



Click to listen



# SECURANCE CONSULTING RESPONSE TO RFP 2023-02-10 CYBER SECURITY ASSESSMENT

February 27, 2023



**Contact for RFP Response:**

**Ellen Anderson**

Government Contract and Proposal Manager  
eanderson@securanceconsulting.com

P: 877.578.0215 ext. 115



**SECURANCE  
CONSULTING**

*the advantage of insight*



[www.securanceconsulting.com](http://www.securanceconsulting.com)

February 27, 2023

Alvin Nepomuceno, IT Director  
Village of Oak Park  
123 Madison Street  
Oak Park, Illinois 60302

Dear Mr. Nepomuceno:

Thank you for considering Securance Consulting for Village of Oak Park's (Village's) upcoming Cyber Security Assessment. We will leverage our 21 years of security and compliance experience working with public sector clients, such as the City of St. Charles, the Village of Schaumburg, and Village of Niles, to ensure Village receives:

- ◆ A comprehensive cyber security assessment of its IT environment
- ◆ A thorough evaluation of its compliance with PCI, HIPAA, and CJIS requirements
- ◆ The benefit of our expertise in helping municipalities to reduce security risks, remediate technical vulnerabilities, and develop cyber security policies and incident response plans with NIST and CIS best practices

Securance will be an expert partner invested in Village's long-term cyber security and compliance.

Bad actors can strike at any moment, and Village is already at risk. It took Securance less than a minute to find sensitive information about Village on the dark web. In the wrong hands, this type of information could be the starting point of a cyber attack. Village needs a partner that can find security gaps like this one and determine their impact. Securance wants to be that partner.

**Email: [villagemanager@oak-park.us](mailto:villagemanager@oak-park.us)**  
**Hashed Password: \$2a\$08\$ywkpjh6cwEEZKVferqCa**  
**Sourced from dark web**

Thank you 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



# TABLE OF CONTENTS

---

REQUIREMENTS MATRIX .....	1
GENERAL DESCRIPTION .....	2
NARRATIVE.....	3
PROJECT MANAGEMENT OVERVIEW .....	25
EMPLOYEES.....	27
PROFESSIONAL REFERENCE LIST .....	31
ANNOTATED LISTING OF PUBLICATIONS, REPORTS, ETC. ....	35
PRICING.....	37
ORGANIZATION OF FIRM .....	41
COMPLIANCE AFFIDAVIT .....	43
M/W/DBE STATUS AND EEO REPORT.....	45

*This proposal contains confidential material proprietary to Securance Consulting. The material, ideas, and concepts contained herein are to be used solely and exclusively to evaluate the capabilities of Securance Consulting to provide assistance to Village of Oak Park (Village). This proposal does not constitute an agreement between Securance Consulting and Village. Any services Securance Consulting may provide to Village will be governed by the terms of a separate written agreement signed by both parties. All offers to provide professional services are valid for ninety (90) days.*

# REQUIREMENTS MATRIX

Securance has formatted our proposal in conjunction with Village’s requirements. Below, we summarize the contents of our proposal:

Title   RFP Section	Requirement	Page No.
V.	All firms interested in providing the deliverables outlined in this RFP must provide detailed responses for each of the questions listed below. Be sure to indicate next to your response the question that is being answered. If the answer is contained within any attached marketing material, please indicate precisely where the response to the particular question is located.	Each question is paired to a section
V.	General Description	<a href="#">2</a>
V.	Narrative	<a href="#">3</a>
V.	Overview	<a href="#">25</a>
V.	Employees	<a href="#">27</a>
V.	Professional Reference List	<a href="#">31</a>
V.	Annotated Listing of Publications, Reports, etc.	<a href="#">35</a>
V.	Pricing	<a href="#">37</a>
VII.	Organization of Firm	<a href="#">41</a>
IX.	Compliance Affidavit	<a href="#">43</a>
X.	M/W/DBE Status and EEO Report	<a href="#">45</a>

# GENERAL DESCRIPTION

A general description of the firm and the history of the firm, including a description of the firm’s experience and ability to provide the services requested. Include the number of years the company has been in business, the location of the corporate headquarters, and the total number of people employed by the company.

## Two Decades of Cybersecurity and Regulatory Compliance Services

Since our inception 21 years ago, Securance has performed more than 2,000 cyber security and regulatory compliance assessments for clients in nearly every industry, including hundreds of local, county, and state government entities.

Our corporate headquarters is located in Tampa Florida, and we currently employ 15 full-time employees and an additional 32 W-2 consultants located across the country.

Securance is a 100-percent minority-owned limited liability company, certified as an 8(a), Small Disadvantaged Business (SDB), and Minority Business Enterprise (MBE).

## Exclusively Staffed with Senior-Level IT Security Professionals

In order to provide the highest quality services, Securance only hires IT consultants with more than 15 years of professional experience. Their expertise in a wide array of assessments, compliance standards, and industry needs is our foundation, allowing us to perform each project we undertake to the unique specifications required by our clients’ specific IT environments, security and control standards, and business objectives.

Please find resumes for the staff proposed for Village’s engagement on pages 25–28.

*The City of Milwaukee has had the pleasure of working with Securance Consulting several times over the past two years and has found the firm professional, responsive and incredibly knowledgeable in governmental IT risk.*

— Isaak Lerner, CISA, SICCIP, CISM  
City of Milwaukee .

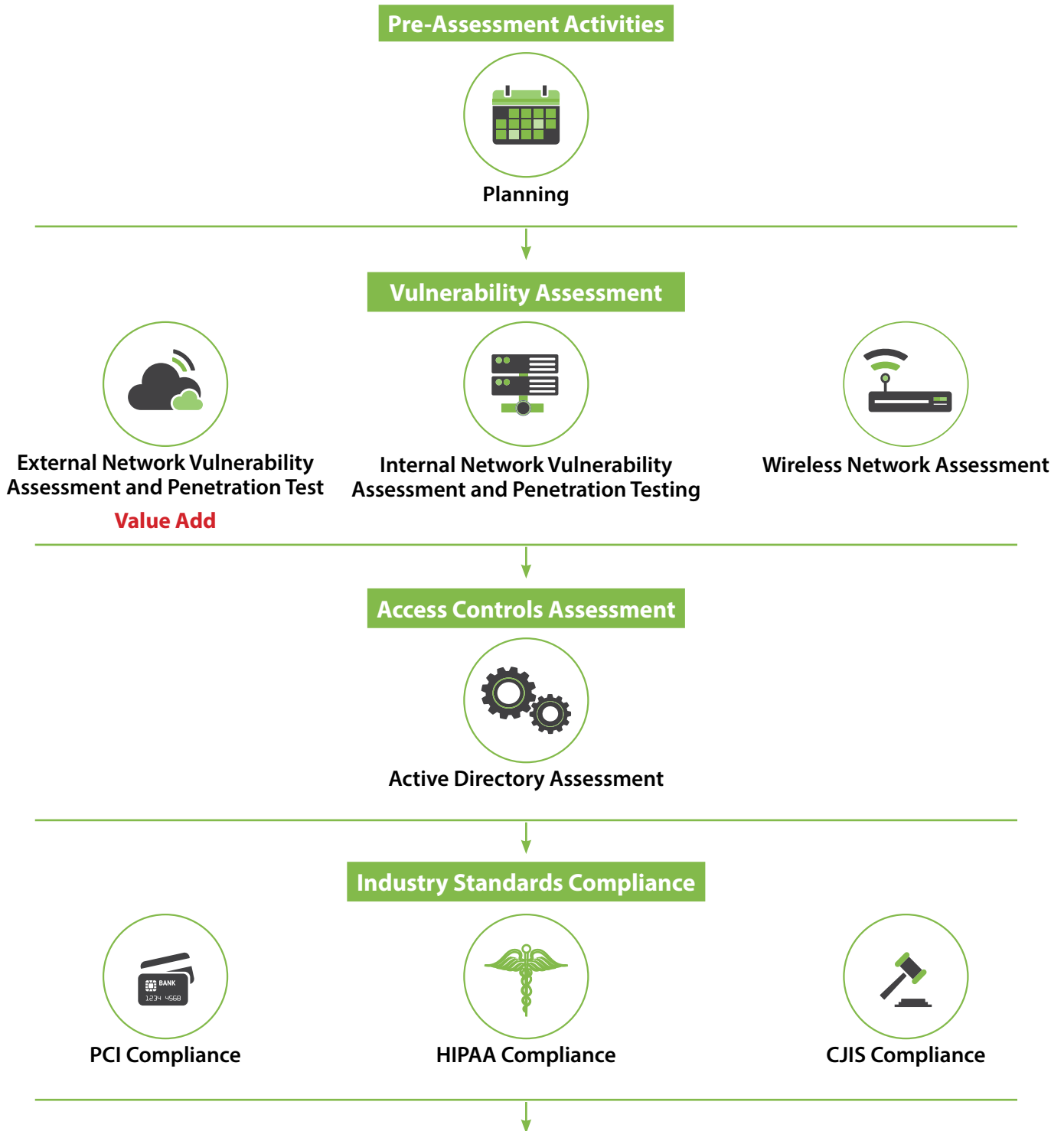
## THE SECURANCE DIFFERENCE



# NARRATIVE

Narrative: In the proposal for each scope of work item, a narrative should be provided on the vendor's approach to the project and a list of what assessment and mitigation recommendation will be provided.

