk assessments, AD reviews, and technology-specific vulnerability assessments for clients in nearly every industry. He is an expert in implementing and assessing security frameworks, such as the NIST CSF.

RELEVANT EXPERIENCE

- Access Control Management
- Account Management
- Active Directory Assessments
- Application Security
- CJIS Compliance
- Data Protection and Recovery
- Internal | External | Wireless Network Security
- Policy and Procedure | IT Governance Reviews
- Project Management
- System Configuration Reviews
- Vulnerability Assessments | Management

RELEVANT EXPERTISE

- **Project Management:** Paul has led Securance engagements from kick-off to final report for 22 years.
- **Risk Assessments:** Paul helps clients identify technology and process risks and develop risk-based cybersecurity assessment plans that allow organizations to focus resources in the right areas and make informed decisions about risk management.
- **Compliance and Framework Assessments:** An expert in federal regulatory requirements, including CJIS, PCI DSS, FISMA, and state privacy and security laws, Paul helps clients to comply and avoid costly breaches and | or fines. He also excels in implementing security frameworks, such as the NIST CSF, to mitigate risks and optimize controls.
- **Vulnerability Assessments:** Paul specializes in performing network scans and vulnerability assessments to identify and prioritize risks within internal and external networks.
- **Data Security:** Paul is skilled in helping organizations protect the confidentiality, integrity, and availability of their critical data.

Consultant Resumes — Key Personnel

RELEVANT ACHIEVEMENTS

- **Village of Oak Park** Evaluated IT governance; assessed internal, external, and wireless networks; conducted social engineering exercises; assessed AD; assessed CJIS, PCI DSS, and HIPAA compliance.
- **Village of Schaumburg** Reviewed IT governance; conducted external, internal, and wireless network vulnerability assessments; assessed patch management, network architecture, and security operations; reviewed the configurations of routers, switches, and firewalls.
- **Village of Orland Park** Conducted NIST CSF gap analysis; conducted internal, external, and wireless network vulnerability assessments and penetration testing; assessed firewall, router, and endpoint configurations; reviewed mobile device security management; reviewed data communications; assessed the police department's CJIS compliance.
- **City of St. Charles** Improved logging and monitoring, change management, patch management, and disaster recovery processes and reduced network and database vulnerabilities by 60 percent.
- **City of Durham** Reduced urgent, critical, and high-risk vulnerabilities associated with the internal network, enterprise application, and database environment by 50 percent; managed the recovery process after the City suffered a major ransomware attack; currently serves as the City's vCISO; oversees the cybersecurity program and security operations center (SOC); and achieved a 100-percent reduction in cybersecurity breaches and incidents.
- **City of Gilroy** Streamlined the City's IT operations by improving governance documentation and implementing a cyber resilience plan, which facilitated a sustainable reduction in vulnerabilities.
- **City of Modesto** Improved governance documentation and reduced key person risk.
- **City of New Haven** Identified vulnerabilities and opportunities to improve policies, procedures, and security configurations; provided extensive remediation support to address identified vulnerabilities, including incident response tabletop exercises and plans to train IT staff and standard users in security awareness; developed a three-year plan to implement all new security program items.
- **City of Pasadena** Reviewed IT operations and processes against the NIST CSF and provided a roadmap to improve the City's security and control posture.
- **City of Phoenix** In addition to identifying and helping remediate vulnerabilities in the City's networks, servers, databases, firewalls, and routers, secured funding for a 24 | 7 | 365 SOC.
- **City of Richmond** Facilitated a significant reduction in technical risks across the internal network following remediation.
- **State of Wyoming** Identified critical-, high-, and medium-risk vulnerabilities to decrease technical threats in the IT environment and improved IT governance to decrease future vulnerabilities.
- **Texas Municipal Retirement System** Improved end-user security awareness by 70 percent and reduced technical risk across the environment by more than 50 percent.
- **Village of Niles** Spearheaded development of policies, procedures, cross-training, and a technology steering committee and reduced key person risk by matching staff to appropriate tasks.

Consultant Resumes — Key Personnel

RAY RESNICK

26 YEARS OF CYBERSECURITY EXPERIENCE

Senior Cybersecurity Consultant | Securance Consulting

EDUCATION

Bachelor of Science

Accounting

PROFESSIONAL CREDENTIALS

- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Certified Cloud Security Professional (CCSP)
- Certified Data Privacy Solutions Engineer (CDPSE)
- Certified Ethical Hacker (CEH)
- Cisco Certified Network Associate (CCNA)
- CompTIA Security+ Certified
- Cybersecurity Maturity Model Certification Registered Practitioner (CMMC RP)

Ray, a retired Commander and Special Operations Officer for the U.S. Navy, specializes in analyzing organizational security needs, analyzing existing security posture, and implementing plans to mitigate risks to an acceptable level. Ray works with IT staff at all levels to assess security risks and controls, identify and prioritize network vulnerabilities, and close compliance gaps that hamper security in the IT environment.

RELEVANT EXPERIENCE

- Active Directory Assessments
- Application Security
- Compliance and Framework Assessments (e.g., CJIS, NIST CSF)
- Cybersecurity Risk Assessments
- Data Security
- Malware Defense Optimization
- Information Security Awareness Training
- Incident Response
- Internal | External | Wireless Network Security
- Policy and Procedure Reviews
- Vulnerability Assessments

RELEVANT EXPERTISE

- **Cybersecurity Risk Assessments:** Ray has been identifying and prioritizing security risks for 26 years. His extensive knowledge of cybersecurity framework and compliance standards, such as NIST, CJIS, ISO, and ITIL allow him to take a holistic approach across all areas of cyber risk management.
- **Vulnerability Assessments:** Ray specializes in scanning internal and external networks to identify vulnerabilities, prioritize risks, and develop recommendations for improved security and alignment with best practice standards.
- **Active Directory Assessments:** Ray has extensive experience assessing organizations' Microsoft AD environments for adequate policies and robust infrastructure.

SECTION 4: ORGANIZATIONAL INFORMATION

Consultant Resumes — Key Personnel

RELEVANT ACHIEVEMENTS

- **Village of Oak Park** Evaluated IT governance; assessed internal, external, and wireless networks; conducted social engineering exercises; assessed AD; assessed CJIS, PCI DSS, and HIPAA compliance.
- **Village of Schaumburg** Reviewed IT governance; conducted external, internal, and wireless network vulnerability assessments; assessed patch management, network architecture, and security operations; reviewed the configurations of routers, switches, and firewalls.
- **Village of Orland Park** Conducted NIST CSF gap analysis; conducted internal, external, and wireless network vulnerability assessments and penetration testing; assessed firewall, router, and endpoint configurations; reviewed mobile device security management; reviewed data communications; assessed the police department's CJIS compliance.
- **City of Durham** Reduced urgent, critical, and high-risk vulnerabilities associated with the internal network, enterprise application, and database environment by 50 percent; managed the recovery process after the City suffered a major ransomware attack; served as backup vCISO to Paul Ashe for the City; helps oversee the cybersecurity program and security operations center (SOC); and achieved a 100-percent reduction in cybersecurity breaches and incidents.
- **City of Kenai** Improved operating effectiveness of critical IT processes.
- **City of Modesto** Improved governance documentation and reduced key person risk.
- **City of New Haven** Identified vulnerabilities and opportunities to improve policies, procedures, and security configurations; provided extensive remediation support to address identified vulnerabilities, including incident response tabletop exercises and plans to train IT staff and standard users in security awareness; developed a three-year plan to implement all new security program items.
- **City of Phoenix** In addition to identifying and assisting to remediate vulnerabilities in the City's networks, servers, databases, firewalls, and routers, secured funding for a 24 | 7 | 365 SOC.
- **City of Richmond** Facilitated a significant reduction in technical risks across the internal network following remediation.
- **North Dakota Public Employee Retirement System** Identified medium-risk vulnerabilities and offered actionable remediation recommendations and recommended the implementation of a program management policy to solidify program change policies.
- **Riverside University Health System** Reduced vulnerabilities within the internal network, web application, operating system, and databases and developed a management plan that prioritized risks, estimated costs, timelines, and resources needed to attain full HIPAA compliance.
- **Texas Municipal Retirement System** Improved end-user security awareness by 70 percent and reduced technical risk across the environment by more than 50 percent.
- **Washington State Investment Board** Reduced key person risk by 90 percent and reduced financial exposure from non-compliance with Washington State Office of the CIO's standards.

Consultant Resumes — Key Personnel

PRIOR ACHIEVEMENTS

- **Copper Collar Enterprises, LLC** | 2012–2018 | Information Security Engineer | Conducted vulnerability scanning, attack and penetration studies, analyzed information and physical security vulnerability assessments; analyzed data security controls to identify weaknesses; designed remediation strategies.
- **Verizon Communications** | 1998–2003 | Database Administrator | Performed database installs, loads, and data conversions. Tuned and altered databases and tables to increase performance. Prepared custom database reports with SQL and shell scripts. Wrote stored procedures, triggers, and database views to increase efficiency and security. Scheduled and performed database back-ups. Troubleshot application code for SQL errors and potential SQL injection vulnerabilities.
- **Verizon Communications** | 1998–2003 | Senior Systems Engineer | Developed automated tools to improve system reliability and disk and CPU utilization; planned, coordinated, and performed application testing, installation, and patch management; responsible for installing, managing, and administering servers, providing training and technical support to end users, and maintaining system documentation.
- **United States Navy Reserve** | 2002–2003 | Commander | Served as Executive Officer, Operations Department Head (N3), Inspector General, Information Technology and Physical Security Department Head (N6), and Intelligence Department Head (N2); responded to crisis management situations in the United States Central Command Area of Responsibility (USCENTCOM AOR). Supervised Crisis Action Team (CAT cell), Joint Personnel Adjudication System (JPAS), and internal badging systems for U.S. Naval Forces Central Command (NAVCENT); prepared and delivered briefings to Flag Level officers regarding political, military, security, and terrorism matters.
- **United States Navy** | 1991–2007 | Deputy Assistant Chief of Staff Naval Liaison Officer | Performed high-level negotiations with senior governmental officials and military officers from 53 coalition nations; responsible for operational planning efforts of U.S. and coalition maritime assets during wartime environment.

Consultant Resumes — Key Personnel

JERRY BRUGGEMAN

31 YEARS OF CYBERSECURITY EXPERIENCE

Senior Cybersecurity Consultant | Securance Consulting

EDUCATION

Bachelor of Science

Cybersecurity

PROFESSIONAL CREDENTIALS

- CompTIA Security+ Certified
- Certified Information Systems Auditor (CISA)

Jerry is a versatile cybersecurity expert with a strong background in risk management and network security. He has helped create and maintain robust cybersecurity programs for large organizations in both the private and public sectors, including the U.S. military. Jerry has significant experience applying regulatory and best-practice frameworks, and optimizing security controls and practices.

RELEVANT EXPERIENCE

- Active Directory Reviews
- Compliance and Framework Assessments (e.g., CJIS, NIST CSF)
- Cybersecurity Risk Assessments
- Data Security | Data Recovery
- Enterprise and Web Application Security
- Incident Response Improvement
- Information Security Awareness Training
- IT Governance
- Network Assessments, e.g., Internal | External | Wireless
- Vulnerability Assessments

RELEVANT EXPERTISE

- **Vulnerability Assessments:** Jerry's exceptional ability to probe for security vulnerabilities helps organizations enhance their security postures and protect against potential threats.
- **Compliance Assessments:** A former director of IT for numerous organizations, public and private, Jerry is an expert in assessing compliance with regulatory requirements, including CJIS, as well as with best practice standards such as the NIST CSF.
- **Network Security** Jerry excels at identifying and addressing vulnerabilities in networks, routers, switches, and firewalls and providing actionable remediation recommendations to address each vulnerability.
- **Incident Response Improvement:** Jerry's expertise in assessing organizations' incident response capabilities has helped numerous organizations ensure they are prepared to handle cybersecurity events effectively and efficiently, reducing potential risk to operational integrity, financial stability, and public image.

Consultant Resumes — Key Personnel

RELEVANT ACHIEVEMENTS WITH SECURANCE

- **Village of Oak Park** Improved the Village's cybersecurity posture by reducing technical risks associated with vulnerabilities in the internal and external networks and provided actionable remediation recommendations to reduce compliance risks within the environment.
- **Village of Schaumburg** Identified urgent-, high-, and medium-risk vulnerabilities to decrease technical threats in the Village's IT environment.
- **City of Cleveland** Reviewed disaster recovery plan; improved endpoint configuration; conducted internal | external vulnerability assessments and penetration tests; enhanced security operations.
- **City of Ontario** Conducted internal | external network vulnerability assessment and penetration test; performed social engineering exercise to evaluate end-user security awareness.
- **County of Sonoma** Assessed operating system, endpoint, and firewall configuration; conducted internal | external network vulnerability assessment and penetration test; tested web application security; assessed wireless network security; performed social engineering exercise; improved compliance with HIPAA breach, notification, and security rules.
- **Elsinore Valley Municipal Water District** Reviewed IT governance | policies and procedures for alignment with NIST CSF; assessed operating system, endpoint, firewall, and router | switch configuration; conducted internal, external, and wireless network vulnerability assessments and penetration tests.
- **Emergence Health Network** Improved the organization's cybersecurity posture by recommending several improvements, including the implementation of a disaster recovery plan and a change management process.
- **Milwaukee Metropolitan Sewerage District** Conducted network penetration tests.
- **Riverside University Health System** Reduced vulnerabilities within the internal network, web applications, operating systems, and databases; developed a remediation plan that prioritized risks, estimated costs, timelines, and resources needed to attain full HIPAA compliance.
- **Rowan University** Conducted external network penetration testing and assessment of network architecture.
- **VIA Metropolitan Transit** Conducted an internal network vulnerability assessment.

SELECT PRIOR ACHIEVEMENTS

- **Healthplan Services (WIPRO)** | 2020–2023 | Director of Information Security | Provided subject matter expertise in risk assessment, compliance, and technical security.
- **VASTEC** | 2013–2020 | Director of Information Security | Spearheaded IT security program, developed disaster recovery and incident response plans, conducted IT risk assessments, performed and analyzed vulnerability scans, and administered virtual environments.
- **U.S. Air Force, 52nd Combat Communications Squadron** | 2010–2013 | Chief of Cyber Systems Operations | Managed a 120-person team across five work centers, conducted vulnerability and risk assessments, tracked and reported KPIs, and developed and deployed tactical networks.
- **U.S. Air Force, 14th Weather Squadron** | 2005–2010 | Manager, Information Assurance | Managed unit network security programs and assessments; conducted vulnerability and risk assessments.

Consultant Resumes — Key Personnel

MONTRELL HILL

19 YEARS OF CYBERSECURITY EXPERIENCE

Senior Cybersecurity Consultant | Securance Consulting

EDUCATION

Bachelor of Science

Business Computer Information Systems

Montrell is an experienced cybersecurity leader who specializes in planning and conducting risk assessments. As an expert in best-practices and regulatory frameworks, he helps enterprises develop effective security controls, identify vulnerabilities and risks, refine their IT processes, and achieve their business and compliance goals.

RELEVANT EXPERIENCE

- Active Directory Reviews
- Access Controls | Management
- Account Management
- Cybersecurity Risk Assessments
- Data Security
- External | Internal Vulnerability Assessments
- System Configuration Reviews
- Incident Response Plan Reviews
- Network Security
- Security Awareness Training
- Vulnerability Management

RELEVANT EXPERTISE

- **Cybersecurity Risk Assessments:** Montrell helps organizations identify and prioritize security risks in their environment and develops actionable recommendations to mitigate them and avoid costly data breaches, ransomware attacks, or system outages.
- **Network Security:** Montrell excels at identifying and exploiting vulnerabilities in networks, routers, switches, and firewalls.
- **Active Directory Reviews:** Montrell assesses organizations' AD environments for adequate policies and robust infrastructure.

