

COOPERATIVE CONTRACT BRIDGE AGREEMENT
BETWEEN THE UNIVERSITY of MARY WASHINGTON AND SECURANCE, LLC
UMW Contract #: COOP 23-1872/ Original Contract #: UCPJMU6771

IT Consulting Services

In accordance with the terms and conditions of the cooperative contract between Securance, LLC, and James Madison University ("Original Contract"), for IT Consulting Services, and the "Cooperative Purchasing" clause, the University of Mary Washington ("UMW" or "University") hereby enters into Agreement with Securance, LLC ("Contractor"), for which the following Scope of Services and terms and conditions shall apply, in conjunction with the terms and conditions of the Original Contract, and to any purchase order issued hereunder.

WITNESSETH that the Contractor and the University, in consideration of the mutual covenants, promises and agreements herein contained, agree as follows:

PERIOD OF CONTRACT: April 7, 2025 through December 10, 2025 with 3 one-year renewal options.

CONTRACT DOCUMENTS: The contract documents shall consist of in order of precedence:

1. This signed Contract;
2. The Contractor's proposal dated February 25, 2025 including all attachments;
3. Any addenda and the original solicitation, RFP # FDC-1175, dated June 15, 2023 to include:
 - a. The Statement of Needs
 - b. The General Terms and Conditions
 - c. The Special Terms and Conditions;

All of which are incorporated herein by reference and constitute the "contract documents." Any contractual claims shall be submitted in accordance with the contractual dispute procedures set forth in the Commonwealth of Virginia Purchasing Manual for Institutions of Higher Education and their Vendors.

SCOPE OF SERVICES: The Contractor shall provide the IT Consulting services described herein.

PRICING: Contractor will charge and hourly rate of \$132.00, with a total project cost not to exceed \$48,840.00.

CONTRACT ADMINISTRATION: The Director of Internal Audit, or designee, shall be identified by the University as the Contract Administrator and shall use all powers under the contract to enforce its faithfulness and performance in conjunction with the University's Procurement Services department.

GENERAL TERMS AND CONDITIONS: Please refer to the link to follow regarding [Required General Terms and Conditions](#) of this Bridge Agreement which are a mandatory part of the resulting contract.

METHOD OF PAYMENT: The Contractor shall be paid using one of the following methods for all University initiated procurements:

1. University Charge Card: At the time of verified receipt of goods or services, and proper invoice, if the Contractor's eVA profile indicates acceptance of credit cards in payment, the University will authorize payment by University charge card, currently through the Bank of America Visa, under the following terms:
 - a. Any "Check-out fees" imposed by the contractor must be disclosed prior to the purchase.
 - b. No check-out fee or surcharge, that was appropriately disclosed in advance of the sale/purchase, shall be greater than 3% of the total sale., effective 4/15/2023. The University expects that these costs, as well as all contractor business expenses will be built into the contractor's quoted price.
2. Virtual Payables through Bank of America: All payments made under Virtual Payables will have a net 16 payment term. For more information about this payment option, contact UMW's Accounts Payable department at: payables@umw.edu or view <http://www.bankofamerica.com/epayablesvendors>.
3. UMW Check or ACH: Payment will be made per the terms of the contract, or 30 days after satisfactory performance of the contract in all provisions thereof and upon receipt of a properly completed invoice, whichever is later; in accordance with Chapter 43, VPPA, Article 4, Code of Virginia.

NOTE: ACH must be set up in advance prior to submittal of any invoices.
<https://www.doa.virginia.gov/reference.shtml#edi>

To be considered eligible for payment, all physical invoices must be received at the address below and should reference the eVA purchase order and UMW contract numbers as applicable. All electronic invoices must be sent to invoices@mail.umw.edu. *The University will not be responsible for late payment or nonpayment of invoices not received directly by Accounts Payable at this email address or at the mailing address indicated (below).*

UNIVERSITY OF MARY WASHINGTON
Attn: ACCOUNTS PAYABLE
1301 COLLEGE AVENUE
FREDERICKSBURG, VA 22401

Note: This public body does not discriminate against faith-based organizations in accordance with the *Governing Rules §36* or against a bidder or offeror because of race, religion, color, sex, national origin, age, disability, or any basis prohibited by state law relating to discrimination in employment.

In witness, whereof, the parties have caused this Contract to be duly executed intending to be bound thereby.