Below, we summarize our understanding of Village's objectives and expectations for this project. Following this, we include technical methodologies for the proposed work.



## Narrative (continued)



## Narrative (continued)



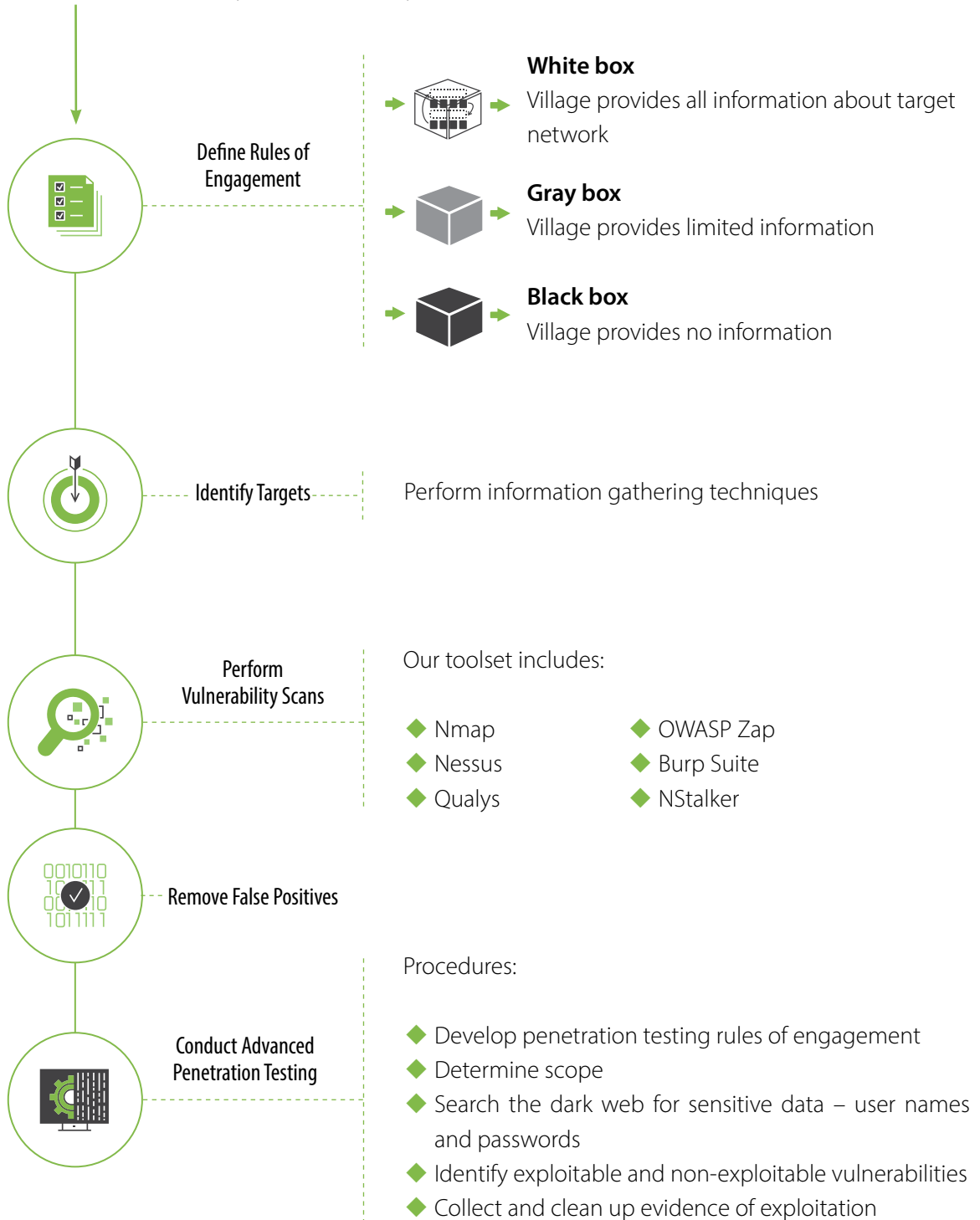


## Narrative

### External and Internal Network Vulnerability Assessment and Penetration Test

Our External and Internal Network Vulnerability Assessment is aligned with industry-leading frameworks, such as NIST SP 800-115, ISSAF, OSSTMM, and OWASP.

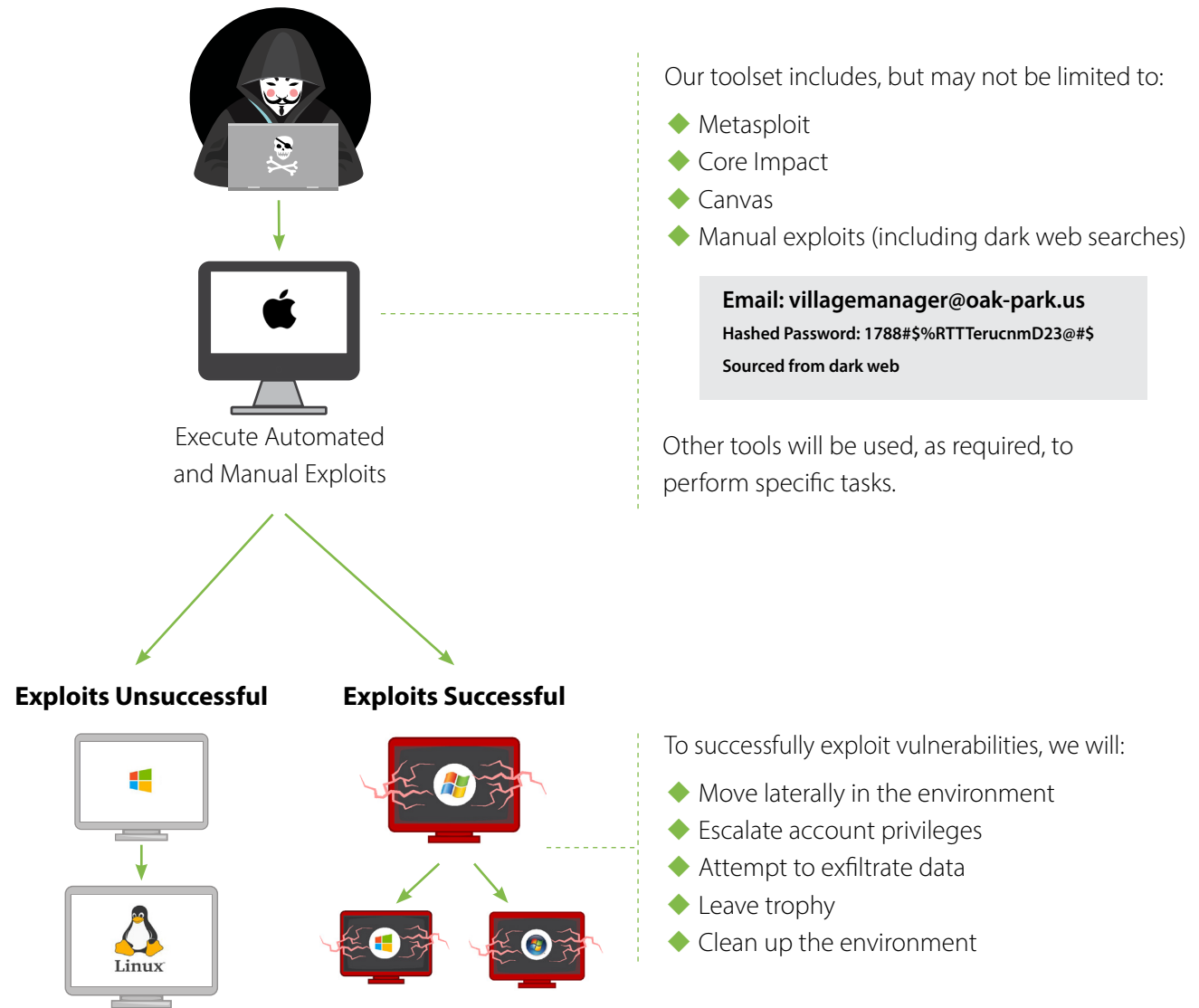
#### Securance communicates every step of the way



## Narrative

### External and Internal Network Vulnerability Assessment and Penetration Test (continued)

#### Securance's Ethical Penetration Testing Process



Securance will conduct the external network vulnerability assessment and penetration test as a value add

*The Maryland National Capital Park and Planning Commission (M-NCPPC) would like to thank you and your organization for the professionalism and completeness of our recent engagement in which you performed our annual Network Vulnerability and General Controls Review. The final report, extensive debrief and technical notes will ensure that the Commission's Desktops, Servers, LAN, Internet, Policies and Active Directory are configured and supported in a manner that will prevent loss of service or function due to neglect or misconfiguration.*