Consultant Resumes — Key Personnel

RELEVANT ACHIEVEMENTS WITH SECURANCE

- **Emergence Health Network** Improved the organization's cybersecurity posture by recommending several improvements, including implementation of a disaster recovery plan and a change management process.
- **Lea County** Reviewed critical IT governance documents including incident response and disaster recovery plans, and assessed IT service and staffing performance against best practices.
- **King County** Conducted a security assessment of the County's industrial control systems (ICS) and physical security controls; helped the County select a network monitoring tool for its ICS environment.
- **Maryland-National Capital Park and Planning Commission** Provided 480 hours of Cybersecurity as a Service (CSaaS) consulting to review the incident response program, vulnerability management process, application security, and perform other cybersecurity services.
- **Omnitrans** Provided a thorough network security review and data protection assessment and offered defined improvements to the employee security awareness program and the incident response plan.
- **St. John's River Water Management District** Conducted an IT organization and staffing review, policy and procedure assessment, and a data and information security review to inform a remediation plan to improve overall efficiency and performance of IT organization.

PRIOR ACHIEVEMENTS

- **First Command Bank** | 2019–2022 | Senior IT Auditor | Developed IT audit programs; performed audits and risk assessments; developed strategies to mitigate risks and remediate vulnerabilities.
- **Raytheon, Richardson** | 2015–2019 | IT Audit Supervisor and Senior Information Governance & Risk Specialist | Performed IT risk assessments and audits; developed audit programs; oversaw fieldwork and deliverables and ensured that audits met internal quality control requirements, professional standards, laws, and regulations; presented audit findings and advised management on risk mitigation strategies.
- **GM Financial** | 2007–2015 | IT Auditor | Led IT audits focused on IT general controls, application controls, data warehouses, platform technologies, network security, data center controls, and compliance; compared IT controls to information security and risk management frameworks, including COBIT, COSO, NIST 800-53, and ISO 27001.
- **Computer Science Corp** | 2005–2007 | IT Consulting | Conducted information security and HIPAA compliance assessments.

SECTION 5: VENDOR REQUIREMENTS | REFERENCES

Securance has more than two decades of experience providing the Village's requested services, and all Securance consultants are located in the United States. Below is the contact information of three clients for which Securance has performed similar projects. We encourage the Village to contact each organization's representative to confirm the validity of our claims and the value of our deliverables.

Please note that our clients prefer to be contacted first via email.

Organization Name	Reference Contact	Services Provided | Dates of Service
Village of Schaumburg	Peter Schaak, Director of IT pschaak@villageofschaumburg.com 847.895.4500	◗ Multiple Projects in 2015, 2016, 2018, and 2023 ◗ Reviewed IT governance; conducted external, internal, and wireless network vulnerability assessments; assessed patch management, network architecture, and security operations; reviewed the configurations of routers, switches, and firewalls
Village of Orland Park	David Buwick, Chief Technology Officer dbuwick@orlandpark.org 708.403.6212	◗ January-December 2023 ◗ Conducted NIST CSF gap analysis; conducted internal, external, and wireless network vulnerability assessments and penetration testing; assessed firewall, router, and endpoint configurations; reviewed mobile device security management; reviewed data communications; assessed the Village police department's CJIS compliance
Village of Niles	Ali, Rehman, IT DIrector rra@vniles.com 847.588.8000	◗ June-August 2021 ◗ Evaluated IT operations and assessed against strategic plan; reviewed policies and procedures; interviewed IT staff and developed a prioritized roadmap of staffing levels and leadership; performed a strengths, weaknesses, opportunities, and threats (SWOT) analysis to assess cybersecurity posture

SECTION 6: PROJECT APPROACH | METHODOLOGY

Our Understanding of the Village's Scope of Work

Below, we summarize our understanding of the Village's expectations for this project and the deliverables. Securance will be prepared to mobilize and deploy its team two weeks after receiving a signed contract. We have included methodologies for some of the assessment tasks on the following pages, and additional methodologies can be provided upon request. Please refer to these methodologies for detailed information about the software we will use to complete the project.; Securance will only use software during vulnerability testing. Outside of that, our software usage will be limited to standard productivity tools - i.e., Microsoft Office and Adobe.

PLANNING AND DESIGN

- Kickoff Meeting:
  - Collect Documentation
  - Set Expectations
  - Discuss Scope
  - Develop Project Plan
  - Determine Point of Contact for Engagement
- Establish Rules of Engagement
- Create | Share Client Assistance Memo

CYBER RISK EVALUATION

- Risk Evaluation
  - Using the NIST CSF, Securance will review the Village's policies, procedures, and security controls, including:
    - Software and Hardware Inventory and Control
    - Data Protection and Recovery
    - Malware Defenses
    - Email Protections
    - Systems Configuration
    - Network Infrastructure Management
    - Network Monitoring and Defense
    - Account Management
    - Access Control Management
    - Vulnerability Management
    - Audit Log Management
    - Security Awareness Training
    - Application Software Security
    - Incident Response Management
    - Information Security Policy Documentation Review
- Health Check of Microsoft AD, Including a Review of:
  - Accounts
  - Policies
  - Privileges
  - Infrastructure
  - Best practices regarding on-premise Microsoft AD and Entra | Azure AD
- Network Assessments
  - Internal and External Network Vulnerability Assessments
  - Wireless Network Testing

DELIVERABLE

- Board-Ready Cyber Risk Evaluation Management Report

Risk-Based Cybersecurity Powered by AI

Securance is **the first and only cybersecurity firm** to use generative AI (GenAI) and large language models (LLMs) to enhance its approach to client-focused assessments.

GenAI and LLMs can transform how businesses across industries gather and analyze information, predict outcomes, and make better decisions. Cybersecurity is no exception. At Securance, we use LLMs to identify potential risks based on a client's technologies, IT processes, and industry. We apply this information to focus our approach and methodologies when conducting cybersecurity risk assessments.

LLMs consider billions of parameters and ingest massive amounts of data from sources such as the Internet, Common Crawl, which collects data from more than 50 billion web pages, and Wikipedia, with approximately 57 million pages. While not perfect, LLMs have a remarkable ability to make predictions based on a relatively small number of prompts, or inputs. GenAI uses LLMs to produce content based on human-language prompts that provide clarity and context.

SECTION 6: PROJECT APPROACH | METHODOLOGY

Risk-Based Cybersecurity Powered by AI

Securance's program leverages OpenAI's GPT-4o model. With 1 trillion parameters, GPT-4o can identify patterns from multimodal data, generate natural and readable output, and perform complex tasks. We use GPT-4o to deliver maximal value to our clients via customized methodologies, targeted assessments, and actionable recommendations to prevent security breaches. During an initial co-development and planning session, we gather information about the client, its technology environment, and IT organization.

We use this data to adjust our input prompts, which include:

- The organization's industry.
- The organization's size.
- The security framework(s) in place.
- The security tools in place.
- Whether the organization has a security operations center (SOC) monitoring its network.

Securance does not include confidential, proprietary, or sensitive data from our clients in our prompts.
Clients can opt out of participating in our private LLM if they choose.

Based on the input prompts, our LLMs and GenAI produce information that informs our assessment approach. Securance's model can even predict cyber breaches, events, and failures and their consequences. Predictions may include the potential for:

- Failures in IT process controls.
- Network, system, and/or application breaches based on the client's cybersecurity profile.
- End-user security failures and phishing attacks.
- Inappropriate access to data or systems by end users.

Harnessing the power of GenAI, Securance provides clients with accurate results, tailored recommendations, and unique advantages that other security firms cannot match. The benefits of a Securance assessment include:

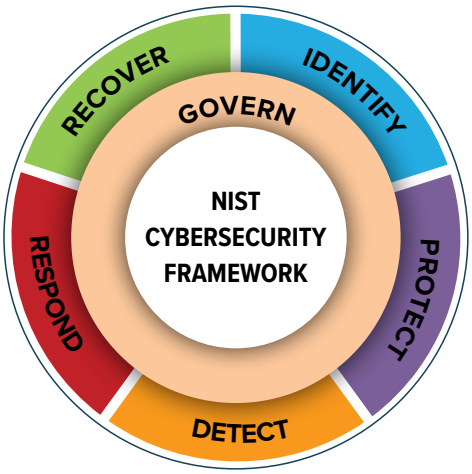
- Comprehensive risk profile.
- Predictive risk analysis, including industry- and technology-specific risks.
- Recommendations to prevent costly network and system breaches.

To learn how we put this into practice, please review our detailed technical methodologies on the following pages.

NIST CSF 2.0 Risk Assessment

Our approach to NIST Cybersecurity Framework (CSF) 2.0 assessments will begin with understanding the Village's business objectives, strategies, and cybersecurity posture. We will then map the gathered information to all NIST CSF 2.0 sub-categories. This allows our team to assess the Village's current tier profile and, in collaboration with its project manager, determine a target tier profile.

Throughout the assessment, Securance will evaluate the Village's CJIS compliance in conjunction with NIST CSF standards in applicable areas, including but not limited to security awareness training, incident response, access controls, and data security.



Our assessment will review the following control areas and all their components to define the Village's cybersecurity posture and risk appetite:

OUR PROCESS

Our team will work with the Village's subject-matter experts to define objectives tailored to each category and sub-category within each function and list the Village's initiatives to achieve the objective. Where initiatives are not in place, we will work with the Village's IT team to define actionable initiatives.

Our team will request and review artifacts supporting the Village's current state for each sub-category in each of the six functions. Our review will be augmented by interviews of the Village's key persons responsible for or knowledgeable about each sub-category. As part of this process, we will assess the Village's current-state tier relative to the framework.

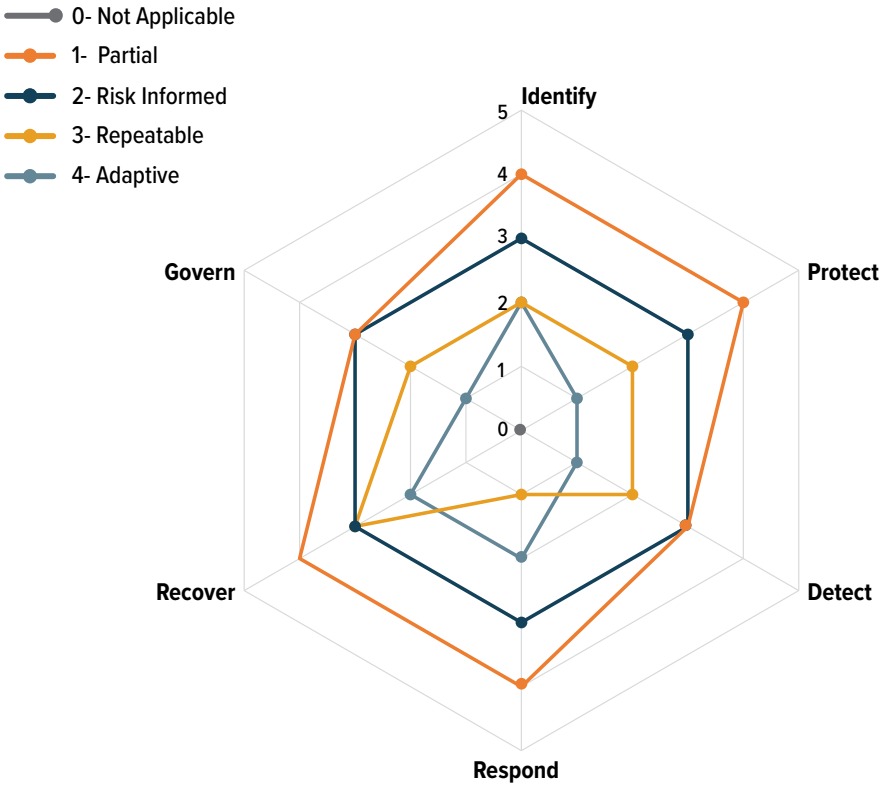
- Tier 1: Partial — Organizational awareness of cybersecurity risks is minimal, and risk is managed in an ad hoc, case-by-case way.
- Tier 2: Risk Informed — There is organizational awareness of risk and cybersecurity protection needs, but no consistent or formal risk management approach has been established.
- Tier 3: Repeatable — Formally approved risk management practices are established, shared, and regularly updated.

NIST CSF 2.0 Risk Assessment (continued)

OUR PROCESS (CONTINUED)

- Tier 4: Adaptive — Cybersecurity risk management is built into the organization's culture, and practices are continuously adapted and improved in response to evolving threats.

An example of how we display the current state by Tier is below.



For each sub-category we will identify an actionable recommendation to move the Village to the next highest tier. This information will be presented in a NIST CSF Roadmap for Improvement.

THEIR APPROACH

- A one-size-fits all assessment that fails to recognize the organization's unique risk profile.

THE SECURANCE WAY...

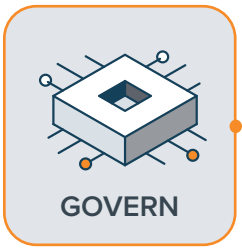
- A customized and evidence-based assessment involving input from various managers, staff, and stakeholders.
- A roadmap designed to improve the maturity of the Village's cybersecurity posture.

....DELIVERS **EXTRA VALUE** TO YOU.

- The Village receives specific, feasible, and clearly communicated recommendations for improving its cybersecurity posture.

NIST CSF 2.0 Risk Assessment (continued)

Below and on the following pages, we elaborate on what our consultants look for when assessing each of the NIST CSF 2.0 sub-categories:



We will assess governance over the Village's overall enterprise risk management. Both cybersecurity and bad actors are perpetually evolving. It is essential to update your risk strategies with the appropriate policies, procedures, and processes to be in alignment with your goals and combat new threats. This function will strengthen your enterprise's governance.

- Organizational Content (GV.OC) — Understand the Village's objectives and priorities and where they fall in the supply chain.
- Risk Management Strategy (GV.RM) — Assess the strategy based on the Village's risk appetite and tolerance.
- Roles, Responsibilities, and Authorities (GV.RR) — Determine whether roles and responsibilities are defined, communicated and enforced.
- Policy (GV.PO) — Review established, communicated, and implemented processes and supporting documentation.
- Oversight (GV.OV) — Review the results of any organization-wide cybersecurity assessment to determine the impact on the risk management strategy.
- Cybersecurity Supply Chain Risk Management (GV.SC) — Assess risk management policies and processes associated with suppliers and other third parties.

We will evaluate the Village's cybersecurity posture. This will include:

- Asset Management (ID.AM) — Assess the Village's hardware and software assets management program.
- Risk Assessment (ID.RA) — Assess internal and external threats.
- Improvement (ID.IM) — Identify improvements across all CSF functions.

We will review the design and test the effectiveness of controls intended to protect data and systems from cyber incidents.

- Identify Management, Authentication, and Access Control (PR.AA) — Assess control access to data and systems.
- Awareness and Training (PR.AT) — Review the Village's end-user security awareness training program.

NIST CSF 2.0 Risk Assessment (continued)

- Data Security (PR.DS) — Assess security and controls over the Village's data.
- Platform Security (PR.PS) — Evaluate the confidentiality, integrity, and availability of physical and virtual platforms.
- Technology Infrastructure Resilience (PR.IR) — Assess management of security architectures to protect assets.

We will assess the Village's system to detect cyber events in a timely manner to reduce their chance of becoming incidents.

- Continuous Monitoring (DE.CM) — Review the monitor resources and assets nonstop.
- Adverse Event Analysis (DE.AE) — Assess abnormalities and understand their potential cybersecurity threat

We will assess how the Village responds to a cybersecurity attack. We will measure how well it contains an event, maintains its reputation, learns from the situation, and reduces inactivity time.