SECURANCE, LLC

Signature: *Gillian Tedeschi*

Printed Name: Gillian Tedeschi

Title: Vice President

UNIVERSITY OF MARY WASHINGTON

Signature: *Alicia Britt*

Printed Name: Alicia Britt

Title: Contract Officer

Date: April 25, 2025

FEI/FIN#: 03-0392503

Phone: 877-578-0215

Email: gtedeschi@securanceconsulting.com

Date: 04/25/2025



February 25, 2025

Virginia Grigsby
Director of Internal Audit
George Washington Hall 219
1301 College Avenue
Fredericksburg, VA 22401

Dear Virginia:

Thank you for considering Securance Consulting for the University of Mary Washington's (UMW's) upcoming information technology auditing services. Securance is an expert IT consulting firm with more than 23 years of experience. We have the breadth of expertise to help UMW's internal audit department by conducting independent assessments of IT security and offering insightful guidance for improvement. **We want to partner with you!** With Securance, UMW will benefit from our:

- ▶ **Senior IT Audit Consultants.** Our team of key consultants, which I will lead, has a combined 120 years of experience — 26 years or more each.
- ▶ **Education-Sector Expertise.** Securance has provided IT security services to dozens of educational institutions at all levels, including several in Virginia, and understands their unique needs and challenges.
- ▶ **Efficient Execution.** We will leverage our experience in the higher education sector to provide UMW with a board-ready draft report within one week of completing fieldwork.
- ▶ **Proven Track Record.** Securance has completed more than 3,000 IT audits and other security assessments during our two decades of service. We have completed all projects on time and within budget, and we will do the same for this engagement.
- ▶ **Proprietary Artificial Intelligence (AI) Tool.** We leverage AI to identify and predict risks, security weaknesses, compliance violations, and even potential attacks. We use generative AI (GenAI) and large language models (LLMs) to focus our approach to assessments and cybersecurity services on the most pertinent risks to our clients' technologies.

On the next page is a small sample of projects similar in scope to UMW's.

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

CONFIDENTIAL —



Client	Project(s)	Contract Value	Description	Performance Period
Radford University	Multiple IT security assessments	\$256,167 (cumulative)	Securance has performed risk-based assessments of the University's cybersecurity, including data protection, facilities and personnel security, threat management, and IT asset management.	2022–present
City of Richmond	Multiple IT security assessments	\$326,285 (cumulative)	Securance has performed many projects for the City, including vulnerability assessments, a social engineering campaign, and network device configuration reviews.	2010–present
Rowan University	IT security audit	\$32,240	Securance performed a network architecture audit, vulnerability assessment penetration testing, and configuration reviews of firewalls, routers, and switches.	2023

We acknowledge that Securance may not be the lowest-priced bidder for the services required by UMW. 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, UMW will not find a firm whose analyses and results are more accurate and exhaustive than ours. Discussions with our clients over the past 23 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.seuranceconsulting.com

TABLE OF CONTENTS

4	ABOUT SECURANCE
5	THE SECURANCE DIFFERENCE
6	WE UNDERSTAND EDUCATION
7	Similar Clients
8	Case Studies
11	OUR UNDERSTANDING OF THE SCOPE
12	RISK-BASED IT AUDITS POWERED BY AI
14	SECURANCE APPROACH AND METHODOLOGY
14	External Network Vulnerability Assessment and Penetration Testing
21	Active Directory Assessment
24	Core Switch Configuration Review
26	Next-Generation Firewall Assessment
29	Enterprise Application Assessment
35	Microsoft File and Print Server Assessment
37	PROJECT TIMELINE
40	PROJECT MANAGEMENT
42	UMW RESOURCES NEEDED TO COMPLETE THE PROJECT
46	SECURANCE'S DEDICATED PROJECT TEAM
47	Resumes — Key Personnel
57	REFERENCES
58	PROPOSED FEES

23+ YEARS

Securance has more than 23 years of experience providing IT audit services similar in scope to those sought by UMW.

EXECUTIVE-LEVEL CONSULTANTS

Our executive-level consultants have provided vulnerability scans, penetration tests, and other technical assessments for clients such as Radford University, Texas A&M University, and Fairfax County Public Schools.

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 UMW's IT environment and organizational objectives. Then we will use that understanding to conduct thorough IT audits and deliver actionable guidance for improvement.

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 the University of Mary Washington (UMW). This proposal does not constitute an agreement between Securance Consulting and UMW. Any services Securance Consulting may provide to UMW will be governed by the terms of a separate written agreement signed by both parties. All offers to provide professional services are valid for 60 days.

ABOUT SECURANCE

More Than Two Decades of IT Audit 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, UMW's proposed engagement manager (EM), founded Securance in March 2002. Since then, we have performed more than 3,000 IT audits for clients in nearly every industry, including numerous higher-education clients, helping them to manage information security risks and remediate network and system vulnerabilities.

Exclusively Staffed with Senior-Level IT Audit Professionals

To provide the highest-quality services, Securance only hires IT consultants with at least 15 years of professional experience. Their expertise in enterprise technology, regulatory standards such as the Commonwealth of Virginia's Information Security Standard (SEC530), and security best practices is our foundation. We tailor each project to our clients' unique IT environments, security and control standards, and business requirements. They are committed to clear and proactive communication and will work with all relevant UMW departments and staff to achieve the project objectives.

THE SECURANCE DIFFERENCE

HANDS-ON
EXECUTIVE
LEADERSHIP ON
EVERY PROJECT



TECHNICAL RISK
TRANSLATED TO
BUSINESS RISK



Powered
by



THE SECURANCE DIFFERENCE

HANDS-ON EXECUTIVE LEADERSHIP ON EVERY PROJECT

A niche IT audit and cybersecurity and consulting 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, work alongside our staff consultants on every project.