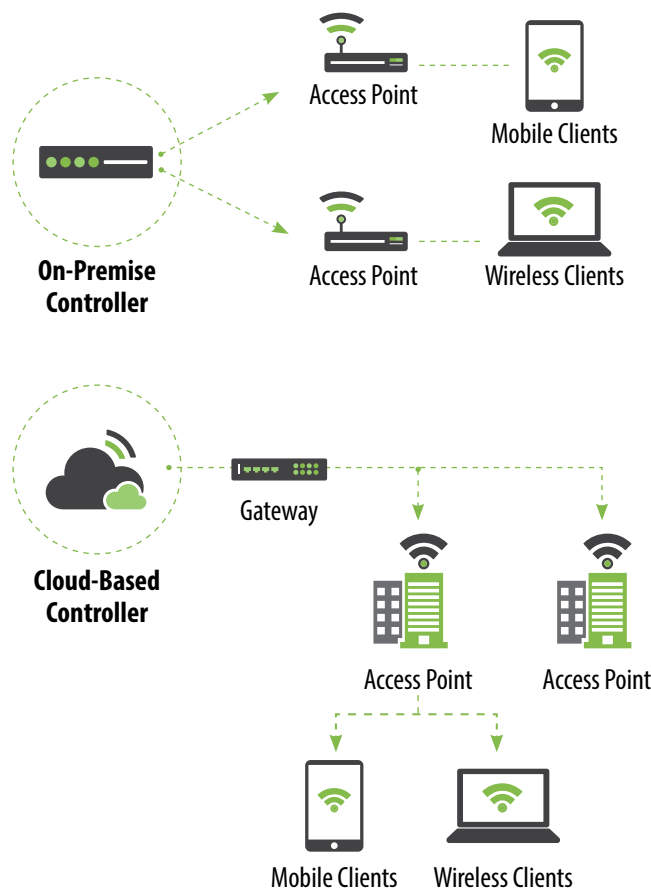
— Joe Bistany  
Maryland National Capital Park and Planning Commission

## Narrative

### Wireless Network Assessment

Securance assesses the configuration and security of both controller and access point-based wireless networks.

#### Controller-Based Wireless Networks



- ◆ Assess controller configurations
- ◆ Evaluate rogue access point detection and management
- ◆ Uncover or identify hidden SSIDs
- ◆ Assess encryption strength
- ◆ Review network segmentation
- ◆ Review administrative access controls and logging
- ◆ Confirm access points can only receive configurations from the controller

We will evaluate cloud-based WiFi networks to the extent allowed by the cloud provider for the controls listed above.

## Narrative

### Wireless Network 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:



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 on the network to access and gain control of the domain controller(s)
- ◆ Exfiltrate data from host machines
- ◆ Hide evidence of our breach

#### Potential Tools Used

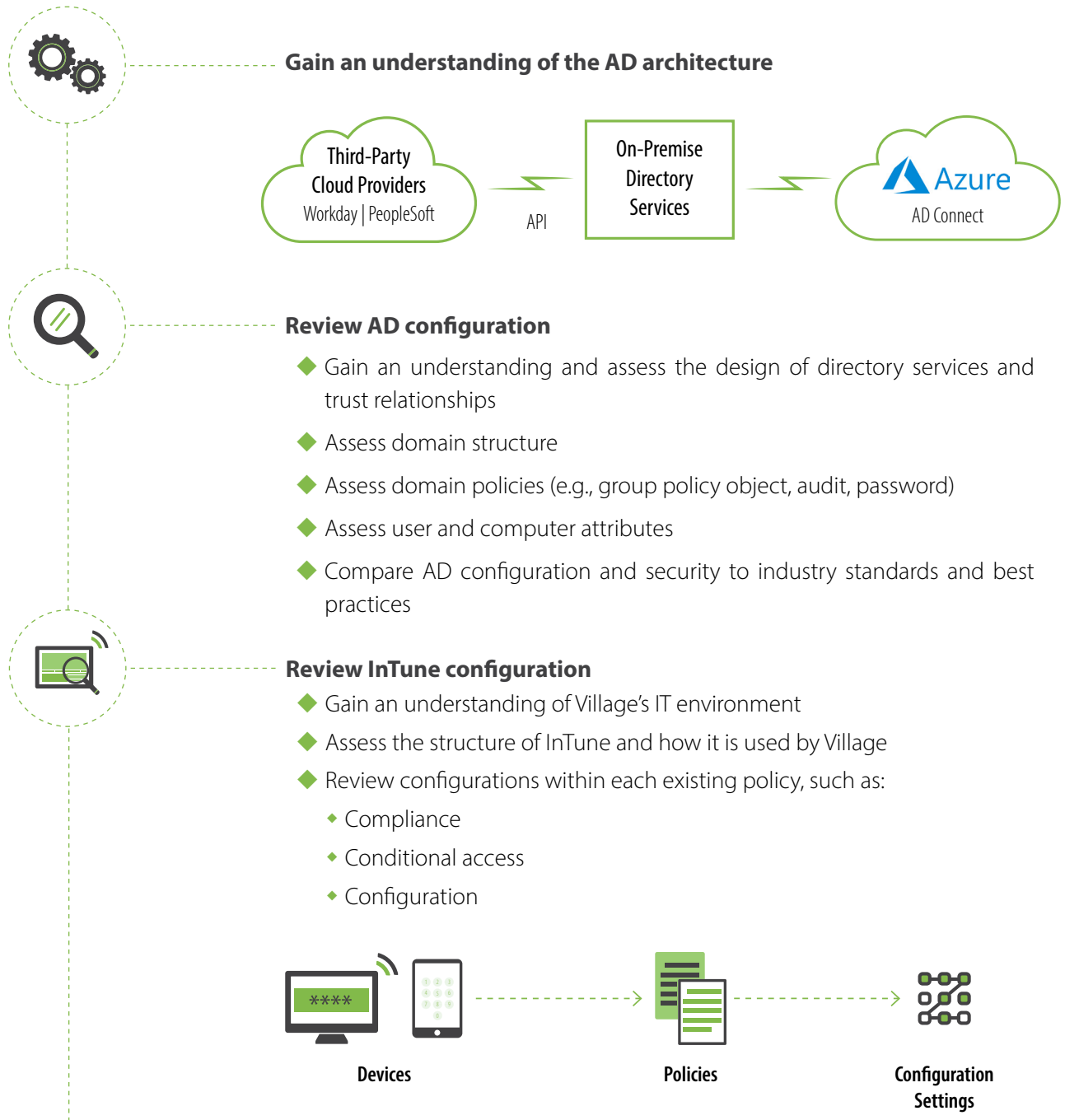
Vistumbler	Ncrack	Mimikatz
iStumbler	Hashcat	Wireshark
Kismet	John the Ripper	Advanced IP Scanner
Aircrack-ng suite	Online rainbow tables	
Besside-ng	Cain and Abel	

## Narrative

### Active Directory Assessment

Securance’s methodology for assessing the security of directory services, such as Active Directory (AD), is comprehensive and supports testing the entire architecture, users, and assets to decrease the likelihood of abuse and escalation attacks.

### Our Process



## Narrative

### Active Directory Assessment



#### Perform application programming interface (API) technical testing



Perform manual and automated testing, including a review of API integration. Our primary tools will be OWASP ZAP and Burp Suite Pro.



Test each API for vulnerabilities in the following attack categories:

- ◆ Authentication
- ◆ Authorization
- ◆ Client-side threats
- ◆ Cryptography  
| encryption strength
- ◆ Deployment  
management
- ◆ Error handling
- ◆ Identity management
- ◆ Input validation
- ◆ Injection vulnerability
- ◆ Logic and business flow
- ◆ Session management

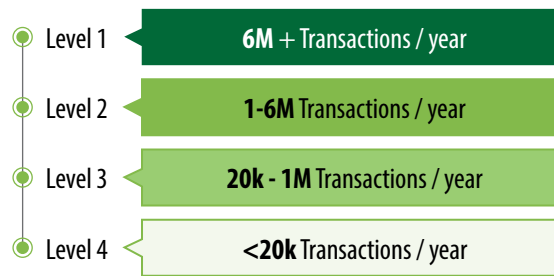
## Narrative

### PCI Compliance Review

The Securance methodology for helping organizations achieve PCI compliance follows the standards dictated by the PCI Security Standards Council (SSC) and includes the following activities:

- ◆ Perform a data flow analysis:
  - ◆ Identify devices, systems, applications, and databases that store, process, or transmit cardholder data
    - ◆ Ensure all components are documented
  - ◆ Evaluate system for segmentation opportunities
  - ◆ Define the in-scope environment for gap analysis
- ◆ Confirm Village’s merchant-level compliance requirements, based on the volume of credit card transactions processed annually:

#### PCI DSS COMPLIANCE LEVELS



- ◆ Perform a comprehensive gap analysis, encompassing all PCI DSS requirements:

#### PCI DSS REQUIREMENTS



## Narrative

### PCI Compliance Review (continued)

For each requirement, we will complete the following assessment procedures:

Requirement	Title	Securance Readiness Procedures				
		Policy Review	Interview	Technical Test	Administrative Test	Artifact Review
1	Install and maintain a firewall configuration to protect cardholder data	✓	✓	✓		
2	Do not use vendor-supplied defaults for system passwords and other security parameters	✓		✓	✓	✓
3	Protect stored cardholder data	✓	✓	✓	✓	✓
4	Encrypt transmission of cardholder data across open, public networks	✓		✓	✓	
5	Use and regularly update anti-virus software or programs	✓		✓	✓	
6	Develop and maintain secure systems and applications	✓	✓	✓	✓	✓
7	Restrict access to cardholder data by business need-to-know	✓	✓		✓	✓
8	Assign a unique ID to each person with computer access	✓	✓	✓	✓	✓
9	Restrict physical access to cardholder data	✓	✓		✓	
10	Track and monitor all access to network resources and cardholder data	✓	✓		✓	✓
11	Regularly test security systems and processes	✓	✓	✓	✓	
12	Maintain a policy that addresses information security for all personnel	✓	✓		✓	



## Narrative

### HIPAA Compliance Assessment: Security Rule

The Securance HIPAA Security Rule compliance assessment methodology includes a comprehensive analysis of the organization's adherence to all applicable Sections of the Rule, per §45 CFR. Our proven approach involves mapping your environment to the Security Rule's Sections and assessing your level of compliance following the OCR audit protocol.

We will ensure Village IT policies are mapped to the Security Rule and review:



#### Operational Compliance

- Interview IT staff relative to Security Rule requirements
- Obtain and review supporting evidence of compliance (e.g., access controls, audit control evidence)

#### Policies, Procedures, and Documentation

- Compliance with requirements of §45 CFR 164, Subparts A and C



#### Administrative Safeguards, such as:

- Assigned Security Responsibility
- Security Awareness and Training
- Contingency Plan



#### Organizational Requirements

- Compliance with:
  - Business Associate Contracts
  - Group Health Plans



#### Technical Safeguards, such as:

- Access Control
- Information Integrity
- Transmission Security



#### Physical Safeguards, such as:

- Facility Access Controls
- Workstation Use and Security
- Device and Media Controls

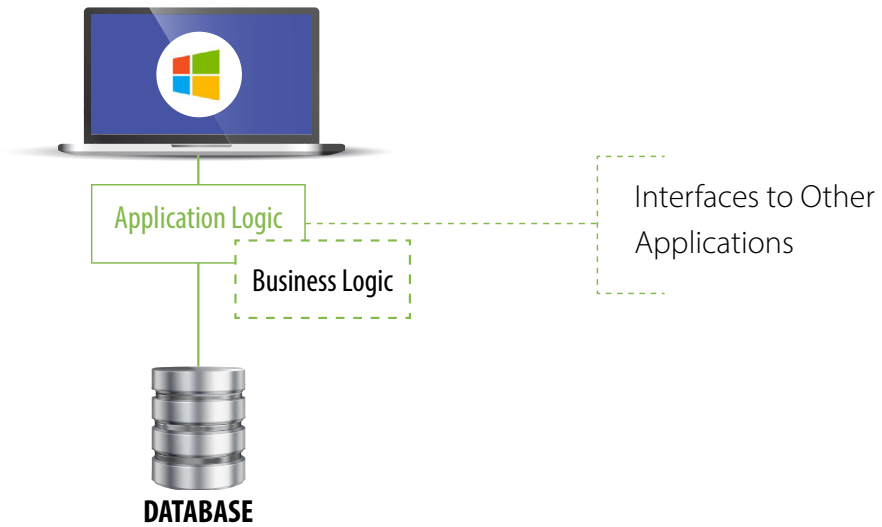


## Narrative

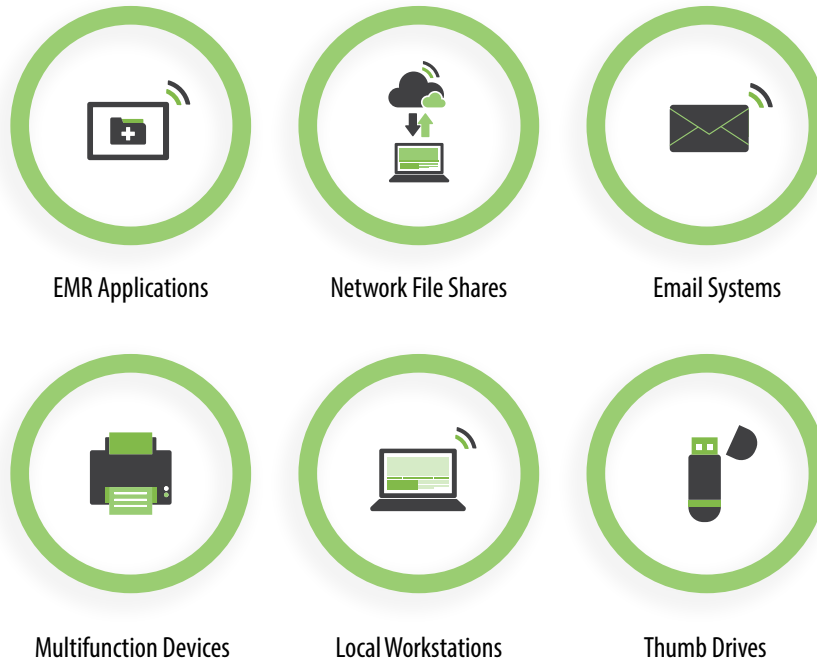
### HIPAA Compliance Assessment: Security Rule (continued)

#### ePHI Information Assets

Securance has experience assessing Tier 1 EMR applications. Our evaluation includes:



Securance identifies all areas where ePHI can live, including:



*With the wealth of knowledge and experience Securance Consulting has exemplified through its work at the County of Riverside, I highly recommend this firm's security consulting services to any organization, large and small, striving to achieve and maintain HIPAA security and privacy compliance.*

— Bob Cheong, CIO  
County of Riverside Information Security Office

## Narrative

### Social Engineering and Physical Security Assessment

Securance performs all methods of social engineering testing, including:

- ◆ Phishing →

Our methodology:

- ◆ Ensures there are effective controls over the human element of security
- ◆ Verifies the security of organizational resources and sensitive information
- ◆ Identifies weakness in user security awareness programs



The company appreciates your patience and dedication working from home in the COVID-19 environment. As a token of our appreciation, we are offering all employees discounts at local retail stores, including, but not limited to, those listed below. Thank you again for all your hard work!



To participate in these savings and have priority access to future offerings, please [click here](#) to register.

Securance's best practices white paper:  
[Unscammable: The Guide to Fostering a Culture of Security Awareness](#)



← Scan the code with your smartphone or tablet camera to read the white paper

**Securance will conduct a phishing campaign against 50 users as a value add**

## Narrative

### Physical Security Controls Review

Securance will ensure that your physical security controls protect information assets from environmental threats, human intruders, and the damage caused by supply system failures (i.e. loss of power, Internet, climate control, or any other infrastructure provider).

Our physical security review includes the following activities:



#### Information Gathering

- ◆ Review physical security policies and procedures
- ◆ Interview personnel responsible for physical security



#### Risk and Vulnerability Identification

- ◆ Perform a walkthrough of the facility | data center
- ◆ Review site selection, considering environmental risks and compliance requirements
- ◆ Evaluate physical and environmental security controls, including:
  - ◆ Access controls and perimeter defenses
  - ◆ Surveillance and monitoring mechanisms
  - ◆ Destruction and sanitization procedures for storage devices
  - ◆ Location of information systems components, wiring, and cabling
  - ◆ Incident management, reporting, and response procedures
  - ◆ Physical security awareness training



#### Analysis

- ◆ Compare physical security measures to best practices and regulations
- ◆ Identify risks, vulnerabilities, and opportunities for improvement

## Narrative

### Virtual Private Network (VPN) | Remote Access Assessment

VPNs ensure that the information being transmitted by devices is known only to authorized users. This data is secured by either IPSec or SSL encryption. IPSec connections are designed to have a pre-shared “key” on both the end-user’s device and server so that data can travel securely between both. SSL connections use public key cryptography that creates a secure connection after exchanging encryption keys. Each type of encryption suffers from vulnerabilities that make connections less secure.