- Incident Management (RS.MA) — Assess management of cybersecurity incidents.
- Analysis (RS.AN) — Assess the analysis processes at the Village.
- Incident Response Reporting and Communication (RS.CO) — Review the communication process with the Village stakeholders and other key personnel.
- Incident Mitigation (RS.MI) — Review the processes in place to mitigate and contain cyber incidents.

We will review the Village's recovery capabilities after a cybersecurity incident to ensure continuity of operations.

- Incident Recovery Plan Execution (RC.RP) — Review the plans and procedures implemented to restore data and systems affected during cybersecurity incidents.
- Incident Recovery Communication (RC.CO) — Assess the line of communication between IT staff and stakeholders for the sake of transparency.

Active Directory Assessment

Active Directory, Azure AD, and multi-factor authentication tool vulnerabilities can give attackers virtually unrestricted access to your organization's network and resources. Securance's methodology for assessing the security of directory services is comprehensive and supports testing the entire architecture, users, and objects to decrease the likelihood of abuse and escalation attacks, including discovering indicators of exposure (IoEs) and indicators of compromise (IoCs) in your hybrid AD environment.

OUR PROCESS

- Our process begins with gaining an understanding of the design of the directory services, including:
  - Domain Services – used to store directory information and manage users and resources
  - Lightweight Directory Services – manages multiple instances on one system and holds directory data in data stores
  - Certificate Services – issue and management of digital security certificates
  - Federation Services – manages user authentication to multiple application, including on different networks
  - Rights Management Services – content encryption and controls access permissions to content

- We evaluate the most common threats, including:
  - Default settings: Microsoft provides Windows AD with predefined security settings, which may not be enough for your organization's needs. Especially since hackers are already familiar with default settings and can use this knowledge when attempting to find and exploit AD security gaps.
  - Unnecessarily broad access rights: There's always a risk that system administrators may grant too many privileges to a certain user or group of users. When provided with a higher level of access than needed to perform their jobs, users can be tempted to abuse their access rights with malicious intent. Also, if accounts with extra access privileges are compromised, external attackers will have access to your most valuable resources and data.

Active Directory Assessment (continued)

OUR PROCESS (CONTINUED)

- Weak passwords for admin accounts: Hackers are likely to use brute force attacks on AD environments, targeting uncomplex passwords for administrative accounts. If those passwords are easy to guess, your organization's data security is at risk.
- Unpatched vulnerabilities on AD servers: Updating software to the latest version along with searching for and patching vulnerabilities is crucial. Otherwise, hackers can find their way into your organization's IT environment by exploiting unpatched applications and operating systems on AD servers.

We also perform a granular view of the following:

- Domain structure
  - Forest, organizational units and their links to group policy objects (GPO)
  - Trusted and trusting domains
  - Use of service accounts
- Use and configuration of multi-factor authentication
- Domain policies
  - Password settings objects or default password policy
  - Audit policy
- Security Option Settings controlled via the registry
- User attributes
  - Privileged user account management
  - Use of shared accounts
  - Accounts allowed to dial in
  - Accounts not requiring passwords
  - Discretionary access controls (DAC) for containers
  - Expired, disabled, and locked accounts
  - Home directories, logon scripts, and profiles
  - Local, global, and universal groups and their respective members
  - Passwords 30 days and older
  - Network shares.
  - User and object rights and privileges
  - Users not required to change their passwords
- Use of administrator tools and how they are configured
  - Netwrix: Monitors user activity across multiple critical systems, including AD, Group Policy, file servers, Windows Server, Exchange, Office 365, and SQL Server.
  - Manage Engine ADAudit Plus: Monitors logons, analyze lockouts, detect changes to users, groups, organizational units (OUs), group

Active Directory Assessment (continued)

OUR PROCESS (CONTINUED)

- policy objects (GPOs), and other AD objects
- Microsoft AD Audit: Plays a critical role in maintaining security, compliance, and operational efficiency within your Windows Server environment
- Microsoft Best Practices Analyzer (BPA): Measures a role's compliance with best-practice rules across eight categories related to effectiveness, trustworthiness, and reliability

- AD host configuration
  - If access to the operating system is obtained or provided, we perform a detailed security review of the operating system configuration. These procedures are performed against all servers that comprise the AD host configuration. Tools used include Rapid7, Tenable, Qualys, and other's based on the fingerprint of the operating system.

- Then, we compare AD configuration and security to industry standards and best practices.

THEIR APPROACH

- Focuses only on basic checks and misses critical areas and generates a generic report without actionable insights.

THE SECURANCE WAY...

- Covers all aspects of AD, including domain controllers, trusts, group policies, security settings, and all user accounts.
- Examines both technical and organizational aspects.

....DELIVERS **EXTRA VALUE** TO YOU.

- Securance will provide the Village with detailed documentation, including findings, recommendations, and remediation step that considers the Village's unique environment, business needs, and compliance requirements.

Internal and External Network Vulnerability Assessment

Vulnerability assessments are fundamental to an organization's security against internal and external cyber threats. With over 22 years of experiencing conducting these assessments for clients in every industry, including local governments. Securance understands how to maximize the value and efficiency of every step in the testing process. Our team will consider the Village's unique digital landscape and adjust our practices to meet its needs, including which method of testing best aligns with its security objectives:

- **Black Box:** the Village does not provide Securance with any internal knowledge of the target system that is not publicly available.
- **Gray Box:** the Village provides Securance with some knowledge of the network's internals, which may include design and architecture documentation and an account internal to the network.
- **White Box:** the Village provides Securance with all information about the target network.

Securance will utilize a combination of industry-leading techniques during this engagement, including the National Institute of Standards and Technology (NIST) Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment), Information Systems Security Assessment Framework (ISSAF), Open-Source Security Testing Methodology Manual (OSSTMM), Open Worldwide Application Security Project (OWASP), and Penetration Testing Execution Standard (PTES).

- Planning the Assessment
- Information Gathering
- Vulnerability Assessment
- Advanced Penetration Testing
- Identifying and Removing False Positives

PLANNING THE ASSESSMENT

- Identify client resources.
- Develop rules of engagement.
  - Securance will work with the Village to confirm and agree upon clear rules of engagement for the project, including details about:
    - Project scope of effort
    - Tool configuration
    - The Village's unique IT environment
    - Privileged testing authority
    - VoIP solution | scan
    - Third-party hosted IP scans
    - How to handle scope creep
    - The client's IP address
    - Approved dates, times, and tools
    - Interest in whitelisting Securance's lab IP
    - Communication rules
    - Escalation plan
    - The Village and Securance contact information
    - The Village's specific concerns
- Develop a specific scope that addresses which systems (if any) should not be assessed.

Internal and External Network Vulnerability Assessment (continued)

INFORMATION GATHERING

External Assessment

- Search for public information about the Village's Internet presence using the American Registry for Internet Numbers (ARIN), social media, the surface web, and the dark web.
- Identify weaknesses in the registration process, like publishing internal staff contact information.

Internal Assessment

- Connect to a “hot” port on the internal network, if applicable for selected testing method.
- Obtain internal IP information about approved targets.
- In stealth mode, perform a port sweep to develop a map of the internal network structure.
- Attempt to identify servers, applications, network infrastructure devices, database systems, web applications, and other technologies based on ports and services.
- Assess fingerprint information.
- Review information with the Village's PM.

VULNERABILITY ASSESSMENT

- Analyze information gathered.
- Our testing includes both soft and aggressive techniques:
  - Soft Techniques
    - Passive port scanning to identify open ports and listening services
    - Default password identification
    - “Safe check” vulnerability scanning
    - Software version identification
    - Firmware version identification
    - Multiple-tool scanning
  - Aggressive Techniques
    - Multi-location network sniffing
    - Applying a denial-of-service attack
    - Aggressive vulnerability scanning
- Identify modes of access.
- Locate trusted hosts.
- Identify sensitive data flows.
- Perform vulnerability scans using various tools and cross-reference available services against a comprehensive listing of vulnerability databases.

Internal and External Network Vulnerability Assessment (continued)

The Securance vulnerability assessment and penetration test performs a series of checks to discover potential methods of breaching your systems. Below is a summary of checks we include in our assessment:

- Buffer overflows
- Hard-coded secrets
- Router vulnerability detection
- Bypass authentication
- HTML source code analysis
- Sensitive error messages
- Case studies and presentations info
- Integer overflows
- Server | service fingerprinting
- Cross-site tracing
- Open relay scan
- SSL configuration
- Database scan
- OS fingerprinting
- Trade publications information
- Default passwords
- Password cracking and guessing
- Command injection
- Job postings information
- Session ID prediction
- Cross-site request forgery
- LDAP injection
- SNMP scan
- Cross-site scripting
- Mailing lists information
- SQL injection
- Validate cryptographic strength
- Directory traversal
- Ping sweep
- Vulnerable sample applications
- DNS records information
- Port scanning
- Web server vulnerability scan
- Firewalking

IDENTIFY AND REMOVE FALSE POSITIVES

The following manual testing methods will be used to identify false positives:

- Tools will be configured specifically to the operating system or firmware version of the network device or system being tested.
- Our staff will rely on the experience of the subject-matter expert to identify false positives, including those caused by backporting.
- Prior to reporting, we will validate our technical findings with IT management.

Internal and External Network Vulnerability Assessment (continued)

THEIR APPROACH

- Uses automated tools with limited manual tests and no checks for false positives.

THE SECURANCE WAY...

- Remains flexible to the Village's larger goals and potentially changing needs as the engagement unfolds.
- Includes investigation of results to ensure that no "false positives" are left with the Village.
- Pairs automated tools with manual testing to provide the Village a thorough, accurate assessment.

.... DELIVERS EXTRA VALUE TO YOU.

- The Village will receive a detailed report that ranks identified vulnerabilities based on ease of exploit, the effort required to remediate them, and the estimated impact of exploit on the Village's business.

Software Tools

Securance may use these tools during the penetration testing engagements, depending on the Village's needs:

- Network Scanning and Enumeration Tools
  - NMAP Scanner: Used for network exploration, host discovery, and security auditing; can map an entire network to find its open ports and services and fingerprint an operating system and can adapt to network conditions, including latency and congestion, during a scan
  - NESSUS Scanner: Network vulnerability assessment tool for measuring system risks; used to probe systems and report vulnerabilities that might create an exposure
  - GFI LANguard: Designed specifically for Windows and enables users to manage and maintain end-point protection across a network; provides visibility into all the elements in a network, and helps assess where there may be potential vulnerabilities
  - Netcat: A UNIX utility that reads and writes data across network connections, using TCP or UDP protocol, which can be used for network troubleshooting, port scanning, and file transferring
  - Wireshark: Allows users to capture and browse the traffic running on a computer network; supports hundreds of protocols and can analyze encrypted traffic if the encryption keys are provided
  - Gobuster: Efficient software that can be used to enumerate hidden directories and files quickly. Many web applications use default directories and file names that are relatively easy to spot. This tool can use brute-force techniques to discover them
  - Amass: Efficient for DNS (Domain Name System) and subdomain enumeration; actively maintained and updated to keep up with the latest techniques and methodologies, and combines various reconnaissance and gathering techniques

Internal and External Network Vulnerability Assessment (continued)

- SAINT: A vulnerability scanner approved by the Payment Card Industry (PCI) that scans networks, servers, and applications for weaknesses and provides detailed reports and remediation recommendations

- Wireless Network Scanning Tools
  - Hashcat: Provides advanced password recovery features and lets testers crack Wi-Fi passwords or password-protected documents such as ZIP files
  - Aircrack-ng: Tool for analyzing and cracking wireless networks. Aircrack-ng's main focuses include packet capture and export of data to text files for further processing, replay attacks, de-authentication, fake access points, and others via packet injection, and Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) for WPA and WPA2 cracking
  - Wifite: A wireless network auditor that deals with current or legacy attacks against WEP and WPA2. It is good for retrieving the password of a wireless access point such as a router
- Password Cracking Tools
  - John the Ripper: Supports hundreds of hash and cipher types, including for user passwords of Unix flavors, macOS, Windows, web apps, groupware, database servers, network traffic captures, encrypted private keys, filesystems and disks, archives, and document files
  - Medusa: A powerful brute-force tool that supports thread-based parallel testing like simultaneous brute-force attack
  - Ncrack: Can test all hosts and devices in a network for weak passwords; a set of command lines that can scan large networks, allowing sophisticated brute-force attacks
  - Rubeus: A tool used in penetration testing for Kerberos sessions that exploits the identified vulnerabilities and performs functions such as crafting keys and granting access using forged certificates
- Sniffing Tools:
  - Wireshark: A network sniffer and TCP I IP analysis tool. It can capture and display the data traveling back and forth on a network in real-time or by analyzing saved capture files; supports hundreds of protocols and can analyze encrypted traffic
  - Ettercap: A packet sniffer that allows users to modify data on the fly and run man-in-the-middle (MITM) attacks; commonly used to intercept passwords with ARP (Address Resolution Protocol) poisoning or spoofing
  - Tcpdump: A powerful command-line packet analyzer that prints out a description of the contents of packets on a network interface, preceded by a timestamp
  - Wfuzz: Runs brute-force attacks on various elements such as directories, scripts, or forms

Wireless Network Security Assessment

Securance assesses the configuration and security of on-premise controller, cloud-based controller, and access point-based wireless networks. Our consultants will interview the wireless network administrator and review the following security controls:

Controller-Based Networks

For wireless networks with an on-premise controller or cloud-based controller, Securance will:

- Assess controller configurations.
- Evaluate rogue access point detection and management.
- Uncover or identify hidden SSIDs.
- Assess encryption strength.
- Review network segmentation, including user authentication and access.
- Review administrative access controls and logging.
- Confirm access points can only receive configurations from the controller.
- Capture a handshake and attempt to crack the encryption.
- Install a rogue access point as a Pineapple device to attempt to divert user access.
- Assess device authentication.

For wireless networks with a cloud-based controller, Securance will evaluate the controls listed above to the extent the configurations are modifiable by the wireless administrator.

Access Point-Based Wireless Networks

Our access point-based assessment is similar to our controller-based assessment. However, because each access point has its own configuration, we will assess each access point individually.

Wireless Network Security Assessment (continued)

Penetration Testing

Using assorted wireless radio devices, including Pineapple tools and various wireless adapters, we will intercept encrypted and unencrypted network packets. Depending on the rules of engagement, we will:

OUR PROCESS (CONTINUED)

- Passively sniff and attempt to capture handshakes between the access point and client.
- Attempt to deauthenticate clients from the wireless network and capture the reestablished handshakes between the access point and client.
- Establish a rogue access point to lure client devices and capture their wireless authentication credentials.
- Attempt to crack the encrypted credentials and use them to breach the wireless network.

After gaining access to the wireless network, we will:

- Deploy executables and scripts to gain a presence on the network.
- Capture device and network information.
- Escalate privileges.
- Disable local firewalls and antivirus software.
- Create a new privileged user.
- Move laterally to access and gain control of the domain controller(s).
- Exfiltrate data from host machines.
- Hide evidence of our breach.

Securance may use the following tools in this assessment:

- Vistumbler
- iStumbler
- Kismet
- Aircrack-ng suite
- Ncrack
- Hashcat
- John the Ripper
- Cain and Abel
- Mimikatz
- Advanced IP Scanner

THEIR APPROACH

- Includes only interviews and configuration review of the wireless network.

THE SECURANCE WAY...

- Assesses both controllers and access points.
- Uses Pineapples to capture and decrypt handshakes to penetrate the internal network.

....DELIVERS EXTRA VALUE TO YOU.

- Securance provides a comprehensive analysis of how the wireless network can be used as a vector to attack the internal network, as well as detailed recommendations to secure the wireless network.

Project Timeline

The table below outlines each step in our assessment process, designating major tasks, subtasks, key milestones, and the anticipated task owner. This project plan will be refined during the planning phases of the engagement between Securance and the Village.