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 the IT department, helping internal audit and senior management understand the risks and making our recommendations truly actionable.

TECHNICAL RISK TRANSLATED TO BUSINESS RISK

Powered
by



Securance is the *only* IT audit 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.

WE UNDERSTAND EDUCATION

The education sector is at high risk for cyber attack because of the breadth and nature of data they store on students and staff, including personally identifiable, healthcare, and financial information. Schools and colleges are also at increased risk because of the size of their attack surfaces, due to the digital capabilities afforded to staff and students via portable devices and the applications used for instruction and tracking, as well as their use of open networks.

Some of the unique challenges the education sector faces include increased attack frequency, limited IT resources, legacy infrastructure, a general lack of cyber awareness, and the need to balance academic openness with cybersecurity. To enable the safe and legally compliant handling of sensitive information, universities like UMW need a technology partner who understands these challenges, as well as the evolving nature of cybersecurity threats. Securance is that partner, and our experience and expertise prove this.

Securance Experience with Education at a Glance

- ▶ **23 years** as a firm serving community college systems, private colleges, major research universities, boards of education, and K–12 school districts.
- ▶ Senior cybersecurity consultants, each with **more than 15 years'** experience serving the education sector.
- ▶ **50** education and **400** government clients.

Given our qualifications, Securance will bring specific value to UMW, including:

- ▶ Experience conducting a variety of IT audits and security assessments for educational institutions and other public entities, including Radford University, Texas A&M University, Ohio University, and Atlanta Public Schools.
- ▶ Familiarity with the needs of public entities in Virginia through several successful partnerships in the state. Besides Radford University, these include the City of Richmond, Fairfax County Public Schools, Henrico County Public Schools, Newport News Public Schools, and the County of Albemarle.
- ▶ Guaranteed responsiveness and continuous communication with UMW's audit department, including on-site work as required, to expedite project completion.
- ▶ Dedication to making our findings and recommendations understandable and actionable for all UMW stakeholders.

WE UNDERSTAND EDUCATION

Similar Clients

Below is a sample of clients that have engaged Securance for IT services similar to those sought by UMW.



WE UNDERSTAND EDUCATION

Case Studies



CLIENT NAME: Radford University
SECURANCE TEAM: Paul Ashe, Chris Bunn, Montrell Hill
PROJECT DURATION: Three months in 2023
CLIENT SINCE: 2023

PROJECT OUTCOMES

Strengthened the University’s security posture by identifying vulnerabilities in its firewall configuration and recommending the implementation of an on-premises security operations center

IT SECURITY AUDIT AND NETWORK ASSESSMENT

CLIENT OBJECTIVES

University sought a vendor to:

- Assess its security posture.
- Perform technical testing of its IT environment as needed.

SECURANCE SOLUTION

The Securance team:

- Compared the University’s IT policies and procedures to industry standards.
- Performed an audit of the AD environment.
- Reviewed and provided recommendations to improve the University’s incident response and disaster recovery plans.
- Performed a remote access assessment.
- Assessed the security of the University’s wireless network.
- Performed a security assessment of the Internet-facing firewall.

WE UNDERSTAND EDUCATION

Case Studies



CLIENT NAME: City of Richmond

SECURANCE TEAM: Paul Ashe, Chris Bunn, Ray Resnick

PROJECT DURATION: Multiple Projects

CLIENT SINCE: 2010

PROJECT OUTCOMES

Identified urgent and critical vulnerabilities within the internal network infrastructure and patch management process

Facilitated a significant reduction in technical risks following remediation

Provided clear recommendations to address critical risks in the City's incident response process and ransomware readiness

CYBERSECURITY AUDIT

CLIENT OBJECTIVES

The City needed a vendor to:

- ▶ Identify technical vulnerabilities, inefficiencies in the incident response process, and IT process risks to improve its security posture.
- ▶ Perform a vulnerability assessment and penetration test of its internal, external, and wireless networks.

SECURANCE SOLUTION

The Securance team:

- ▶ Assessed database, router / switch, and firewall configurations and security to identify and address risks.
- ▶ Conducted internal, external, and wireless network vulnerability assessments and penetration tests.
- ▶ Assessed the City's incident response process / ransomware readiness and provided actionable recommendations to mitigate identified critical risks.
- ▶ Performed a detailed analysis of the City's enterprise application databases and operating systems.
- ▶ Assessed the City's patch management and remote access policies.
- ▶ Conducted an email phishing campaign to assess end-user security awareness.

WE UNDERSTAND EDUCATION

Case Studies



CLIENT NAME: Henrico County Public Schools (HCPS)

SECURANCE TEAM: Paul Ashe, Chris Bunn

PROJECT DURATION: 1 month

CLIENT SINCE: 2022

PROJECT OUTCOMES

Identified critical vulnerabilities in the internal network

Validated the need for continuing security awareness training

CYBERSECURITY AS A SERVICE

CLIENT OBJECTIVES

HCPS sought a vendor to provide ongoing cybersecurity as a service (CSaaS), including the following tasks:

- ▶ Identify vulnerabilities in its networks and other selected technologies.
- ▶ Evaluate staff security awareness.
- ▶ Assess the security of its data.