### Our Process



## Narrative

### VPN | Remote Access Assessment (continued)



#### **Log Monitoring**

We will review the logs using manual and automated techniques to verify that:

- ◆ Logging for security events is enabled
- ◆ Logs are housed in a central location
- ◆ Sensitive information is not logged, e.g., passwords
- ◆ Logs are not altered
- ◆ Alerts are set up
- ◆ Logs are aggregated with other technology logs
- ◆ Logs are reviewed on a regular basis



#### **VPN Policy Ruleset Review**

We will evaluate County's access and policy ruleset to:

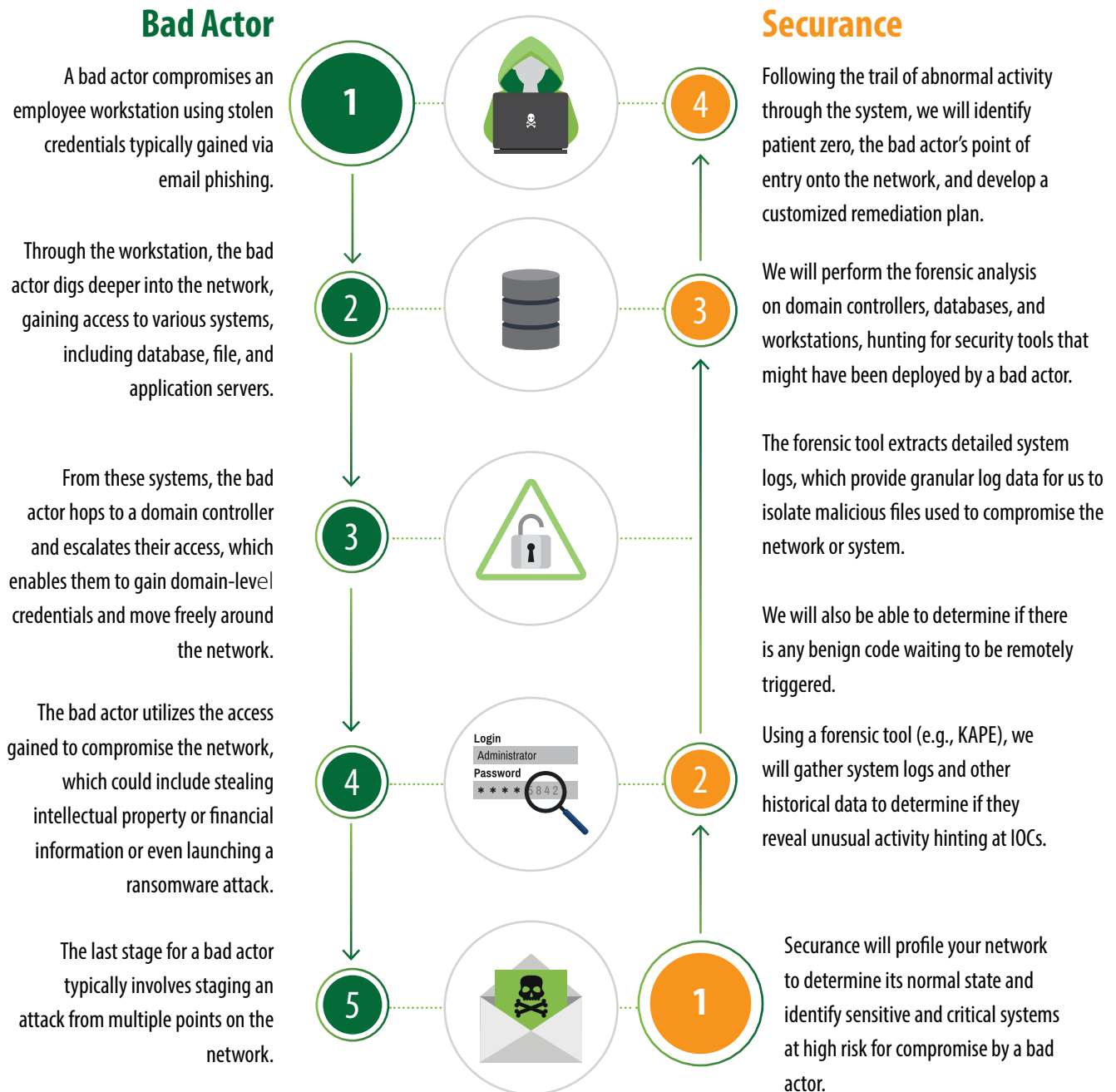
- ◆ Verify policies' cybersecurity strength
- ◆ Identify gaps and | or misconfigurations
- ◆ Ascertain if any policies are missing
- ◆ Identify extraneous policies
- ◆ Determine if authentication mechanisms are viable, strong, and appropriate
- ◆ Confirm that capacity and server | appliance load is appropriate | adequate

## Narrative

### Advanced Persistent Threat | Indicators of Compromise Assessment

Indicators of Compromise (IOCs) are digital evidence that indicate the potential presence of malicious activity, whether an attack has already occurred or will occur. Identifying IOCs informs an organization of network breaches and which security components must be strengthened to deter future incidents.

The below diagram depicts Securance’s comprehensive process for determining instances of network compromise and completing a forensic analysis to identify IOCs. We provide an example of how a bad actor might compromise an organization and how we work backward through the breach to determine the original compromised host, or patient zero.



Securance will conduct an APT | IOC assessment as a value add

## Narrative

### Incident Response Plan Development

Incident response plans (IRPs) help protect organizations from unexpected information security events, including data breaches, denial of service attacks, firewall breaches, outbreaks of viruses or malware, and even insider threats. Organizations should respond to security incidents with robust plans of action, in which roles and responsibilities, detection and eradication methods, and preventive measures are clearly defined.

The IRP we develop will:

- ◆ Document incident response procedures for the organization
- ◆ Ensure intelligent and agile organizational communication
- ◆ Facilitate quick recovery of affected core systems
- ◆ Pinpoint incident causes
- ◆ Establish preventive incident measures

### Our Process

Securance will develop a new IRP that includes the following required components:





## Narrative

### Incident Response Plan Development (continued)

#### Our Process (continued)



#### Preparation

Village's plan will include:

- ◆ Documented IR policies
- ◆ Clear communication guidelines
- ◆ Employee training
- ◆ Cyber hunting exercises
- ◆ Threat detection capability



#### Identification

- ◆ Monitor
- ◆ Detect -----> ◆ Attack vectors (NIST SP 800-61):
  - ◆ Impersonation | Spoofing
  - ◆ Improper Usage
  - ◆ Loss or Theft of Equipment
  - ◆ Other
- ◆ Alert
  - ◆ Unknown
- ◆ Report
  - ◆ Attrition
  - ◆ Web
  - ◆ Email/Phishing
  - ◆ External/Removable Media



#### Containment

Strategies for blocking breach spread



#### Eradication

Root cause removal procedures



#### Recovery



#### Lessons learned

Procedure set to leverage past experience

## Narrative

### Policy and Procedure Development

Our methodology for assessing | developing IT policies and procedures addresses all common components of an IT organization.

#### Securance:



**Defines** a policy as management’s intentions relative to mitigating a risk. Policies should be supported by detailed procedures that provide policy implementation guidance to IT engineers and administrators.



**Does not** support procedural language embedded in policy language, or policies for the sake of policies. We will understand Village’s organization and right-size each document to suit Village’s needs and IT environment specifically.

#### Our process includes:



Gaining an understanding of Village’s daily IT operations



Reviewing existing, or drafting new, policies that map to day-to-day operations

- ◆ Conducting IT process owner interviews
- ◆ Determining gaps in policies, procedures, and standards
- ◆ Drafting policies customized to Village’s IT environment
- ◆ Reviewing draft policies with IT process owners



Mapping policies to desired security and control frameworks

- ◆ Reviewing draft policies with IT process owners to ensure each policy maps to daily activities



Implementing new policies by training IT staff to adhere to them

## Narrative

### Policy and Procedure Development

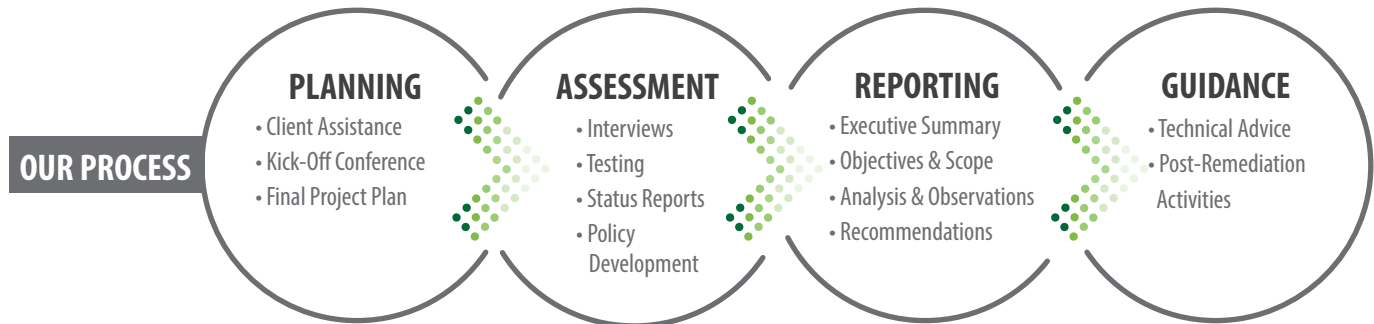
To ensure Village's policies and procedures are comprehensive, accurate, and effective, Securance will evaluate them for the criteria below or develop policies or procedures that contain these criteria.