Cyber Risk Evaluation	Week 1	Week 2	Week 3	Resources
Planning and Design				
Kick-off Meeting				Paul Ashe Village PM
Prepare Client Assistance Memo				SC Consultants
Respond to Client Assistance Request				Village Staff
Review Client Assistance Request				SC Consultants
Risk Evaluation				
NIST CSF Risk Assessment				SC Consultants
Assess key people, processes, and technologies against NIST CSF, and CJIS (as applicable), to identify control gaps				SC Consultants
Review IT governance documents				SC Consultants
Conduct interviews with relevant IT staff				Paul Ashe Village Staff
Perform gap analysis of current security tier level against NIST CSF				SC Consultants
Develop a current state framework profile				SC Consultants
Develop a NIST CSF roadmap				SC Consultants
Identity Services Health Check				
Active Directory Assessment				SC Consultants
Gain an understanding of the AD architecture				SC Consultants
Review AD configuration				SC Consultants
Assess InTune configuration				SC Consultants
Perform application programming interface (API) technical testing				SC Consultants
Compile findings and review with Village PM			1	Paul Ashe Village PM

▼ PROJECT STATUS MEETINGS ◆ WORK PRODUCT REVIEWS

Project Timeline (continued)

Cyber Risk Evaluation	Week 3	Week 4	Resources
Network Vulnerability Assessment			
Internal Network Vulnerability Assessment			SC Consultants
Obtain internal network IP information			SC Consultants
Perform vulnerability scanning			SC Consultants
Analyze results to remove false positives			SC Consultants
Review results of scan with the Village		2	Paul Ashe Village PM
External Network Vulnerability Assessment			SC Consultants
Perform information gathering of public information			SC Consultants
Perform vulnerability scanning			SC Consultants
Analyze results to remove false positives			SC Consultants
Review results of scan with the Village		3	Paul Ashe Village PM
Wireless Assessment			SC Consultants
Identify controllers and SSIDs			SC Consultants
Interview wireless network administrator			SC Consultants
Perform wireless network scanning			SC Consultants
Obtain and assess wireless or AP configuration			SC Consultants
Perform manual penetration activities			SC Consultants
Analyze results and review with wireless administrator		4	Paul Ashe Village Staff
Draft Management Report			SC Consultants
Review Management Report with the Village's Key Stakeholders			Paul Ashe Village Stakeholders
Review Final Report and Hold Exit Conference	**TBD**		Paul Ashe Village PM

▼ PROJECT STATUS MEETINGS ◆ WORK PRODUCT REVIEWS

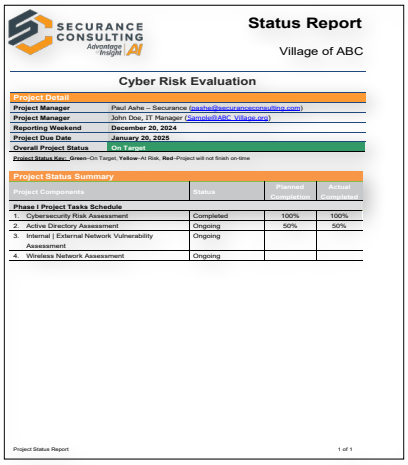
Project Management

Securance is dedicated to performing this engagement as efficiently as possible. The assigned engagement manager (EM) will be responsible for ensuring project success by facilitating regular communication and providing status reports that will track progress, possible risks, and other pertinent information. Their specific responsibilities are outlined below:

The EM will manage and oversee the entire project and be responsible for the following tasks:

- **Project Kick-Off:** Securance will hold a kick-off conference with the Village. During this meeting, we will introduce our project team, and define the project scope, objectives, timeline, and deliverables. We will also review the Client Assistance Request, which is a memo listing all documentation and interviews required to complete the assessment. We will establish the frequency of meetings and project status updates, key stakeholders, and lines of communication for both the Village and Securance.
- **Work Plan:** Within one week of receiving the notice to proceed, Securance will submit a detailed work plan for the Village's review and approval. Our work plan will include due dates for all deliverables, as well as intermediate milestones. We will update the work plan, as necessary, throughout the project.
- **Status Reports:** Throughout the engagement, the Village's project manager (PM) will receive project status reports that will identify the past week's completed tasks, planned tasks for the upcoming week, pending requests for information, and any issues and | or risks that have been identified, with actions taken to mitigate them.

CLICK
ON THUMBNAIL TO VIEW THE STATUS REPORT



SECURANCE CONSULTING
Advantage | Insight | AI

Status Report
Village of ABC

Cyber Risk Evaluation

Project Detail	
Project Manager	Paul Ashe – Securance (pashe@securanceconsulting.com)
Project Manager	John Doe, IT Manager (Jsmith@ABC_Village.org)
Reporting Weekend	December 20, 2024
Project Due Date	January 20, 2025
Overall Project Status	On Target

Project Status Key: Green–On Target, Yellow–At Risk, Red–Project will not finish on-time

Project Status Summary			
Project Components	Status	Planned % Completion	Actual % Complete
Phase I Project Tasks Schedule			
1. Cybersecurity Risk Assessment	Completed	100%	100%
2. Active Directory Assessment	Ongoing	50%	50%
3. Internal | External Network Vulnerability Assessment	Ongoing		
4. Wireless Network Assessment	Ongoing		

Project Status Report 1 of 1

Project Management (continued)

OUR PROCESS (CONTINUED)

Shared Tasks

Securance's EM and key personnel will be responsible for the following tasks throughout the Village's project:

- Issue and Risk Management: Securance prioritizes issues by considering the following:
  - Overall impact an issue may have on the project.
  - Length of time the issue has been unresolved.
  - Criticality of the issue to the Village's IT environment.

These factors will be looked at as a whole and discussed with the Village's PM to determine the ultimate priority of each issue. Additionally, as part of our status reports, we will document all project findings and related evidence in an "Issue Tracker" document that will also be shared with the Village's PM. The use of this tracker helps to avoid unwanted surprises and | or disputes over findings.

- Continuous Improvement: We will invite the Village employees to shadow our consultants as they execute technical engagements. Additionally, to ensure continuous improvement of the Village's security objectives, our team will conduct a knowledge transfer session upon completion of the assessment.

THEIR APPROACH

- Limited communications related to project status.
- Findings not communicated until drafted.

THE SECURANCE WAY...

- Constant and consistent project communication.
- Immediate communication of urgent and critical findings.
- Confirmation of findings prior to drafting.

....DELIVERS EXTRA VALUE TO YOU.

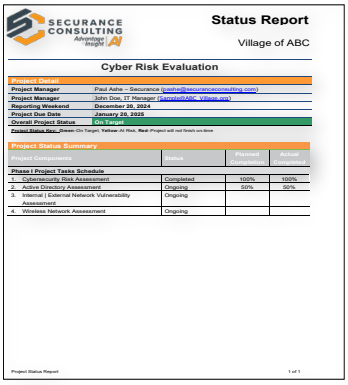
- Securance provides exceptional project management expertise, leveraging 22 years of experience conducting more than 3,000 cybersecurity risk assessments, to deliver project success on time and on budget.

Reporting | Deliverables

Status Reporting

Throughout the engagement, the Village's PM will receive project status reports that will identify the past week's completed tasks, planned tasks for the upcoming week, pending requests for information, and any issues and | or risks that have been identified, with actions taken to mitigate them.

CLICK
ON THUMBNAIL TO VIEW THE STATUS REPORT


Status Report
Village of ABC
Cyber Risk Evaluation

Cyber Risk Evaluation Management Report

Within one week of completing our fieldwork for the cyber risk evaluation, Securance will provide the Village with a board-ready management report tailored to its environment and needs and developed with input from the Village's stakeholders and IT management. Our analysis of the risks identified within the Village's environment will take into account its threat profile and the likelihood and impact of exploitation of existing vulnerabilities. The report will document our analysis, prioritize risks based on their potential impact on the business, provide realistic remediation recommendations aligned with the Village's risk appetite, and include a budgetary analysis of all recommendations. Comprised of two sections, the report will include an executive summary and a detailed cyber risk evaluation report, each of which is described on the following pages.

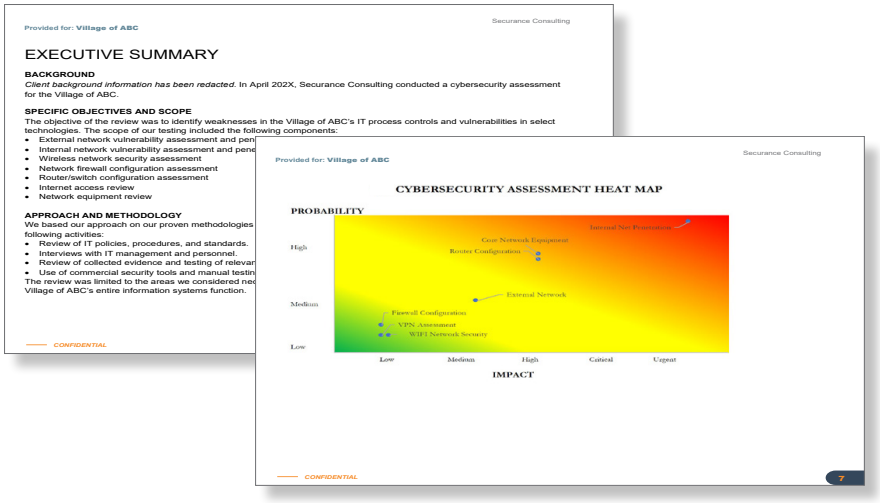
During the engagement, if Securance identifies a vulnerability defined as urgent or critical by the Common Vulnerability Scoring System (CVSS), or any other risk that we feel needs immediate attention, our team will promptly notify the Village. Once the Village's staff has addressed the risk or threat, Securance will reassess it to validate remediation success.

Reporting | Deliverables

Executive Summary

The executive summary will outline the engagement's scope, approach, findings, and recommendations in a manner suitable for management and will be presented to the Village's stakeholders during the exit conference.

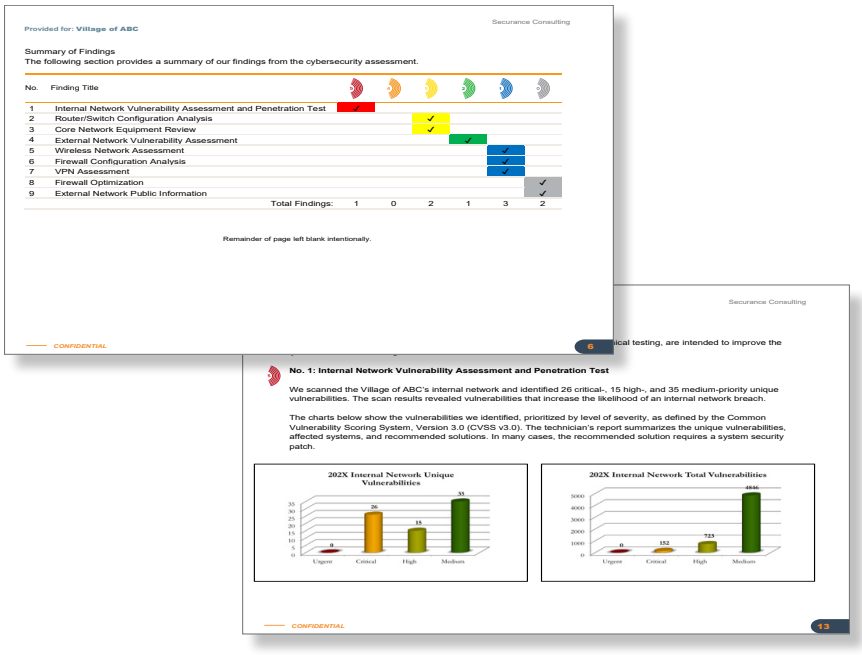
CLICK
ON THUMBNAILS TO VIEW THE REPORTS



Detailed Cyber Risk Evaluation Report

The detailed cyber risk evaluation report will provide specifics regarding the project scope, approach, and methodology, as well as findings, actionable recommendations, and a budgetary analysis co-developed by Securance and the Village.

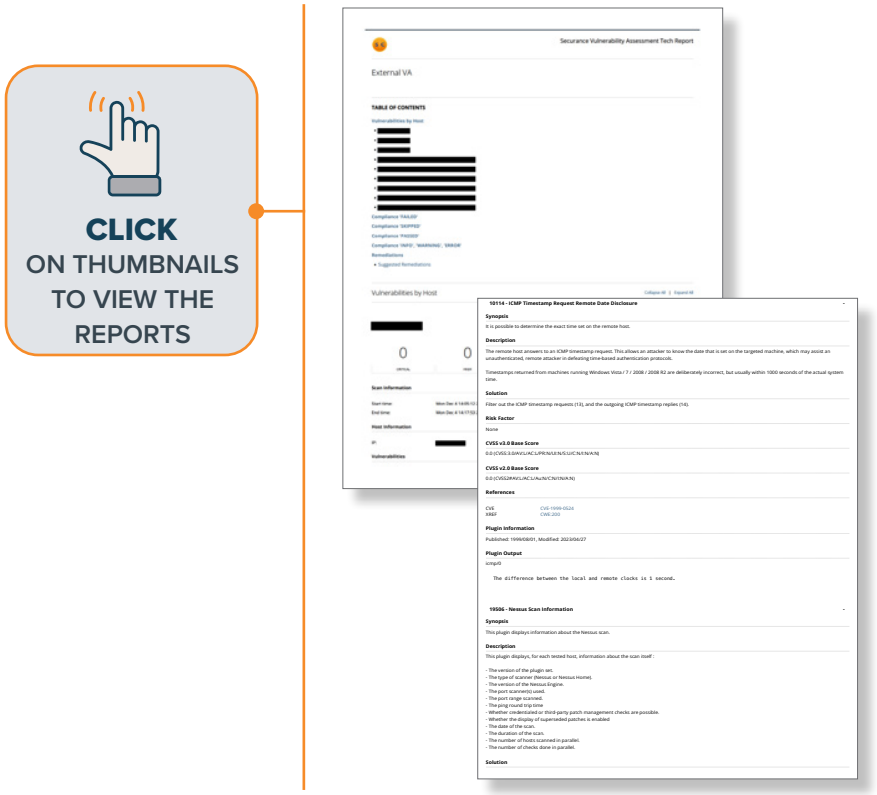
CLICK
ON THUMBNAILS TO VIEW THE REPORTS



Reporting | Deliverables (continued)

Technician's Report (Network Vulnerability Assessments Only)

Along with the management report, the Village will receive a technician's report that is intended to guide engineers and administrators through the remediation process. The technician's report will contain raw data extracted from our security tools. While the management report will focus on urgent, critical, high, and medium risks and vulnerabilities that require management's attention, the technician's report will cover all vulnerabilities, even low-risk vulnerabilities and advisory comments.



SECTION 7: COST OF PROPOSAL

Securance has provided itemized pricing for the major aspects of this project in the table below.

Project Scope Item	Hours	Line Item Fee
Planning and Design (includes kick-off call, client assistance request memo, and final project plan) — Value Add	16	~~$2,048~~
Risk Evaluation (based on NIST CSF, including CJIS requirements for applicable processes and control areas)	110	$14,080
Identity Services Health Check (AD assessment)	24	$3,072
Network Vulnerability Assessment	-	-
External Network Vulnerability Assessment (25 IPs) — Value Add	12	~~$1,536~~
Internal Network Vulnerability Assessment (230 IPs)	20	$2,560
Wireless Network Assessment (policy, rules, settings, and configuration review)	12	$1,536
Cyber Risk Evaluation Management Report	26	$3,328
Project Management — Value Add	8	~~$1,024~~
Status Reporting — Value Add	12	~~$1,536~~
Knowledge Transfer — Value Add	4	~~$512~~
24 Hours of Remediation Support Consulting — Value Add	16	~~$2,048~~
Independent Project Review*	Included	Included
Subtotal	-	**$33,280**
Value Add Price Reduction	-	**~~$8,074~~**
Total	**260**	**$24,576**

**Each assessment completed by Securance is reviewed by a consultant independent of the project, to ensure that the engagement thoroughly addresses all scope items, all observations are factual and appropriately documented, recommendations are feasible and customized to the client, and all assessment components adhere to the firm's quality control standards.*

The professional fees listed above are inclusive of all out-of-pocket expenses, and the Village will **NOT** be billed for expenses such as mileage, meals, and incidentals. No additional fees beyond those proposed will be charged to the Village without the Village's prior written consent.