SECURANCE SOLUTION

The Securance team has:

- ▶ Performed vulnerability assessments of HCPS's external, internal, and wireless networks.
- ▶ Conducted email phishing and phone pretexting social engineering campaigns.
- ▶ Reviewed the configuration of HCPS's firewalls.

OUR UNDERSTANDING OF THE SCOPE

We understand that UMW requires the audits listed below. Detailed methodologies for selected assessments can be found on the following pages. Additional methodologies will be provided upon request.



- ▶ Kick-off Meeting
- ▶ Establish Rules of Engagement
- ▶ Create I Share Client Assistance Memo

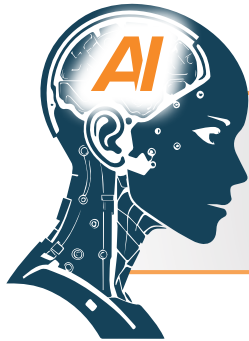


- ▶ IT Infrastructure Reviews
 - Internet Security Review (External Network Vulnerability Assessment and Penetration Test) — **Value Add**
 - Active Directory Assessment
 - Core Switch Assessment
 - Firewall Configuration Review (Fortinet)
 - Transport Layer Security (TLS) | Wide-Area Network (WAN) Review
 - Dynamic Host Configuration Protocol (DNCP) | Domain Name Server (DNS) Assessment
 - Microsoft File and Print Server Assessment
- ▶ Titanium Security Review
- ▶ AMAG Security Review
- ▶ Computer-Aided Dispatch (CAD) Review



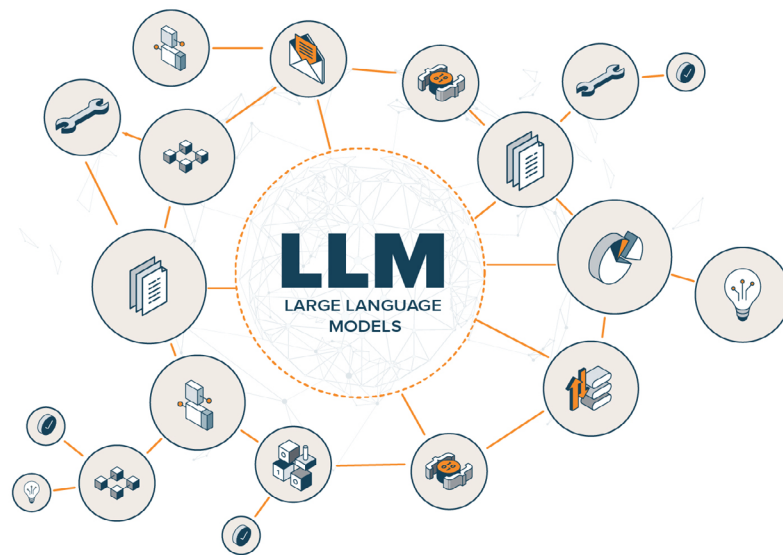
- ▶ Documentation of Findings and Recommendations

RISK-BASED IT AUDITS POWERED BY AI



Securance is **the first and only IT audit 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. IT risk management 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 IT audits.



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.

RISK-BASED IT AUDITS 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 its internal audit or 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.
- ▶ Whether the organization has an internal audit department.

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:

- ▶ A 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 selected detailed technical methodologies on the following pages. Other methodologies can be provided upon request.



SECURANCE APPROACH AND METHODOLOGY

External Network Vulnerability Assessment and Penetration Testing

Vulnerability assessments and penetration tests are fundamental to an organization's security against internal and external cyber threats. With 23 years of experiencing conducting these assessments for clients in every industry, including higher education. Securance understands how to maximize the value and efficiency of every step in the testing process. As a value-added service at no additional charge, our team will consider UMW'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:** UMW does not provide Securance with any internal knowledge of the target system that is not publicly available.
- ▶ **Gray Box:** UMW 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:** UMW 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 and develop rules of engagement.
 - Securance will work with UMW to confirm and agree upon clear rules of engagement for the project, including details about:

• Project scope of effort	• How to handle scope creep	• Communication rules
• Tool configuration	• The client's IP address	• Escalation plan
• UMW's unique IT environment	• Approved dates, times, and tools	• UMW and Securance contact information
• Privileged testing authority	• Interest in whitelisting Securance's lab IP	• UMW's specific concerns
• VoIP solution scan		
• Third-party hosted IP scans		
- ▶ Develop a specific scope that addresses which systems (if any) should not be assessed.

SECURANCE APPROACH AND METHODOLOGY

External Network Vulnerability Assessment and Penetration Testing (continued)

INFORMATION GATHERING

External Assessment

- ▶ Search for public information about UMW'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.

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.

SECURANCE APPROACH AND METHODOLOGY

External Network Vulnerability Assessment and Penetration Testing (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 I 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

ADVANCED PENETRATION TESTING

- ▶ Develop penetration testing rules of engagement.
- ▶ Determine the approved target systems for penetration testing.
- ▶ Utilize information gathered, including user names and passwords.
- ▶ Perform exploit testing.
- ▶ Collect and clean up evidence of exploitation.