Criteria	Definition
Overview	Summary of the need for the policy
Scope	Devices, data, documents, or systems covered under the policy
Purpose	Overall objective of the policy
Policy	A measure by which an organization conducts a process; may be aligned to a particular framework
Disciplinary Action	Defined actions the organization will take in the event of a failure to comply with the policy
Definitions	A table of definitions for terms used within the policy
Exceptions	Any circumstances under which the policy would not apply
Expected Impact	Projected outcome of maintaining and implementing the policy
Revision History	A table denoting when the policy was last updated and what areas were modified
Approval	Process for formally instating the policy and the party responsible for approval

# PROJECT MANAGEMENT OVERVIEW

a. Proposers shall describe the manner in which they would oversee the work, b. how they propose to communicate the project status to the Village, and c. how disputes or issues are addressed.

## a. Project Management Plan



Securance is dedicated to performing this engagement as efficiently as possible. Paul Ashe, your engagement manager, will be responsible for ensuring project success by facilitating regular communication and providing status reports that will track project progress, possible project risks, and other information pertinent to the project. Dispute resolution is detailed on the next page.



Ray, Chris, and Ibrahim, will work with Paul to:

- ◆ Plan, coordinate, and execute the assessments based on Village’s environment
- ◆ Identify risks, vulnerabilities, compliance gaps, and other opportunities for improvement
- ◆ Prepare assessment reports, draft policies, IRP, status reports, and other deliverables for review with Village’s PM
- ◆ Ensure he is notified of any project issues or delays

## Project Management Overview

### a. Project Management Plan (continued)

We anticipate that as part of the project, Village's project manager will:

- ◆ Ensure all client assistance requested items are provided in a timely manner and assist in scheduling Village staff for interviews with Securance
- ◆ Join project status meetings as necessary
- ◆ Review the cyber security assessment report to obtain a clear understanding of the findings and recommendations
- ◆ Provide Securance with feedback relative to the tone and format of the report

### b. Status Reports

For this project Securance will issue weekly status reports designed to capture and communicate the following information about an ongoing project:

- ◆ Budget to actual hours and projected hours to complete project
- ◆ Project issues or risks that may hinder project completion
- ◆ Change control items (typically only applicable if the scope changes)
- ◆ Project milestone status
- ◆ Upcoming activities
- ◆ Summary of any potential findings

### c. Dispute Resolution and Quality Control Procedures

We make client satisfaction our number-one priority and work hard to avoid complaints from our clients. If an issue arises, we address it prior to escalation. Our IT consultants will immediately advise the Securance engagement manager of any client complaints or other project issues. The engagement manager will then notify your PM and work with him | her to resolve any issues in a timely and mutually satisfactory manner.

In our experience, the most common roadblocks to successful project completion and client satisfaction are:

#### ◆ Disruption of network services

Securance takes measures to ensure that client networks, systems, and applications are not harmed or otherwise disrupted during the course of a security assessment. We do not perform brute force testing, denial-of-service attacks, or unproven experimental tests without explicit written permission from our client. We perform all security assessments according to leading standards (e.g., NIST standards) and best practices.

#### ◆ Disagreement over technical risk rankings

Our risk rankings are based on the Common Vulnerability Scoring Standards (CVSS), Version 3. However, when evaluating risks, we also take into account the likelihood and potential impact of an attack on our client's unique IT environment and the mitigating controls our client already has in place. We generate customized rankings and remediation recommendations that suit our clients' particular computing environments. As a result, our rankings are often lower than their CVSS counterparts.

#### ◆ Project delays due to delays in receipt of requested documentation

Securance will provide Village PM with weekly status reports. Each report will contain a section detailing open items and pending requests for information.

# EMPLOYEES

Describe which employees (name, title and expertise) will be working on this Project and their roles within the project



Paul has provided hands-on project management to lead Securance engagements over the past 21 years. A former IT consultant for Ernst & Young, Paul translates his knowledge and experience into an effective, time- and budget-conscious project management style. He conducts cybersecurity assessments, develops IT policies, assesses regulatory compliance, including PCI, HIPAA, and CJIS, and performs technology-specific vulnerability and penetration tests for clients in nearly every industry. He is an expert in incident response planning and business continuity.

## EDUCATION

### Master of Science

Accounting Information Systems

### Bachelor of Science

Accounting and Management Information Systems

## Paul Ashe 24 Years' Experience

President and Engagement Manager

Securance Consulting

### CERTIFICATIONS



(pending)

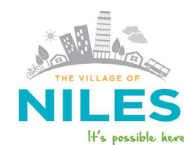


(pending)

### RELEVANT EXPERIENCE

- ◆ Active directory reviews
- ◆ APT testing
- ◆ CJIS compliance
- ◆ Cybersecurity program development
- ◆ Data loss prevention
- ◆ HIPAA compliance
- ◆ IT security policy development
- ◆ Network security
- ◆ NIST and CIS best practices
- ◆ PCI compliance
- ◆ Physical security controls reviews
- ◆ Remote access security
- ◆ Social engineering campaigns
- ◆ VPN and WAN security
- ◆ Wireless network assessments

### RELEVANT PROJECTS



VILLAGE OF SCHAUMBURG



## Employees



Chris is an expert in IT security and risk assessment and regulatory compliance, including HIPAA, CJIS, and PCI. With more than 34 years of IT experience, Chris' expertise in developing IT processes, evaluating network security, assessing and remediating potential threats, and identifying and resolving compliance issues has benefited numerous city, county, and state government entities.

### EDUCATION

#### Master of Science

Management Information Systems

#### Bachelor of Science

Computer Science for Business

## Chris Bunn 34 Years' Experience

Senior IT Security Consultant

Securance Consulting

### CERTIFICATIONS



### RELEVANT EXPERIENCE

- ◆ Cybersecurity assessments
- ◆ Cybersecurity program development
- ◆ Data loss prevention
- ◆ HIPAA and HITECH compliance
- ◆ IT security policy development
- ◆ Network security
- ◆ NIST | CIS alignment
- ◆ PCI compliance
- ◆ Physical security controls reviews
- ◆ Risk assessment and threat analysis
- ◆ Social engineering | user security awareness
- ◆ Wireless network assessments

### RELEVANT PROJECTS



## Employees



Ray, a retired Commander and Special Operations Officer for the U.S. Navy, specializes in analyzing organizational security needs, assessing existing security posture, and implementing plans to mitigate risks to an acceptable level. He is an expert in the performance of penetration and wireless network testing, alignment with best-practice frameworks, including NIST and CIS, and developing effective policies to improve IT security and prevent data loss. Ray has the ability to work with IT staff at all levels to address risks, vulnerabilities, and gaps that hamper network and application security.

### EDUCATION

**Bachelor of Science**  
Accounting

## Ray Resnick

## 24 Years' Experience

Senior IT Security Consultant

Securance Consulting

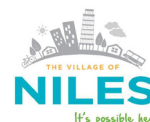
### CERTIFICATIONS



### RELEVANT EXPERIENCE

- ◆ Active directory reviews
- ◆ APT testing
- ◆ Cybersecurity policy development
- ◆ Data loss prevention
- ◆ Incident response planning
- ◆ HIPAA compliance
- ◆ Network security
- ◆ NIST CSF and CIS best practices
- ◆ Physical security controls reviews
- ◆ Policy development
- ◆ Risk and threat analysis
- ◆ Social engineering | user security awareness
- ◆ Wireless network security

### RELEVANT PROJECTS





## Employees



### Ibrahim Badrawi 15 Years' Experience

Senior IT Security Consultant

Securance Consulting

#### CERTIFICATIONS



Ibrahim is a cybersecurity specialist more than 15 years of experience in vulnerability assessments and penetration tests of external, internal, and wireless networks. His expertise includes current and emerging cyber threats and attack scenarios, compliance with best practice frameworks such as NIST and CIS, policy planning and development, and incident response.

#### RELEVANT EXPERIENCE

- ◆ Active directory reviews
- ◆ IT security
- ◆ Cybersecurity assessments
- ◆ NIST and CIS alignment
- ◆ Data loss prevention
- ◆ Physical security assessments
- ◆ Incident response planning
- ◆ Risk and threat analysis
- ◆ Internal | external network security
- ◆ Social engineering | user security awareness
- ◆ IT policy development
- ◆ Wireless network assessments

#### EDUCATION

##### Bachelor of Science

IT Management

##### Associates Degree

Applied Science and Network Administration

#### RELEVANT PROJECTS



# PROFESSIONAL REFERENCE LIST

Professional Reference List: Provide a list of minimum three (3) references. The list should include a specific contact name, address, phone number, and agency of employment. Each reference should include a brief description and length of the project developed with the reference.

Securance has performed similar assessments for the following clients. We invite you to talk with them to confirm the quality and added value of the services we provided.