Hourly Rate

Securance's cost proposal is based on an hourly rate of $128, inclusive of labor, system licenses, and other reimbursable expenses. The hourly rate applies to all tasks and personnel resources required to complete this project. Any follow-up assessments or consulting engagements will be billed at the same hourly rate.

SECTION 7: COST OF PROPOSAL

Assumptions | Payment Terms

NTE Cost Proposal

To provide the Village with cost certainty, we are offering a "not to exceed" (NTE) proposal, which means that the total cost of the project or service will not exceed the amount specified on the previous page. However, we guarantee we will complete all items identified in the scope of services and listed in the contract or statement of work. Often the actual project fee is less than the NTE fee listed. Our reasons for using this pricing model include:

- Our methodologies assume IT processes are mature and all components of the assessment are already in place. However, if we identify assessment components that are immature or were recently implemented, our testing effort will be less than proposed. This could result in significant savings to the Village.
- We may need to conduct fewer interviews than anticipated to gain a full understanding of the risk associated with an assessment component. We can then pass those savings on to the Village.
- The Village's project manager may ask our team to suspend additional testing based on the risks, threats, and vulnerabilities we discover and report. In this situation, our effort will be reduced, and we will pass those savings on to the Village or allocate those hours to other areas, as deemed necessary.
- The Village's project manager may wish to change the scope based on additional information obtained before project execution. In that case, there is no need to re-negotiate fees as our model is flexible to permit scope changes.

Assumptions

Securance's proposed fees are based on the information that has been made available to us and on our understanding of the engagement. If the basis of our pricing is inaccurate, then the total cost to complete this engagement may differ from the firm, fixed price in this proposal. If events or circumstances, such as changes in scope, loss or unavailability of the Village personnel, or unavailability of documentation occur, Securance will determine their effect on the engagement scope, timing, and | or fees and promptly notify the Village of any such changes. Securance will not proceed with any changes or additions to the scope of work without the Village's explicit written approval.

Payment Terms

Securance will submit an invoice after delivering a draft management report. All fees are due within 60 days following receipt of invoice. Securance will deliver the final management report following receipt of payment.

Project Hours

Engagement manager Paul Ashe will service approximately 70 hours of the Village's 260 total project hours. Senior cybersecurity consultant Montrell will service approximately 90, and senior cybersecurity consultants Ray and Jerry will each service approximately 50 hours.

SECTION 7: COST OF PROPOSAL

Building a Successful Partnership

For Securance, this is not just another project. It is an opportunity to help optimize the Village's resource allocation and risk management so it can securely provide the services its citizens and employees rely on. Through comprehensive assessments and detailed reporting, Securance will set the Village up for a resilient security posture.

After reviewing the Village's needs and taking the time to understand its business, Securance believes that we are the best fit for this opportunity, and **we want to partner with you!**

As one way to demonstrate our commitment to the Village's cybersecurity and the lasting value brought by the Securance advantage, we are offering the following free value adds to enhance our engagement.

Deliverable	Value
Planning and Design	Securance will provide our project planning and design processes at no additional cost to the Village. Our processes include a kick-off meeting | call, client assistance request memo, and a final project plan.
External Network Vulnerability Assessment	Securance will conduct the Village's requested external network vulnerability assessment at no extra charge.
Project Management	At no additional charge, we will oversee the progress and completion of the Village's project from beginning to end. Our proven project management methodology has been used successfully on projects for organizations across the country.
Status Reporting	Securance recognizes the importance of ongoing communication with the Village To ensure the Village's project remains on schedule and that all potential issues are addressed, we will issue weekly status reports and review them with the Village PM during weekly status meetings.
Knowledge Transfer	To ensure our assessment provides high value, fully understandable information, we will conduct a knowledge transfer session with appropriate Village staff. This session will provide answers as to why and how Securance performed specific tasks, so Village staff are able to repeat the tasks as desired.
24 Hours of Remediation Support Consulting	To enhance the effectiveness of this engagement and to demonstrate our commitment to the Village, Securance will include 24 hours of free management-level consulting and remediation support to be used at the Village's discretion.

If you have questions or would like additional information, do not hesitate to contact us. We want to make sure you have everything you need to make your decision.

We want to partner with you and will be your best partner!

SECTION 8: ACKNOWLEDGMENTS, ADDITIONS, AND EXCEPTIONS

Acknowledgments and Exceptions

Securance will meet all of the Village's requirements as stated in the scope of work. Securance does not take any exceptions to the Village's terms and conditions,

Additions

Please see below for additional information about the resources we will need from the Village to complete the project.

When a contract or statement of work is executed, there are specific items Securance will need to perform the engagement. To ensure the Village obtains the most out of its partnership with Securance, we have provided an initial list of information, access requests, and documentation our experienced team will need to hit the ground running.

RESOURCES NEEDED

Access to the Village's Staff

- Adequate access to management and other key personnel for consultation and interviews.
  - Very little of these individuals' time will be taken, but some contact will be necessary
- Access to a project manager for scheduling interviews with appropriate Village staff
- Access to technical staff (if needed) during the length of the technical testing (very little time needed)
- Immediate access on a part-time basis to a cybersecurity staff member who can assist with questions (when needed)

Logical and Other Access Requests

- IP addresses relevant to the project
- Authority to access network components

Client Assistance Request Summary (please see an example on the following page)

Rules of Engagement Memo (please see an example on pages 53 and 54)

Office Space for On-Site Work

- Identification badges or equivalent should be available on arrival (if needed)
- Lockable cabinet for documentation
- Workspace when on site

Sample Client Assistance Request

Securance
2024 Village of North Aurora Client Assistance Request
Location:

No.	Phase I	Description	Status/Notes/Comments
1	External Network	Please provide the contact information for the external network vulnerability assessment.	
2	External Network	Please provide a listing of all of the Internet-facing IP addresses to be assessed.	
3	External Network	Please provide any specific IP addresses that are out-of-scope that may be hosted by 3rd parties or too sensitive to be scanned.	
4	External Network	Please provide any information related to the period of daytime when scanning can be begin.	
5	Internal Network	Please provide the contact information for the internal network vulnerability assessment.	
6	Internal Network	Please provide the address from which we will authorized to work while performing the internal network vulnerability assessment.	
7	Internal Network	Please provide a listing of all of the internal IP addresses to be assessed.	
8	Internal Network	Please confirm if all initial scanning can be performed at one time.	
9	Internal Network	Please advise if there are any specific systems or IP addresses that should not be scanned.	
10	Internal Network	Please advise if there is a VOIP system. These systems typically failover during vulnerability testing.	
11	Internal Network	Please provide all available network diagrams. The more detailed the better.	
12	Wireless Network	Please provide the contact information for the Wireless Network Administrator.	
13	Wireless Network	Please provide a brief summary of the wireless solution implemented by the City of Richmond (i.e., Controller-based, Cloud-based, AP-based).	
14	Wireless Network	How many and what are the SSID's?	
15	Wireless Network	For each SSID please provide the following: a) Encryptions method and strength b) Device detection enabled? c) Access granted (i.e. Internet only, all prodution servers, departmental servers, etc.) d) Is there a specific segment for mobilproduction e) MAC address filtering enabled? f) Sample connection log g) Is device authentication configured?	
16	Security Policies - NIST CSF	Please provide a copy of the IT strategic plan.	
17	Security Policies - NIST CSF	Please advise how IT assets are managed, including hardware, software, and data.	
18	Security Policies - NIST CSF	Please provide a copy of the Cybersecurity Program.	
19	Security Policies - NIST CSF	Please advise if there is a 3rd party Security Operations Center (SOC) to monitor its network 7x24x365.	
20	Security Policies - NIST CSF	Please provide a copy of the Vendor Risk Management program.	
21	Security Policies - NIST CSF	Please provide a copy of the configuration of the Data Loss Prevention (DLP) policy.	
22	Security Policies - NIST CSF	Please provide the contact information (e.g., Name, Email, Phone) of the person within the IT organization, that would have the most knowledge of the following NIST CSF Domain: 1) Identify: Asset Management 2) Identify: Business Environment 3) Identify: IT Governance 4) Identify: IT Risk Assessment 5) Identify: IT Risk Management Strategy 6) Identify: Supply Chain Risk Management	
23	Security Policies - NIST CSF	Please provide the contact information (e.g., Name, Email, Phone) of the person within the IT organization, that would have the most knowledge of the following NIST CSF Domain: 1) Protect: Identify Management Authentication and Access Control 2) Protect: Awareness and Training 3) Protect: Data Security 4) Protect: Information Protection Processes and Procedures 5) Protect: Maintenance 6) Protect: Protective Technology	
24	Security Policies - NIST CSF	Please provide the contact information (e.g., Name, Email, Phone) of the person within the IT organization, that would have the most knowledge of the following NIST CSF Domain: 1) Detect: Anomalies and Events 2) Detect: Security Continuous Monitoring 3) Detect: Detection Processes	

Sample Rules of Engagement Memo

MEMORANDUM

DATE:	December 2024 (version 1.0)
TO:	Village of ABC
FROM:	Securance LLC
RE:	Cyber Risk Evaluation Rules of Engagement (RoE) - SAMPLE

This memo represents the mutually agreed upon RoE for the upcoming cyber risk evaluation.

ITEM	CLIENT RESPONSE
1. Scope of Effort	Internal and External Network Vulnerability Assessments Wireless Network Assessment
2. IT Environment Uniqueness	
3. How to Handle Scope Creep	
4. Approved Date(s)	Internal System:
5. Approved Time(s)	
6. Approved Tool(s)	Webinspect, NStalker, Nmap, Rapid7, Qualys, Tenable, Cobalt Strike, Canvas, D2, Others as necessary
7. Tool Configuration	
○ Disable DDOS (Yes | No)	
○ Disable Brute Force (Yes | No)	
○ Disable Experimental Test (Yes | No)	
○ Privileged Testing (Yes | No)	
○ Disable Intrusive Test (Yes | No)	
○ Scan all TCP|UDP Ports (Yes | No)	
○ Report by Hostname (Yes | No)	
8. If Privileged Testing (Admin Level: Yes | No)	
9. Scan 3rd Party-Hosted IP's (Yes | No)	
10. Provide Client Lab's IP Address (Yes | No)	

Sample Rules of Engagement Memo (continued)

MEMORANDUM

ITEM	CLIENT RESPONSE
13. Interest in Whitelisting Lab's IP	
14. Communication Ground Rules	Communication will be via email. Provide daily status updates via: Email SMS Conference Call
15. Escalation Plan	Any signs of disruption, immediately contact consultant to discuss.
16. Communication Tools	Email, mobile and lab's direct phone (see consultant's info)
17. Client Specific Concern 1?	Disruption
18. Client Specific Concern 2?	
19. Securance PM Contact Information	
○ Project Manager Name	
○ Project Manager Email Address	
○ Project Manager Mobile Phone	
○ Project Manager Office/Lab Phone	
20. Security Engineer Contact Information	
○ Consultant Name	
○ Consultant Email Address	
○ Consultant Mobile Phone	
○ Consultant Office/Lab Phone	

By: _____ Title: _____

Securance: Please Sign — Please Type

Name: _____ Date: _____

Please Type — Please Type

By: _____ Title: _____

Client Project Manager: Please Sign — Please Type

Name: _____ Date: _____

Please Type — Please Type

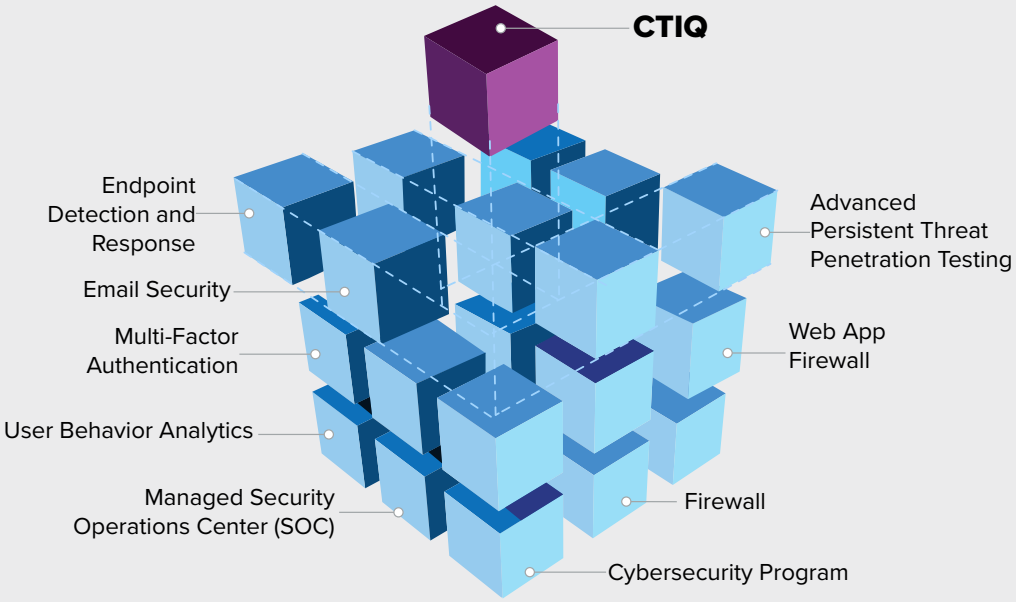
SECTION 9: CERTIFICATE OF INSURANCE

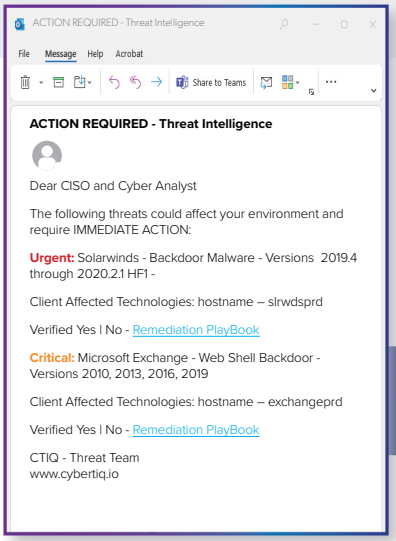
Securance will provide proof of insurance prior to the Village's award of the contract.

THE GROWING CHALLENGE IN CYBERSECURITY

REDUCE ALERT FATIGUE | **RECEIVE ONLY RELEVANT INFORMATION** | **PRIORITIZE THREATS**

REVOLUTIONIZE YOUR CYBER DEFENSE WITH AI-POWERED INTELLIGENCE





ACTION REQUIRED - Threat Intelligence

File Message Help Acrobat

Share to Teams

ACTION REQUIRED - Threat Intelligence

Dear CISO and Cyber Analyst

The following threats could affect your environment and require IMMEDIATE ACTION:

Urgent: Solarwinds - Backdoor Malware - Versions 2019.4 through 2020.2.1 HF1 -

Client Affected Technologies: hostname – slrwdsprd

Verified Yes I No - Remediation PlayBook

Critical: Microsoft Exchange - Web Shell Backdoor - Versions 2010, 2013, 2016, 2019

Client Affected Technologies: hostname – exchangeprd

Verified Yes I No - Remediation PlayBook

CTIQ - Threat Team
www.cybertiq.io

CTIQ utilizes advanced AI technology to gather real-time data from various intelligence sources and centralizes it into one platform. You will receive emails that provide clarity, context, and actionable remediation recommendations specific only to the technology in your environment.