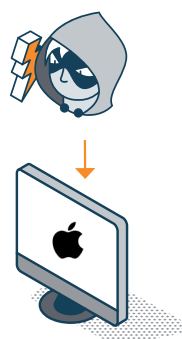
Our advanced penetration methodology makes use of automated tools, such as Core Impact, Metasploit, and Canvas, to exploit common security vulnerabilities throughout an organization. We leverage tools like Cobalt Strike to perform lateral testing, gain control of other systems on the network, and attempt to exfiltrate sensitive data. In addition to automated testing, Securance will also perform manual penetration testing to find weaknesses missed by the automated tools.

SECURANCE APPROACH AND METHODOLOGY

External Network Vulnerability Assessment and Penetration Testing (continued)

Our manual testing techniques include:

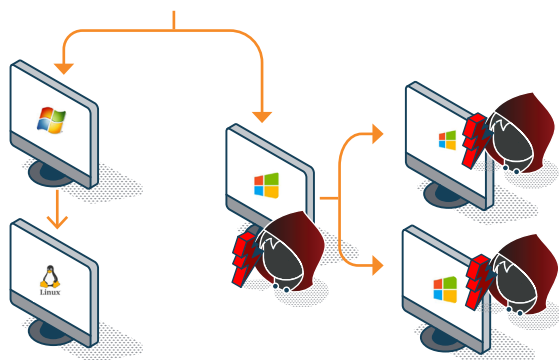
- ▶ Modification of scripts used in automated tools.
- ▶ Threat hunting on compromised hosts.
- ▶ Use of manual scripts available in the wild.
- ▶ Installation of security tools on compromised hosts.
- ▶ Keyboard entry on compromised hosts.
- ▶ Exploit of risk found based on newly installed security tools on compromised hosts.



Our penetration testing will involve:

- ▶ Moving laterally in the environment.
- ▶ Escalating account privileges.
- ▶ Attempting to exfiltrate data.
- ▶ Leaving a trophy.
- ▶ Cleaning up the environment.

Execute Automated and Manual Exploits



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.

SECURANCE APPROACH AND METHODOLOGY

External Network Vulnerability Assessment and Penetration Testing (continued)

THEIR APPROACH

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

THE SECURANCE WAY...

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

.... DELIVERS EXTRA VALUE TO YOU.

- ▶ UMW will receive a detailed report explaining how a bad actor might breach its network, and, more importantly, the specific steps required to prevent breaches.

Software Tools

Securance may use these tools during the penetration testing engagements, depending on UMW'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

SECURANCE APPROACH AND METHODOLOGY

External Network Vulnerability Assessment and Penetration Testing (continued)

- 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
- 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

► 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

► Penetration Testing Tools

- AppDetective: Designed to identify potential security risks and compliance violations in relational database management systems (RDBMS); can also perform penetration testing support, configuration management, and privileged escalation detection
- Cobalt Strike: Threat emulation software to create targeted attacks for penetration testing; simulates real-world attacks and tests the security defenses of organizations' networks and systems
- Burp: A software suite that can perform advanced scans, typically used for traffic interception, such as for HTTP requests
- Metasploit: Contains a vast collection of exploit modules that target known vulnerabilities in various operating systems, applications, and network services; automates the process of exploiting vulnerabilities to gain unauthorized access to target systems
- Fiddler: Collection of manual tools for dealing with web debugging, web session manipulation, and security and performance testing

► Exploitation Tools

- SolarWinds: A powerful combination of network discovery, system and security management, monitoring and attack tools
- Metasploit Framework: An advanced open-source platform for developing, testing and using exploit code, as well as identifying vulnerabilities and testing the effectiveness of security controls
- Core Impact: A powerful exploitation tool that can use access from one exploit to further exploit other devices

SECURANCE APPROACH AND METHODOLOGY

External Network Vulnerability Assessment and Penetration Testing (continued)