Name and Location	Term of Service	Reference Contact	Description of Service
City of Modesto 1010 Tenth Street Suite 6600 Modesto, CA 95354	January 2020 - February 2021	Phil Calbreath IT Security Officer 209.571.5594 pcalbreath@modestogov.com	IT Security Audit Services
City of St. Charles 2 E. Main St. St. Charles, IL 60174	Multiple projects 2018 - 2021	Larry Gunderson Director of Information Systems 630.377.4400 lgunderson@stcharlesil.gov	IT Security Assessments IT Audit with IRP Tabletop Exercise
Village of Schaumburg 101 Schaumburg Court Schaumburg, IL 60193	2015, 2016, 2018	Peter Schaak Director of Information Technology 847.923.3825 pschaak@villageofschaumburg.com	Network Security Assessment HIPAA Security Assessment System Security Assessment

*In my experience in working with Securance, I have found them to be thoroughly professional, knowledgeable, and capable. Because of this, they are one of the few companies that I trust to provide critical services to ensure the security and integrity of our systems.*

— Michael I Sanders  
Denny's Inc. .

## Professional Reference List

### Similar Project Experience

#### CASE STUDY

**Client Name:**  
City of St. Charles (City)

**Securance Team:**  
Paul Ashe  
Chris Bunn

**Project Duration:**  
3 Months

#### IT Security Assessment

##### Client Objectives

The City needed a vendor to:



Identify technical threats, vulnerabilities, and risks in the City's IT environment

##### Securance Solution

The Securance team:



Assessed the design and operating effectiveness of IT processes and controls user provisioning, backup, change management, logging, monitoring, remote access, third-party access, and patch management)



Identified and validated technical vulnerabilities in the external, internal, and wireless networks, databases, operating systems, and web applications



Supported the City throughout the remediation phase by performing task-specific remediation validation tests

#### QUANTIFIABLE VALUE

**60%**

**Reduction in network and database vulnerabilities**



**Improved logging and monitoring, change management, patch management, and disaster recovery processes**

## Professional Reference List

### Similar Project Experience

#### CASE STUDY

**Client Name:**  
City of Highland Park  
(City)

**Securance Team:**  
Paul Ashe  
Chris Bunn

**Project Duration:**  
6 Weeks

#### Cybersecurity Assessment

##### Client Objectives

City needed a vendor to:



Identify and rank technology-specific vulnerabilities | risks in the:

- ◆ Internal network
- ◆ External network
- ◆ Wireless network
- ◆ Active Directory



Assess the adequacy of the City's cybersecurity insurance policy



Review the City's IT general computer controls and processes

##### Securance Solution

The Securance team:



Identified technology-specific vulnerabilities in the City's technologies and provided detailed remediation recommendations



Assessed IT processes relative to NIST standards of security and controls

#### QUANTIFIABLE VALUE



**Decreased technical threats in City's environment**



**Eliminated key person risk**



**Improved alignment with NIST SP 800-53**

## Professional Reference List

### Similar Project Experience

#### CASE STUDY

**Client Name:**  
Village of Schaumburg  
(Village)

**Securance Team:**  
Paul Ashe  
Chris Bunn

**Project Duration:**  
1 Month

#### HIPAA | HITECH Risk Assessment

##### Client Objectives

Village needed vendor to:



Assess the Village's compliance with the HIPAA Privacy and Security Rules, identify potential liabilities, and draft a remediation plan



Develop a solid HIPAA procedure | protocol library and training program

##### Securance Solution

The Securance team:



Performed a HIPAA Privacy and Security Rule assessment of select departments to determine their level of compliance



Reviewed HIPAA policies, procedures, and forms to determine adequacy of PHI and ePHI governance



Interviewed department managers to determine if their department generates, manages, or hosts systems that contain HIPAA protected information (Privacy Rule compliance)



Developed a detailed prioritized roadmap defining tasks and subtasks to achieve compliance

#### QUANTIFIABLE VALUE



**Adoption of additional policies, a new HIPAA training regimen, and a new database software compliant with HIPAA**



**The implementation of our recommendations resulted in compliance with HIPAA and a significant reduction in risk**



## ANNOTATED LISTING OF PUBLICATIONS, REPORTS, ETC.

---

Annotated listing of publications, reports, etc. of prior research work or needs assessments. Provide list of similar deliverables your company provided from previous engagements to comparable municipalities | agencies

Village will receive two final reports at the end of the engagement, a management report and a technician's report. The Securance engagement manager will review the reports with Village's team and other stakeholders to ensure that the findings and recommendations are understood, and to answer any questions that Village may have. In addition, we will provide free technical support and advice throughout the remediation phase. We provided similar deliverables to the City of St. Charles, the City of Highland Park, and the Village of Schaumburg. Comprehensive sample reports can be provided upon request.

### **Management Report**

Within one week of completing our fieldwork for the cyber security assessment, Securance will provide Village with a board-ready management report tailored to its environment and needs and developed with input from Village's stakeholders and IT management. Our analysis of the risks identified within 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, and provide realistic remediation recommendations aligned with Village's risk appetite. It will be customized to include all elements detailed in section IV.13 of the RFP. The report will include an executive summary and a detailed project report, both of which are described below.

### **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 Village's stakeholders during the exit conference. It will include summary of findings from the technical testing, the PCI, CJIS, and HIPAA compliance reviews.

*Click on the thumbnails  
to view the reports.*

## Annotated Listing Of Publications, Reports, ETC.

### Management Report

#### Detailed Project Report

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

*Click on the thumbnails  
to view the reports.*

### Technician's Report

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.

*We are very grateful for how easy you and your staff made this process for us. While your findings certainly contain sufficient detail for our IT partner to execute necessary changes going forward, the report is written in such a way that it's easily read by those of us with non-IT backgrounds. Your ability to boil down complicated technical matter to language that the rest of us can understand helps us to convey your work and its importance to our board and ultimately to our taxpayers.*

— Ryan Gruber

Washington County Community Development Agency .

# PRICING

Pricing: Vendors should provide a clear and comprehensive cost breakdown by line item and identify its total cost for the project. Vendor's should provide hourly rates for possible future consulting or changes to the project scope. Vendors should indicate if their services are available through any State of Illinois or local contracts. All pricing should be valid for 90 days from the proposal submission deadline.

Securance has provided itemized pricing for the major aspects of this project in the table below. Pricing is valid for ninety (90) days.

Project Scope Item	Line Item Fee
IV.1a External Network Vulnerability Assessment and Penetration Testing (28 IPs) — Value Add	\$3,968
IV.1b Internal Network Vulnerability Assessment and Penetration Testing (650 IPs, 1location)	\$4,960
IV.1c. Wireless Network (21 wireless access points)	\$2,976
IV.2. Access Controls Active Directory Assessment	\$2,976
IV.3a PCI Compliance Assessment	\$4,960
IV.3b HIPAA Compliance Assessment (Security Rule Only)	\$9,920
IV.3c CJIS Compliance Assessment	\$7,440
IV.4 Physical Access (1 location)	\$744
IV.5 Remote Access	\$1,984
IV.6 Internet Access	\$1,984
IV.7 Social Engineering (50 targets email phishing) — Value Add	\$1,984
IV.8 Connections to External Partners	\$1,984
IV.9 Advanced Persistent Threat Assessment   Indicators of Compromise Assessment — Value Add	\$4,960
IV.10 Develop Organizational Security Policy	\$1,984
IV.11 Develop Cybersecurity Incident Response Plan	\$3,968
IV.12 Develop Data Loss Prevention Policy	\$2,976
IV.13 Reporting Deliverables	\$4,960
Knowledge Transfer Session — Value Add	\$992
Retest of Urgent and Critical Vulnerabilities — Value Add	\$4,960
Travel	Included
Independent Project Review*	Included
<b>Subtotal</b>	\$71,672
<b>Value Add Price Reduction</b>	<b>(\$17,856)</b>
<b>Total</b>	\$53,816

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



## Pricing

### 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 Village personnel, or unavailability of documentation occur, Securance will determine their effect on the engagement scope, timing, and | or fees and promptly notify Village of any such changes. Securance will not proceed with any changes or additions to the scope of work without Village's explicit written approval.

### Hourly Rate

Securance's cost proposal is based on an hourly rate of \$124, inclusive of labor, travel, 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.

### Payment Terms

Securance will submit an invoice after delivering a draft management report. All fees are due within 30 days following receipt of invoice. Securance will deliver the final management report following receipt of payment.

*As we have recently completed our very first network security assessment and worked with Securance to do so, I just want to say it was a pleasure working with you and your team and we're very pleased with the final results.*

*Like all public agencies we have a limited budget and you delivered a high quality and economic service to us that was appropriately tailored for managing the risks specific to our organization. Thanks again for a job well done*

— Jay Meredith, Finance Director  
City of Grants Pass

## Pricing

### Added Value

Securance will provide Village with five value-added deliverables. Each of the deliverables described in the table below is intended to help Village continually improve its overall information security posture long after this engagement is over.