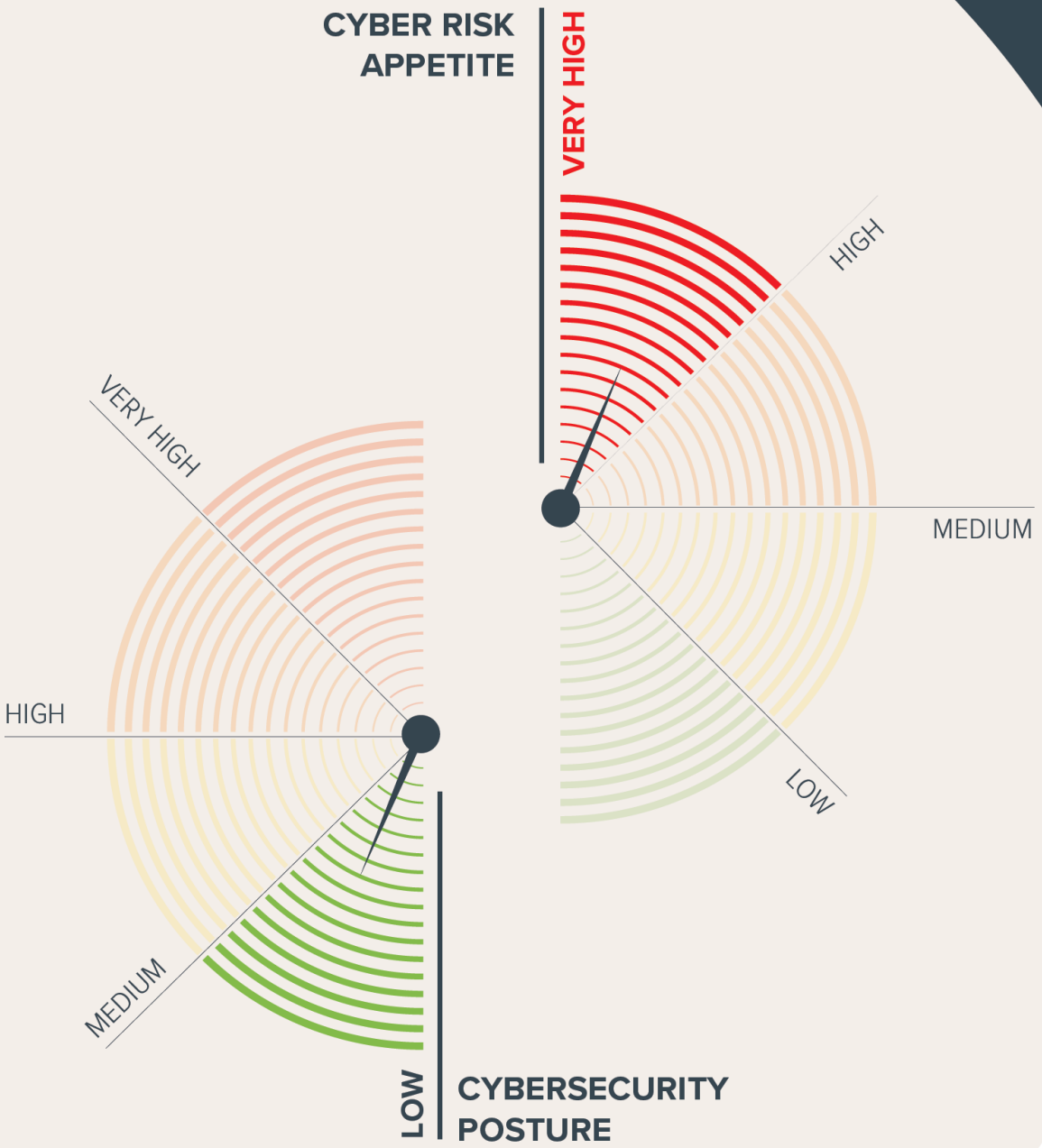
BECOME A BETA CLIENT

https://cybertiq.io/ | info@cybertiq.io

APPENDIX: SAMPLE REPORT

SECURANCE CONSULTING

Advantage of Insight AI



Cybersecurity Assessment

Date: April 23, 202X

VERSION MANAGEMENT

Version	Date Approved	Approved By	Brief Description
1.0.0	April 14, 202X	Securance	Initial Draft
1.1.0	April 18, 202X	Securance	SC Internal Edits
1.2.0	May 3, 202X	Securance	Client Edits
FINAL	May 3, 202X	Securance	

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND

Client background information has been redacted. In April 202X, Securance Consulting conducted a cybersecurity assessment for the Village of ABC.

SPECIFIC OBJECTIVES AND SCOPE

The objective of the review was to identify weaknesses in the Village of ABC's IT process controls and vulnerabilities in select technologies. The scope of our testing included the following components:

- External network vulnerability assessment and penetration testing
- Internal network vulnerability assessment and penetration testing
- Wireless network security assessment
- Network firewall configuration assessment
- Router/switch configuration assessment
- Internet access review
- Network equipment review

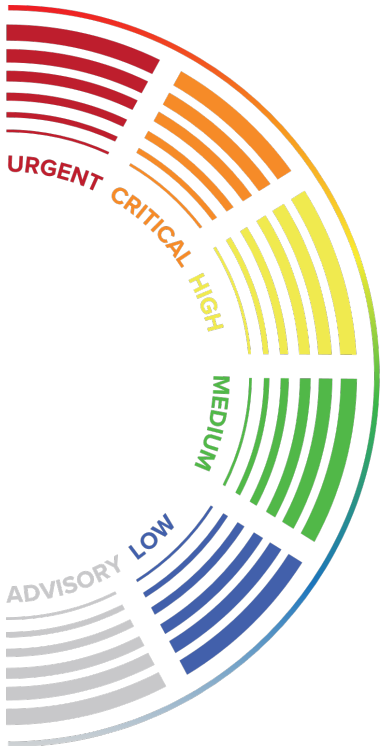
APPROACH AND METHODOLOGY

We based our approach on our proven methodologies to ensure a comprehensive assessment. This approach included the following activities:

- Review of IT policies, procedures, and standards.
- Interviews with IT management and personnel.
- Review of collected evidence and testing of relevant IT operations and processes.
- Use of commercial security tools and manual testing techniques.

The review was limited to the areas we considered necessary to complete the assessment and was not intended to cover the Village of ABC's entire information systems function.

Finding Legend:



Urgent-Risk (Level 5) Immediate remediation required.	*Note: If finding is a technical vulnerability, it provides remote intruders with remote root or remote administrator capabilities.*
Critical-Risk (Level 4) Immediate action recommended with remediation ASAP.	*Note: If finding is a technical vulnerability, it provides intruders with remote user, but not remote administrator or root user, capabilities.*
High-Risk (Level 3) Immediate action recommended with remediation in 90 days.	*Note: If finding is a technical vulnerability, it provides hackers with access to specific information, including security settings, stored on the host. This level of vulnerability could result in potential misuse of the host by intruders.*
Medium-Risk (Level 2) Action recommended with remediation in 180 days.	*Note: If finding is a technical vulnerability, it may expose some sensitive information, such as precise versions of services, from the host. With this information, hackers could research potential attacks to try against a host.*
Low-Risk | Informational (Level 1) Effective control.	*No immediate changes recommended. Opportunity for slight improvement.*
Advisory Comment	*Action suggested at the discretion of management.*

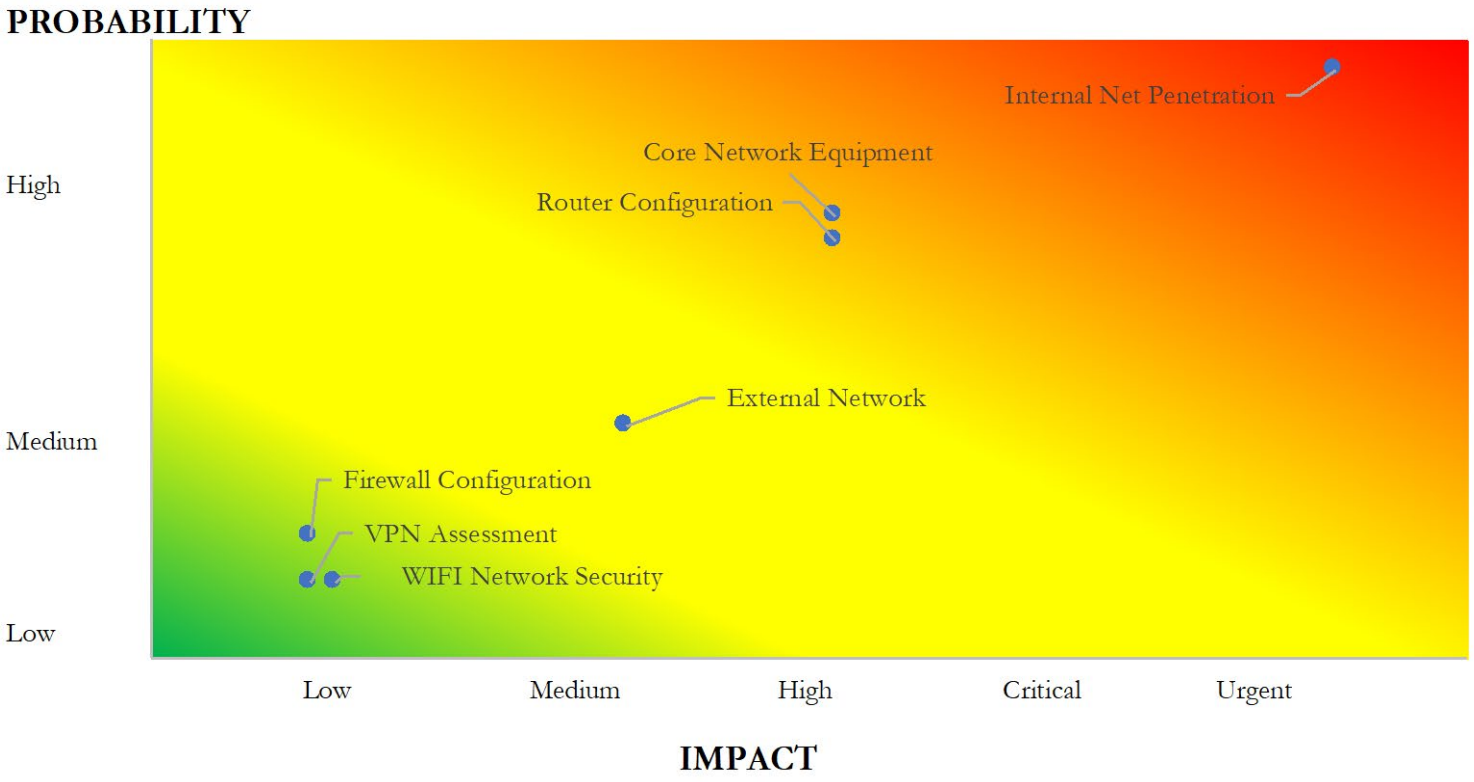
Summary of Findings

The following section provides a summary of our findings from the cybersecurity assessment.

No.	Finding Title	5	4	3	2	1	0
1	Internal Network Vulnerability Assessment and Penetration Test	✓					
2	Router/Switch Configuration Analysis			✓			
3	Core Network Equipment Review			✓			
4	External Network Vulnerability Assessment				✓		
5	Wireless Network Assessment					✓	
6	Firewall Configuration Analysis					✓	
7	VPN Assessment					✓	
8	Firewall Optimization						✓
9	External Network Public Information						✓
	Total Findings:	1	0	2	1	3	2

Remainder of page left blank intentionally.

CYBERSECURITY ASSESSMENT HEAT MAP



No. 1: Internal Network Vulnerability Assessment and Penetration Test – we scanned the Village of ABC's internal network and identified 26 critical-, 15 high-, and 35 medium-priority unique vulnerabilities. The scan results revealed vulnerabilities that increase the likelihood of an internal network breach. We also performed exploit testing and successfully breached the internal network. While we identified no urgent vulnerabilities, given the success at exploiting critical vulnerabilities, we have elevated to overall network security posture to urgent.

However, we note that there are several critical vulnerabilities associated with the same technology. Addressing the vulnerability with the technology will in fact address many of the vulnerabilities.

No. 2: Router/Switch Configuration Analysis – we performed a detailed configuration analysis of 10 routers/switches. Based on our analysis, firmware needs to be updated, and there are opportunities to harden the configurations.

No. 3: Core Network Equipment Review – we reviewed the duration of manufacturer support, and the impact end-of-support equipment may have on Village of ABC's overall security posture. Based on our analysis, we believe that the Village of ABC's core network equipment that has not been, or is not being, replaced is at a high risk of being compromised by an attacker. We did note that the Village of ABC is replacing Cisco routers and switches that are nearing or have exceeded their end of sale and end of software maintenance dates with late model Fortinet devices.

No. 4: External Network Vulnerability Assessment – we scanned the Village of ABC's external network and identified one critical-, one high-, and five medium-priority unique vulnerabilities. The scan results revealed vulnerabilities that increase the likelihood of an external network breach. We did not attempt to exploit any of the vulnerabilities.

Conclusion

Based on the procedures we performed, our knowledge of the Village of ABC's computing environment, and our IT security experience, it is our opinion that opportunities exist to improve the Village of ABC's IT security and internal controls. However, we also recognize that the Village of ABC's IT management understands the importance of, and strives for, security and control across the computing environment.

We recommend that the Village of ABC review and implement our recommendations to improve security and process controls. The remainder of this report provides a detailed analysis of our approach and methodology, the risks and vulnerabilities we identified, and detailed mitigation recommendations.

Remainder of page left blank intentionally.

CYBERSECURITY ASSESSMENT

The objective of the review was to assess the Village of ABC's IT processes and identify vulnerabilities in select technologies.
The scope of the review included the following:

1. External network subnets XXX.XX.XX.XXX/XX and XXX.XX.XX.XXX/XX.

2. Internal network subnets, including:
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XX.XX.XX.XXX/XX
   - XXX.X.XX.XXX/XX
   - XXX.X.XX.XXX/XX
   - XXX.X.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.X.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/X
   - XXX.XX.XX.XXX/X
   - XXX.XX.XX.XXX/X
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.X.XX.XXX/XX
   - XX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XX/XX
   - XXX.XX.XX.XX/XX
   - XXX.XX.XX.XX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/X
   - XXX.XX.XX.XXX/X
   - XXX.XX.XX.XXX/X
   - XXX.XX.XX.XX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.X.XX.XXX/XX
   - XXX.X.XX.XXX/XX
   - XXX.X.XX.XXX/XX
   - XXX.XX.XX.XXX/X
   - XX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.X.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.XX.XX.XXX/XX
   - XXX.X.XX.XXX/XX
   - XXX.XX.XX.XXX/XX

3. Wireless network (Ruckus VSZ-E wireless controller)

4. Configuration analysis of the following Fortigate firewalls:
   - FortiGate-40F (hostname: XX)
   - FortiGate-601E (hostname: XX)
   - FortiGate-70F (XX)

5. Configuration analysis of the following Cisco Catalyst routers/switches, by hostname:
   - XX
   - XX
   - XX
   - XX
   - XX
   - XX
   - XX
   - XX
   - XX
   - XX

6. Internet access review – review of the security posture of the virtual private network (VPN) controller.

7. Network equipment review – review of a listing of IT assets.

APPROACH AND METHODOLOGY

To achieve the Village of ABC's objectives, we relied on our proven assessment methodologies, summarized below:

EXTERNAL AND INTERNAL NETWORK TESTING

We used discovery, vulnerability assessment, and penetration testing procedures, listed below, to identify weaknesses in IP network services:

- Internet Discovery – using public tools, manual tasks, publicly available information, and information from the Village of ABC's IT management, we created a profile of computer addresses and other information about the Village of ABC's external and internal networks.
- External and Internal Network IP Scans – using Nmap and Nessus Professional vulnerability scanner, we scanned the approved ranges of external and internal IP addresses. We configured scanning policies that minimized disruption to the Village of ABC's external and internal network systems and devices. This included disabling denial of service and brute force attack attempts.
- False Positive Identification – we analyzed the results and, based on our knowledge and information from the scans, attempted to identify and remove all false-positive vulnerabilities.
- Penetration Testing – we attempted to exploit select vulnerabilities on the internal network and gain access to system resources.