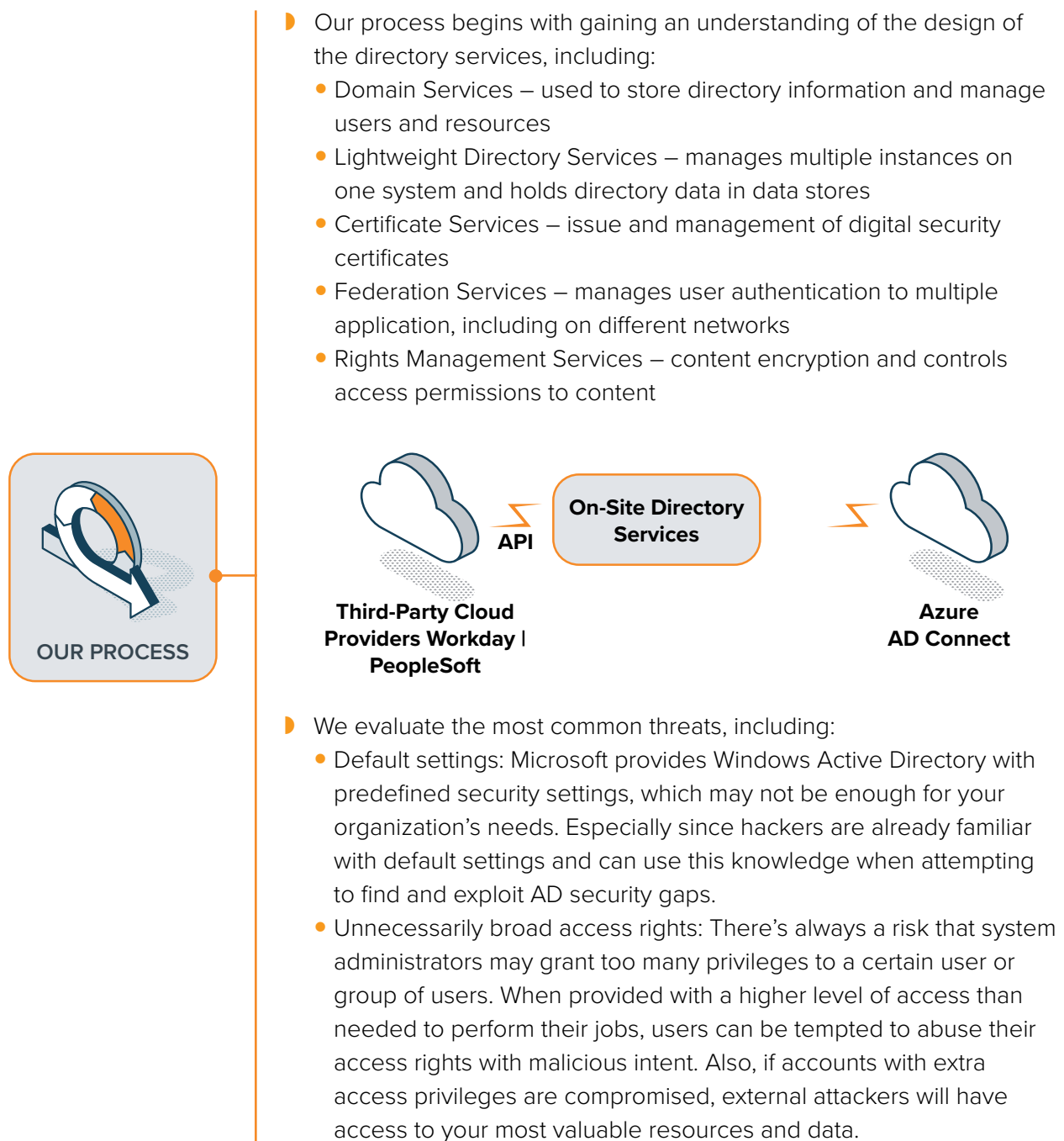
- BeEF (Browser Exploitation Framework): Aids in enumeration, phishing, and social engineering; provides GUI and practical client-side attack vectors to target different contexts and achieve various tasks, such as stealing credentials
- SQLmap: Automates the process of detecting and exploiting SQL injection flaws and database server takeovers; can detect various types of SQL injections, and supports an extensive range of databases
- SET (Social Engineer Toolkit): Performs advanced social engineering attacks, allowing users to create payloads, phishing pages like Google login, and other web attacks
- ▶ **Sniffing Tools:**
 - Wireshark: A network sniffer and TCP/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



SECURANCE APPROACH AND METHODOLOGY

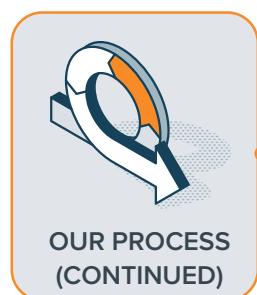
Active Directory Assessment

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.



SECURANCE APPROACH AND METHODOLOGY

Active Directory Assessment (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 Active Directory, 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 policy objects (GPOs), and other AD objects

SECURANCE APPROACH AND METHODOLOGY

Active Directory Assessment (continued)



- 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 others based on the fingerprint of the operating system.
- ▶ Then we compare Active Directory 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 Active Directory, including domain controllers, trusts, group policies, security settings, and all user accounts.
- ▶ Examines both technical and organizational aspects.

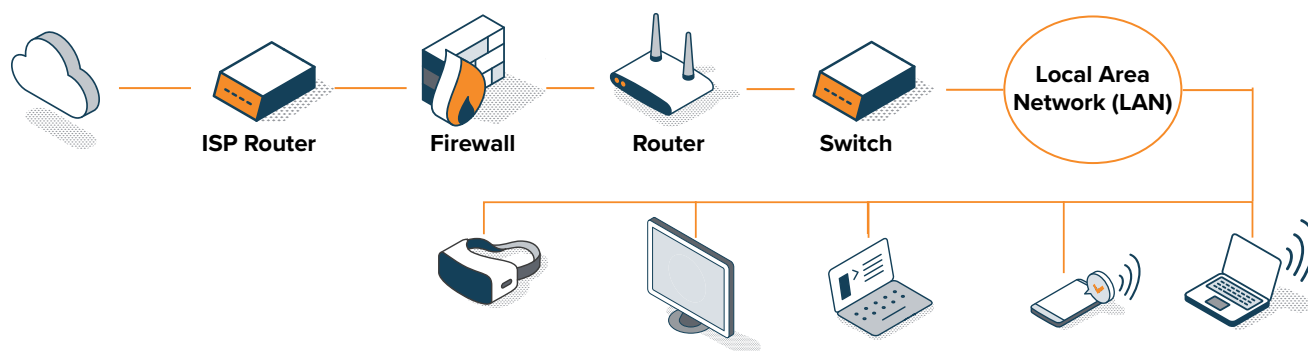
....DELIVERS EXTRA VALUE TO YOU.