Deliverable	Value
<b>External Network Vulnerability Assessment   Penetration Testing</b>	We will provide the requested vulnerability assessment and penetration test of the external network at no additional cost. For more information, please see our external   internal vulnerability assessment and advanced penetration testing methodology beginning on page 5 of our proposal.
<b>Social Engineering</b>	This requested scope item will be provided at no cost to Village. It will prove the adequacy of or demonstrate the need for improved security awareness training by conducting phishing social engineering exercises.
<b>Indicators of Compromise Testing</b>	Securance will scour Village’s IT environment for evidence of past or ongoing compromise, particularly focusing our inspection on domain controller(s) and file servers. See our methodology on page 12.
<b>Remediation Retesting of Urgent and Critical Vulnerabilities and Findings</b>	What organizations do after an assessment is just as important as the assessment itself. At Securance, our passion is working with clients who implement our proven recommendations to improve their risk and security profiles over the long term. We will retest urgent and critical vulnerabilities and findings within 180 days of the delivery of our final report.
<b>Knowledge Transfer</b>	To ensure our assessment provides high value, is fully understandable, and the information obtained is sustained, 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 task at will.



APPENDIX

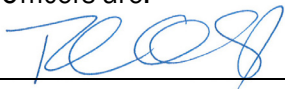
# ORGANIZATION OF FIRM

## **SECTION VII ORGANIZATION OF FIRM**

**Please fill out the applicable section:**

**A. Corporation:**

The Contractor is a corporation, legally named Securance LLC and is organized and existing in good standing under the laws of the State of Florida. The full names of its Officers are:

President 

Secretary \_\_\_\_\_

Treasurer \_\_\_\_\_

Registered Agent Name and Address: Paul Ashe, 13916 Monroes Business Park, Suite 102, Tampa, FL 33635

The corporation has a corporate seal. (In the event that this Proposal is executed by a person other than the President, attach hereto a certified copy of that section of Corporate By-Laws or other authorization by the Corporation that permits the person to execute the offer for the corporation.)

**B. Sole Proprietor:**

The Contractor is a Sole Proprietor. If the Contractor does business under an Assumed Name, the

Assumed Name is N/A, which is registered with the Cook County Clerk. The Contractor is otherwise in compliance with the Assumed Business Name Act, 805 ILCS 405/0.01, et. seq.

**C. Partnership:**

The Contractor is a Partnership which operates under the name N/A

The following are the names, addresses and signatures of all partners:

<u>N/A</u>	<u>N/A</u>
_____ Signature	_____ Signature

(Attach additional sheets if necessary.) If so, check here N/A.

If the partnership does business under an assumed name, the assumed name must be registered with the Cook County Clerk and the partnership is otherwise in compliance with the Assumed Business Name Act, 805 ILCS 405/0.01, et. seq.

## Organization of Firm

**D. Affiliates:** The name and address of any affiliated entity of the business, including a description of the affiliation: None.

  
\_\_\_\_\_  
Signature of Owner

[THIS SPACE LEFT INTENTIONALLY BLANK]



# COMPLIANCE AFFIDAVIT

---

## SECTION VIII COMPLIANCE AFFIDAVIT


I, Paul Ashe, (Print Name) being first duly sworn on oath depose and state:

1. I am the (title) President of the Proposing Firm and am authorized to make the statements contained in this affidavit on behalf of the firm;
2. I have examined and carefully prepared this Proposal based on the request and have verified the facts contained in the Proposal in detail before submitting it;
3. The Proposing Firm is organized as indicated above on the form entitled “Organization of Proposing Firm.”
4. I authorize the Village of Oak Park to verify the Firm’s business references and credit at its option;
5. Neither the Proposing Firm nor its affiliates<sup>1</sup> are barred from proposing on this project as a result of a violation of 720 ILCS 5/33E-3 or 33E-4 related to bid rigging and bid rotating, or Section 2-6-12 of the Oak Park Village Code related to “Proposing Requirements.”
6. The Proposing Firm has completed the M/W/DBE status indicated below on the form entitled “EEO Report.”
7. Neither the Proposing Firm nor its affiliates are barred from enter into an agreement with the Village of Oak Park because of any delinquency in the payment of any debt or tax owed to the Village except for those taxes which the Proposing Firm is contesting, in accordance with the procedures established by the appropriate revenue act, liability for the tax or the amount of the tax. I understand that making a false statement regarding delinquency in taxes is a Class A Misdemeanor and, in addition, voids the agreement and allows the Village of Oak Park to recover all amounts paid to the Proposing Firm under the agreement in civil action.
8. I am familiar with Section 13-312 through 13-3-4 of the Oak Park Village Code relating to Fair Employment Practices and understand the contents thereof; and state that the Proposing Firm is an “Equal Opportunity Employer” as defined by Section 2000(E) of Chapter 21, Title 42 of the United States Code and Federal Executive Orders #11246 and #11375 which are incorporated herein by reference. **Also complete the attached EEO Report or Submit an EEO-1.**
9. I certify that the Firm is in compliance with the Drug Free Workplace Act, 41 U.S.C.A, 702

---

<sup>1</sup> Affiliates means: (i) any subsidiary or parent of the agreeing business entity, (ii) any member of the same unitary business group; (iii) any person with any ownership interest or distributive share of the agreeing business entity in excess of 7.5%; (iv) any entity owned or controlled by an executive employee, his or her spouse or minor children of the agreeing business entity.


**Compliance Affidavit**

Signature: 

Name and address of Business: Securance LLC, 13916 Monroes Business Park, Suite 102, Tampa, Florida 33635

Telephone 877.578.0215 E-Mail eanderson@securanceconsulting.com

Subscribed to and sworn before me this 20th day of February, 2023.

  
Notary Public

- Notary Public Seal -



[THIS SPACE LEFT INTENTIONALLY BLANK]

# M/W/DBE STATUS AND EEO REPORT

## **SECTION X** **M/W/DBE STATUS AND EEO REPORT**

Failure to respond truthfully to any questions on this form, failure to complete the form or failure to cooperate fully with further inquiry by the Village of Oak Park will result in disqualification of this Proposal.

1. Contractor Name: Securance LLC

2. Check here if your firm is:

- Minority Business Enterprise (MBE) (A firm that is at least 51% owned, managed and controlled by a Minority.)
- Women’s Business Enterprise (WBE) (A firm that is at least 51% owned, managed and controlled by a Woman.)
- Owned by a person with a disability (DBE) (A firm that is at least 51% owned by a person with a disability)
- None of the above

[Submit copies of any M/W/DBE certifications]

3. What is the size of the firm’s current stable work force?

15 Number of full-time employees

0 Number of part-time employees

4. Similar information will be requested of all sub-contractors performing work pursuant to the applicable agreement. Forms will be furnished to the lowest responsible contractor with the notice of agreement award, and these forms must be completed and submitted to the Village before the execution of the agreement by the Village.

Signature: 

Date: 2.20.2023



### M/W/DBE Status and EEO Report

#### EEO Report

Please fill out this form completely. Failure to respond truthfully to any questions on this form, or failure to cooperate fully with further inquiry by the Village of Oak Park will result in disqualification of this Proposal. An incomplete form will disqualify your Proposal.

An EEO-1 Report may be submitted in lieu of this report

7

Contractor Name Securance LLC  
 Total Employees 15

Job Category	Total # of Empl.	Males							Females				Total Minorities
		Total Males	Total Females	Black	Hispanic	American Indian	Alaskan Native	Asian & Pacific Islander	Hispanic	American Indian	Alaskan Native	Asian & Pacific Islander	
Officials & Managers	4	1	3	1									1
Professionals	7							1					1
Technicians	0												0
Sales Workers	0												0
Office & Clerical	4								1				1
Semi-Skilled	0												0
Laborers	0												0
Service Workers	0												0
Management Trainees	0												0
Apprentices	0												0

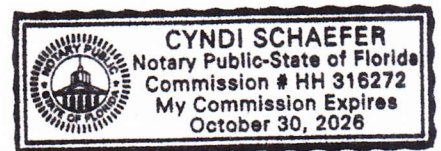
This completed and notarized report must accompany your Proposal. It should be attached to your Affidavit of Compliance. Failure to include it with your Proposal may disqualify you from consideration.

Paul Ashe, being first duly sworn, deposes and says that he/she is  
 (Name of Person Making Affidavit)  
President of Securance LLC and that the above EEO  
 (Title or Officer)

Report is true and accurate and is submitted with the intent that it be relied upon.

Cyndi Schaefer  
 (Signature)

2/20/23  
 (Date)



**M/W/DBE Status and EEO Report**

# State of Florida

## Minority Business Certification

### Securance LLC

Is certified under the provisions of  
287 and 295.187, Florida Statutes, for a period from:  
12/14/2021 to 12/14/2023



J. Todd Inman  
Florida Department of Management Services



Office of Supplier Diversity  
4050 Esplanade Way, Suite 380  
Tallahassee, FL 32399  
850-487-0915  
[www.dms.myflorida.com/osd](http://www.dms.myflorida.com/osd)



**SECURANCE  
CONSULTING**

*the advantage of insight*

13916 Monroes Business Park, Suite 102 • Tampa, FL 33635

**[www.securanceconsulting.com](http://www.securanceconsulting.com)**