WIRELESS NETWORK TESTING

We used commercial wireless system scanners, including KisMAC and Air Magnet, to assess the wireless network. Our procedures included, but were not limited to, the following:

- Wireless Discovery – we created a profile of available wireless networks and determined each network's service set identifier (SSID) and level of encryption.
- Architectural Assessment – we gained an understanding of the wireless architecture and the process of administering the wireless network.
- Attempted to Gain Access – after identifying the wireless networks, we tried to access each one by obtaining a username and password from a connected user without his knowledge.

FIREWALLS/ROUTERS/SWITCHES

We used Firewall Analyzer and Nipper Studio to perform a line-by-line analysis of each firewall, router, and switch configuration file.

IT PROCESS RISK ASSESSMENT

During this phase, our procedures included:

- Review of IT policies, procedures, and standards.
- Interviews with the Village of ABC's IT process owners.
- Review of supporting assessment evidence and artifacts.

The review was limited to the areas we considered necessary to complete the assessment and was not intended to cover the Village of ABC's entire information systems function.

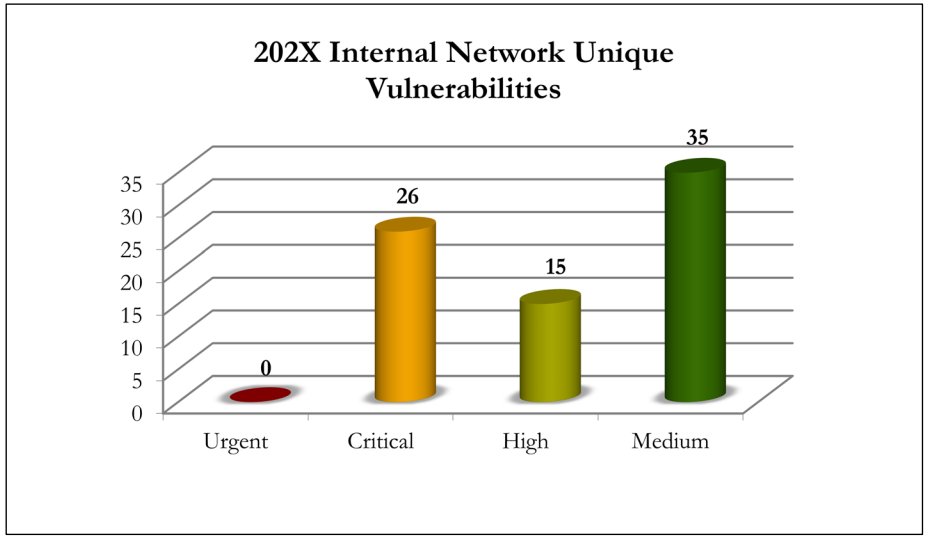
FINDINGS AND RECOMMENDATIONS

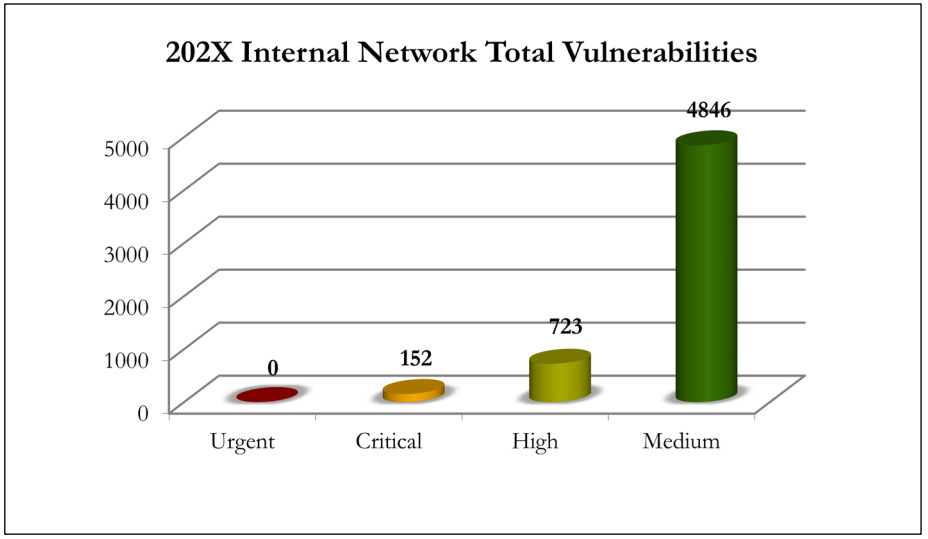
The following recommendations, based on our cybersecurity assessment and technical testing, are intended to improve the security and control of the Village of ABC's IT environment.

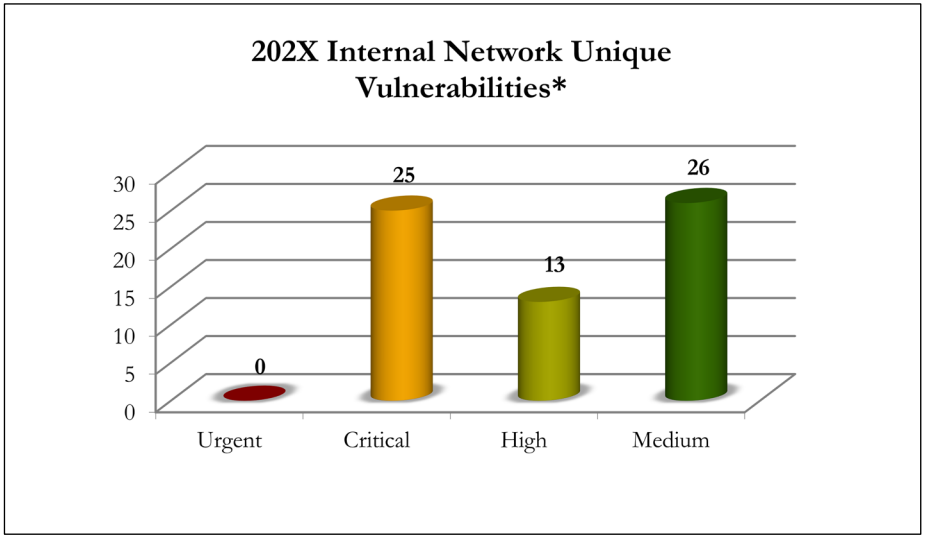
No. 1: Internal Network Vulnerability Assessment and Penetration Test

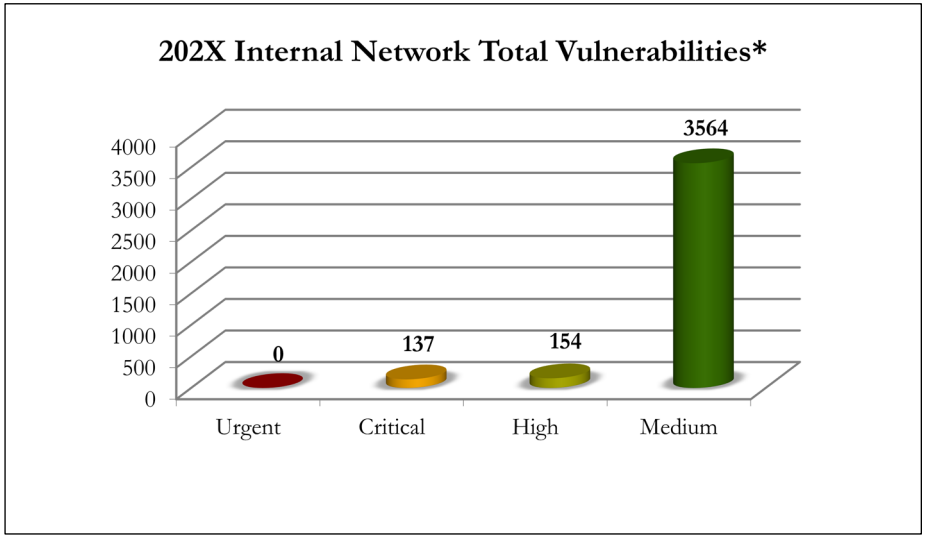
We scanned the Village of ABC's internal network and identified 26 critical-, 15 high-, and 35 medium-priority unique vulnerabilities. The scan results revealed vulnerabilities that increase the likelihood of an internal network breach.

The charts below show the vulnerabilities we identified, prioritized by level of severity, as defined by the Common Vulnerability Scoring System, Version 3.0 (CVSS v3.0). The technician's report summarizes the unique vulnerabilities, affected systems, and recommended solutions. In many cases, the recommended solution requires a system security patch.









*Excluding SSL and TLS vulnerabilities.

Securance analyzed the results of the internal vulnerability assessment to determine an effective penetration testing plan. We identified several hosts and systems to target during the penetration test. We presented the results to the Village of ABC's IT management, which assessed the list and approved penetration testing of the following systems.

HOSTNAME | IP	VULNERABILITY SUMMARY	EXPLOIT RESULTS
• XXX.X.XX.XXX	iLO 4 < 2.53 Remote Code Execution Vulnerability	**Success:** Created new user. Account: jaTxgVMi/ EKfrOjpgxYTT.
• XXX.X.XX.XXX • XXX.X.XX.XXX	Microsoft RDP RCE	Exploit completed, but no session created on any host.
• XXX.X.XX.XXX • XXX.X.XX.XXX • XXX.X.XX.XXX	NFS Exported Share Information Disclosure	**Success:** Mounted new directory on all hosts.

No. 1: Internal Network Penetration Test continued

HOSTNAME | IP	VULNERABILITY SUMMARY	EXPLOIT RESULTS
• XXX.X.XX.XXX	Apache Solr <8.4.0 Remote Code Execution	**Success**: Gained shell and elevated privileges to administrator.
• XXX.X.XX.XXX	OpenSSL Heartbeat Information Disclosure	**Success:** Captured private key.
• XXX.X.XX.XXX • XXX.X.XX.XXX • XXX.X.XX.XXX • XXX.X.XX.XXX • XXX.X.XX.XXX	SMB Signing Not Required	**Success**: Obtained 40 usernames and password hashes; all hosts produced results.

While our exploits targeting the six hosts listed above were not fully successful, it is worth noting the following:

- We proposed targeting 29 hosts and received approval to perform exploit testing against 13 hosts.
- We identified 40 hosts with 20 unique critical vulnerabilities and 154 hosts with 15 unique high vulnerabilities.
- A bad actor would not request approval to attempt exploits, would have unlimited time to deploy advanced persistent threat techniques, and might experience success. The details of our penetration testing efforts are in the technician's report.

Potential Risk:

As a result of our testing, we believe that the Village of ABC's internal network is at an urgent risk of being compromised by an attacker. If a breach were to occur, depending on the type of breach, systems could be rendered unresponsive, and data could be compromised.

Recommendation:

We recommend that the Village of ABC's IT staff review the vulnerabilities identified and address the critical-, high-, and medium-priority vulnerabilities associated with systems that meet the following criteria:

- The system is maintained by the Village of ABC's IT staff.
- Applying the recommended patch will not disrupt the other technologies that the system supports.
- The system is neither a target for replacement nor a part of the legacy server plan.

Vulnerability details are provided in a separate technician's report. Low-risk vulnerabilities and informational disclosures are only provided in the technician's report. A finding and technical vulnerability legend is provided on page 5.

Remainder of page left blank intentionally.

No. 2: Router/Switch Configuration Analysis

We performed a detailed configuration analysis of the following routers/switches:

- XXX.X.XX.XXX
- XXX.X.XX.XXX
- XXX.X.XX.XXX
- XXX.X.XX.XXX
- XXX.X.XX.XXX
- XXX.X.XX.XXX
- XXX.X.XX.XXX
- XXX.X.XX.XXX
- XXX.X.XX.XXX
- XXX.X.XX.XXX

Appendix A (redacted) summarizes the risks we identified, prioritized by level of severity, as defined by CVSS v3.0. We further adjusted the risks based on our experience and knowledge of the Village of ABC's network architecture.

Potential Risk:

Our testing indicates that the Village of ABC's network is at a moderate to high risk of being compromised due to a weakness in a router/switch configuration. If the network is attacked, systems could be rendered unresponsive, data could be compromised, or segments of the network could be used to breach internal systems.

Recommendation:

We recommend that the Village of ABC's IT management review and implement the configuration settings noted in Appendix A (redacted) to support a secure computing environment. We also recommend continued vigilance, as new threats continually emerge.

No. 3: Core Network Equipment Review

We reviewed the list of ten routers and switches that the Village of ABC's IT management considers to be core equipment. The review assessed the duration of manufacturer support and the impact end-of-support equipment may have on the Village of ABC's overall security posture. The table below shows the status of manufacturer support for each router/switch.

HOST NAME	BRAND	DEVICE TYPE	MODEL	END OF SALE DATE	END OF SW MAINT	END OF VULNERABILITY/SECURITY SUPPORT	END OF HW SUPPORT	MANUF. REPLACEMENT
XX	Cisco	Switch	WS-C2960X-24TS-L	31-OCT-22	31-OCT-23	31-OCT-27	31-OCT-27	C9200L-24T-4G
XX	Cisco	Switch	WS-C2960X-24TS-L	31-OCT-22	31-OCT-23	31-OCT-27	31-OCT-27	C9200L-24T-4G
XX	Cisco	Router	ISR-4431/K9	7-NOV-23	31-AUG-25	30-NOV-28	30-NOV-28	C8200-1N-4T
XX	Cisco	Router	ISR-4431/K9	7-NOV-23	31-AUG-25	30-NOV-28	30-NOV-28	C8200-1N-4T
XX	Cisco	Router	ISR-4431/K9	7-NOV-23	31-AUG-25	30-NOV-28	30-NOV-28	C8200-1N-4T
XX	Cisco	Router	ISR-4431/K9	7-NOV-23	31-AUG-25	30-NOV-28	30-NOV-28	C8200-1N-4T
XX	Fortinet	Switch	FortiSwitch 448E-FPOE	Information not Published	Information not Published	Information not Published	Information not Published	Information not Published

XX	Fortinet	Switch	FortiSwitch 1024D	Information not Published	Information not Published	Information not Published	Information not Published	Information not Published
XX	Fortinet	Switch	FortiSwitch 448E	Information not Published	Information not Published	Information not Published	Information not Published	Information not Published
XX (SCADA)	Cisco	Router - Industrial	IR809	12JUL-21	12-JUL-22	11-JUL-24	31-JUL-26	IR1101-A-K9

No. 3: Core Network Equipment Review continued

As a result of our review, we believe that the Village of ABC's core network equipment that has not been, or is not being, replaced is at a high risk of being compromised by an attacker. We noted that the Village of ABC is replacing Cisco routers and switches that are nearing or have exceeded their end-of-sale and end-of-software maintenance dates with late model Fortinet devices. The Fortinet equipment models being procured are newer models, and the manufacturer has not published end-of-life dates.

Potential Risk:
If a breach were to occur due to a security configuration weakness or technical vulnerability in the network infrastructure (i.e., routers and switches), systems could be rendered unresponsive, data could be compromised, or segments of the network could be used to breach internal systems.