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

SECURANCE APPROACH AND METHODOLOGY

Core Switch Configuration Review

Reviews of network devices like switches are critical for maintaining secure network infrastructure. Securance has conducted router and switch reviews for clients across all major industries, including educational institutions, over our 23-year history. The Securance methodology for evaluating the security of these network devices focuses on ensuring components are correctly configured and firmware is updated to create and maintain a network devoid of infrastructural weaknesses.



Pre-Assessment

- ▶ Interview device administrator(s) to gain a preliminary understanding of the devices in the network and their current configurations.

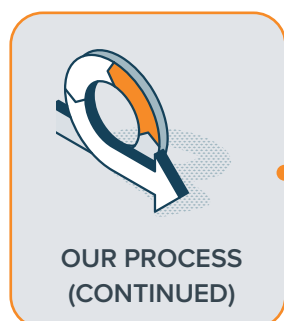
Analysis

- ▶ Perform an automated and manual, line-by-line review of device configuration, ensuring:
 - The device is running the most up-to-date firmware version.
 - Default manufacturer passwords are not in use.
 - Insecure protocols are not in place:
 - Telnet configuration.
 - Unencrypted communications.
 - File transfer protocol (FTP).
 - Access control is strong—Securance will review Access Control Lists (ACLs) to control traffic flow, restrict unauthorized access, and enhance security.
 - Network Address Translation (NAT) is properly implemented to effectively manage translating private and public IP addresses.
 - Virtual Local Area Networks (VLANs) are configured to better segment network traffic.
 - Spanning Tree Protocol (STP) is configured to prevent network loops and ensure redundancy.
 - Port Security is configured to enhance protection against unauthorized devices.



SECURANCE APPROACH AND METHODOLOGY

Core Switch Configuration Review



- Quality of Service (QoS) settings are configured to prioritize certain aspects of UMW's network traffic.
- Changes to the device configuration comply with organizational change management procedures.

Vulnerability Scan

- ▶ Perform an unauthenticated and I or authenticated vulnerability scan of the device to identify vulnerabilities associated with the specific device. Based on the identified vulnerabilities, perform specific exploit testing with a goal of obtaining full control of the device.

Monitoring

- ▶ Review logs using manual and automated techniques to verify that:
 - Logging for security events is enabled.
 - Logs are housed in a central location.
 - Sensitive information, such as passwords, are not logged.
 - Logs are not altered.
 - Alerts are set up.
 - Logs are aggregated with other technology logs.
 - Logs are reviewed on a regular basis.

Gap Analysis

- ▶ Compare device configuration and policies to the Center for Internet Security (CIS) benchmarks to identify gaps and develop a plan for UMW to remediate them.

THEIR APPROACH

- ▶ Typically, a desktop and administrative review of the device's configuration.
- ▶ Results are based on superficial analysis, providing incomplete recommendations.

THE SECURANCE WAY...

- ▶ Thorough examination of configuration, security, and best-practice adherence.
- ▶ Performs vulnerability scan to focus on critical areas and potential network risks.

....DELIVERS EXTRA VALUE TO YOU.

- ▶ UMW will receive a risk-focused and well documented report that provides clear solutions with actionable improvement steps.