Recommendation:
We commend the Village of ABC's IT management for implementing a phased equipment replacement program and encourage them to proceed with the plan. With respect to network equipment that is not currently scheduled to be replaced, we recommend updating the firmware and adjusting the configurations as per Appendix A (redacted).

No. 4: External Network Vulnerability Assessment

We scanned the Village of ABC's external network and identified one critical-, one high-, and five medium-priority unique vulnerabilities. The scan results revealed vulnerabilities that increase the likelihood of an external network breach. We did not attempt to exploit any of the vulnerabilities.

The charts on the following page show the vulnerabilities we identified, prioritized by level of severity, as defined by CVSS v3.0. Refer to the technician's report for the details of the unique vulnerabilities, affected systems, and recommended solutions. In several cases, the recommended solution requires a system security patch.

Potential Risk:

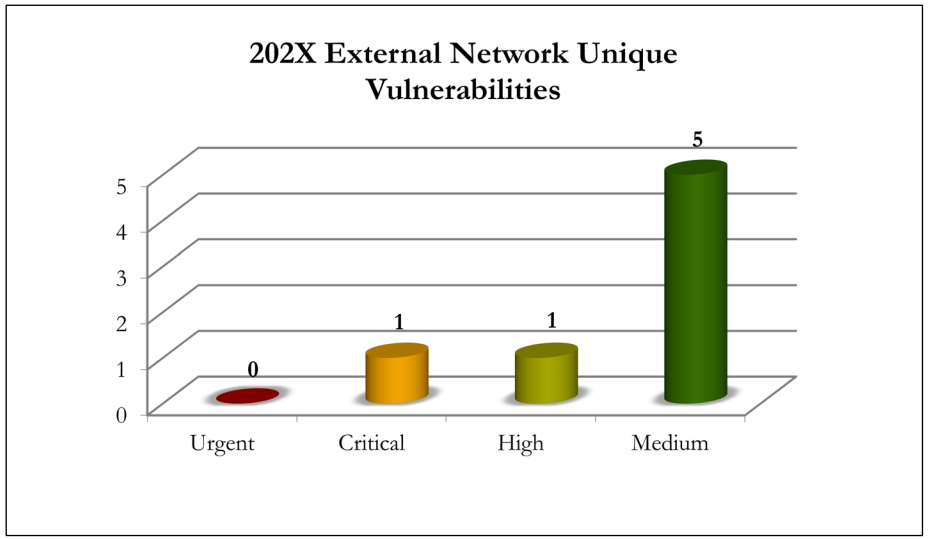
As a result of our testing, we believe that the Village of ABC's external network is at a moderate risk of being compromised by an attacker. If a breach were to occur, depending on the type of breach, systems could be rendered unresponsive, data could be compromised, or segments of the network could be used to breach internal systems.

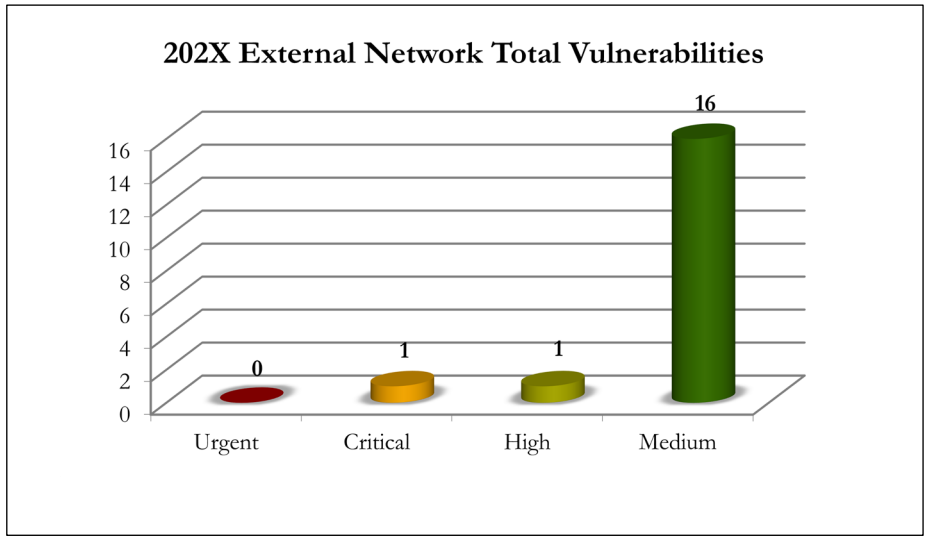
Recommendation:

We recommend that the Village of ABC's IT staff review the vulnerabilities identified and address the critical-, high-, and medium-priority vulnerabilities associated with systems that meet the following criteria:

- The system is maintained by the Village of ABC's IT staff.
- Applying the recommended patch will not disrupt the other technologies that the system supports.
- The system is neither a target for replacement nor a part of the legacy server plan.

Vulnerability details are provided in a separate technician's report. Low-risk vulnerabilities and informational disclosures are only provided in the technician's report. A finding and technical vulnerability legend is provided on page 5.





*Excluding SSL and TLS vulnerabilities.

No. 5: Wireless Network Assessment (Ruckus VSZ-E Controller)

During our site visit, we identified a cloud-based controller that authorizes access to the following SSIDs:

SSID	LEVEL OF ACCESS	INTERNET	INTERNAL NETWORK	ENCRYPTION/ SECURITY	USER AUTHENTICATION	DEVICE AUTHENTICATION
VoSPublic	Internet Only	✓		None	Captive Portal	No
VoSPrivate	Internet, File Server IAW AD	✓	✓	CCMP	WPA2-Enterprise 802.1x	No (Only Allows Windows devices)
WirelessIoT	Internet Only	✓		None	None	No
VoSMobile_ optout	Internet, GIS, CITIworks	✓	✓	CCMP	WPA2-Personal	No (Rejects Windows Devices)

As part of our review, we also noted the following:

- The wireless access point logs are not ported to a syslog or other centralized log server.
- Successful and unsuccessful connections to the wireless network are logged by the Ruckus controller but are not monitored or reviewed.
- We successfully captured four unique password hashes. However, none of the hashes were found in a 3.2-billion-word dictionary.

Potential Risk:

The wireless network is at a low to moderate risk of being used by an attacker or unauthorized user to compromise the Village of ABC's technologies. If a breach were to occur, the network could be rendered unresponsive, or an unauthorized user could access information resources.

Recommendation:

We recommend that the Village of ABC's IT management implement device authentication for devices accessing the internal network wirelessly and port access point logs to a syslog server.

No. 6: Firewall Configuration Analysis

We performed a detailed configuration analysis of three Fortigate firewalls and noted the following:

- Hostname: XX
  - URL filtering is enabled.
  - Connections are appropriately logged.
  - Intrusion protection policies are configured and implemented.
  - Anti-virus protection is configured and implemented.
  - Access control list (ACL) configurations are streamlined, and we did not identify any unnecessary risks.
- Hostname: XX
  - ACL configurations are streamlined, and we did not identify any unnecessary risks.
- Hostname: XX
  - ACL configurations are streamlined, and we did not identify any unnecessary risks.

Potential Risk:

Our assessment indicates that the Village of ABC's network is at a low risk of being compromised due to a security risk or exploitable weakness in one of its firewalls. If the network were attacked, depending on the type of attack and its level of success, systems could be rendered unresponsive, and data could be compromised.

Recommendation:

We commend the Village of ABC's IT management for streamlined firewall configurations. However, we recommend that IT management subscribe to SSL inspection services.

No. 7: VPN Assessment

We reviewed and assessed the security and configuration of the VPN solution used to manage remote access to the Village of ABC's network, and noted the following:

- The VPN technology is a module within the firewalls.
- VPN administrator access is limited to appropriate personnel.
- Employees are granted VPN access by default.
- Vendors are not required to acknowledge and sign the Computer Security Policy before obtaining VPN access.
- Vendors are not required to have a Village of ABC sponsor to obtain VPN access.
- Vendor accounts are set to expire after defined time periods.
- Vendors are given access only to technologies that are necessary, not to the entire network.
- Multi-factor authentication (MFA) is not implemented.

VPN access appears appropriate and effectively managed.

Potential Risk:

The absence of an evidence-based user provisioning process for remote network access increases the risk of unauthorized or unwarranted access to the organization's systems, resources, and data. Depending on the level of access and the technical capability of the individual, a VPN account could be used to inappropriately access an application and/or data.

Recommendation:

We commend the Village of ABC's IT management for effectively managing remote user access. We recommend that the Village of ABC implement MFA for VPN accounts and continue engaging third parties to periodically review the remote access process.

No. 8: Firewall Optimization

Through a detailed review of the Internet-facing firewalls, we identified opportunities to improve and streamline their configurations.

FIREWALL	XX	XX	XX
• Rules	12	14	739
• Services	250	248	380
• Host Groups	107	110	1674
• Covered Rules	2	0	19
• Redundant Rules	0	0	53
• Consolidate Rules	0	0	55
• Rules No Remarks	2	13	593
• Unattached Objects	58	116	118
• Duplicate Objects	10	5	38

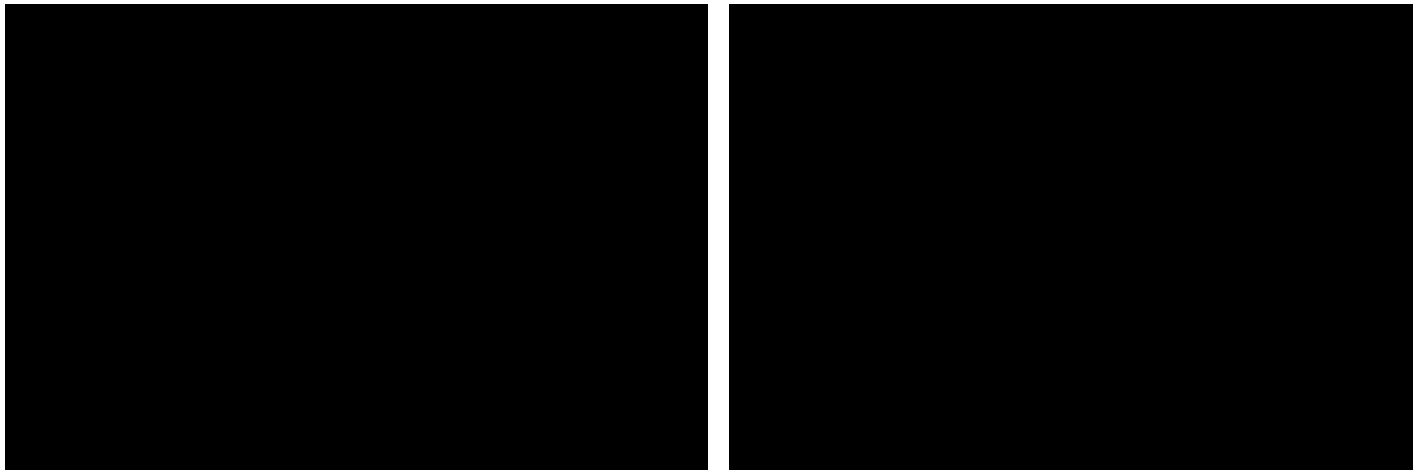
Recommendation:

These items represent housekeeping tasks that should be performed to maintain clean systems. Allowing these items to remain provides opportunities for network breaches, confusion, and/or potentially excessive access.

No. 9: External Network Public Information

We searched for publicly available information about the Village of ABC's Internet-facing (external) network and found that the American Registry for Internet Numbers (ARIN) identifies subnet XXX.XX.XXXX/XX as registered to the Village of ABC. Subnet XXX.XX.XX.XXX/XX is registered to XYZ Corporation.

The registry information for subnet XXX.XX.XX.XXX/XX is not appropriately sanitized to minimize unnecessary sharing of information, such as names and email addresses.



We also searched the "surface web," social media sites (Glassdoor, Facebook, Instagram, YouTube, Twitter, and LinkedIn), and the "dark web" (i.e., .onion), using the TOR browser and multiple sites (ahmia.fi, The Hidden Wiki, TORCH, and Candle), but did not find additional information about the Village of ABC's Internet-facing network.

Potential Risk:

Public information about an organization's Internet-facing network is both unnecessary and an entry point for attackers.

No. 9: External Network Public Information continued

Recommendation:

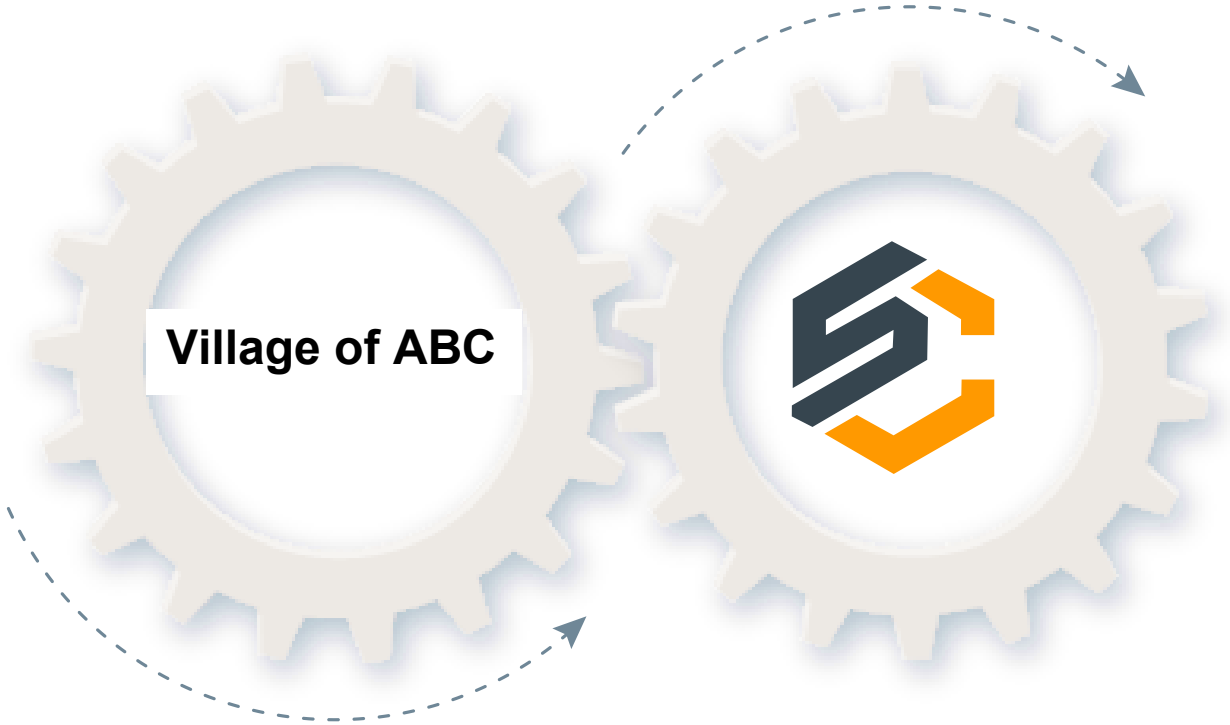
We recommend that the Village of ABC use the sanitization services offered by registrars. In addition, we recommend that the Village of ABC periodically review IP address registrations, the surface web, and the dark web to ensure all available information is properly sanitized.

Remainder of page left blank intentionally.

SECURANCE VALUE

Securance Consulting would like to THANK YOU for your business. Aside from benefiting from the highest level of service possible, you also received unique advantages that only Securance Consulting delivers. Our hands-on approach is tailored to fit the needs of the information technology department. Our technical expertise, outstanding reputation and personalized attention ensure you receive a level of service that no other cybersecurity firm can surpass.

As a Securance customer, you can be confident in your decision to manage technology risk by partnering with Securance!



13916 Monroes Business Park, Suite 102 • Tampa, FL 33635
www.securanceconsulting.com