SECURANCE APPROACH AND METHODOLOGY

Next-Generation Firewall Assessment

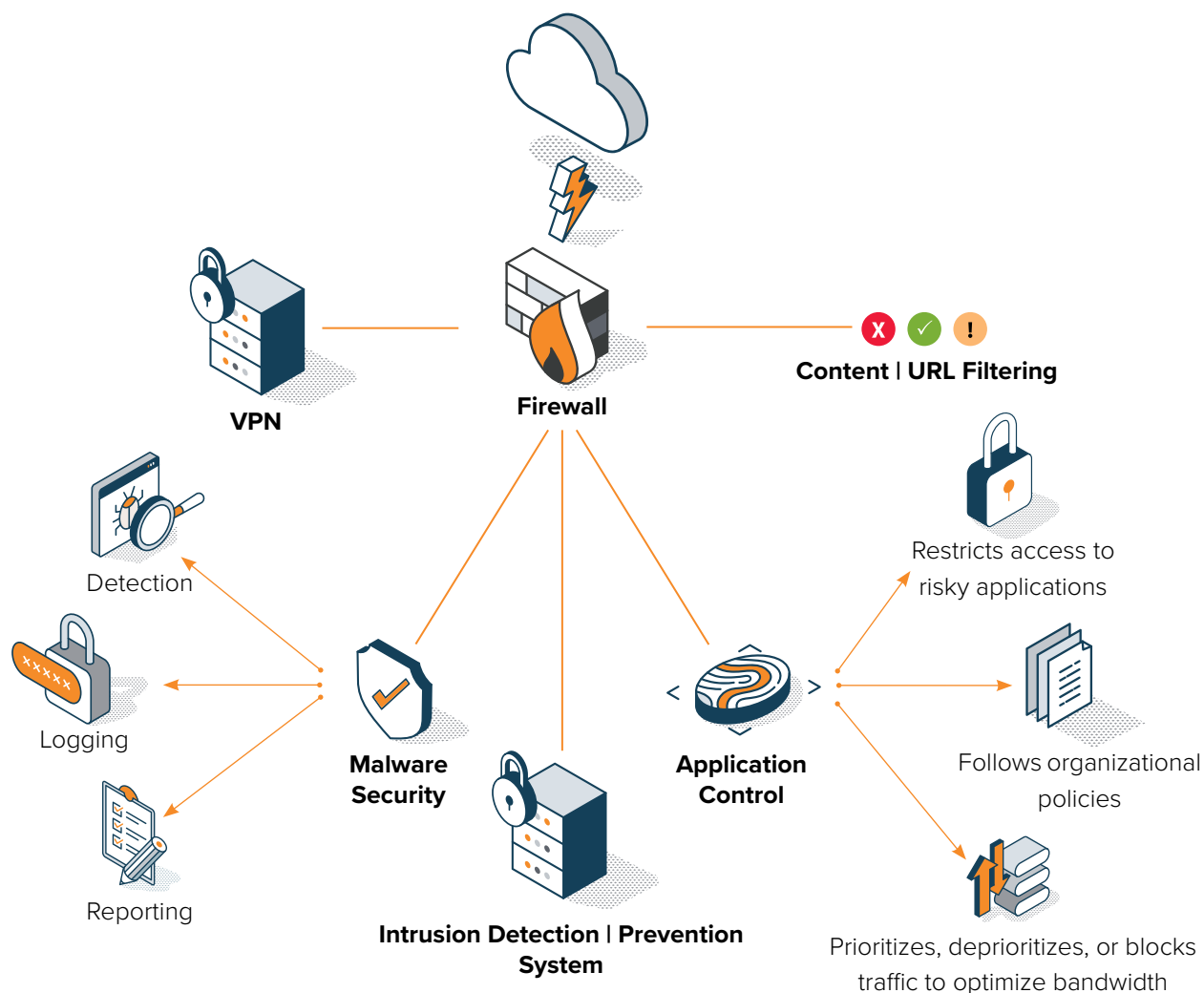
Securance's approach to performing firewall configuration reviews covers misconfigurations, vulnerabilities, supporting IT processes, and other weaknesses that could leave an organization susceptible to attack. To ensure that UMW's current firewall configuration is secure, we will assess it against best-practice guidelines. We will discern the optimal configuration for your firewall according to your network environment and security goals. Our comprehensive assessment begins with gaining an understanding of the role the device plays in protecting and segmenting UMW's network infrastructure. Once we have gained an understanding of the firewall's role, our process includes the following steps.



SECURANCE APPROACH AND METHODOLOGY

Next-Generation Firewall Assessment (continued)

Next-generation firewalls can also provide several subscription-based services, as illustrated below.



We will evaluate the configuration of any such services used by UMW:

- ▶ Intrusion detection | prevention system
 - Ensure IPS is calibrated appropriately to solely stop intruders and not UMW's actual users
 - Ensure IDS and IPS are placed where they best function in the infrastructure
 - Deploy IDS out of band so it can analyze all traffic and generate intrusion events from suspect or malicious traffic
 - Deploy IPS in the path of traffic so that all traffic must pass through the appliance to continue to its destination, or it can disrupt the connection in the event of malicious intent
 - Configure to block an attack

SECURANCE APPROACH AND METHODOLOGY

Next-Generation Firewall Assessment (continued)

- ▶ VPN
 - Establish another layer of protection to UMW's network
 - Establish connections with network defenders
 - Encrypt your network
- ▶ URL | Content Filtering
 - Ensure filtering is enabled and up to date to safeguard users from online threats through precise control over user access and engagement with Internet content and recognizing patterns indicative of undesirable content
- ▶ Application Control
 - Restrict access to risky applications
 - Follows organizational policies
 - Prioritize, deprioritize, or block traffic to optimize bandwidth
- ▶ Malware Security
 - Ensure anti-malware definitions are updated in real time
 - Includes:
 - Logging
 - Reporting
 - Detection
 - Honeypot files
 - Cyclic redundancy check (CRC)
 - Machine learning behavior analysis
 - Signature-based detection
 - Static file analysis
 - Dynamic malware analysis
 - Application allowlisting

THEIR APPROACH

- ▶ A desktop and administrative review of ruleset.
- ▶ Shallow knowledge of next-generation firewalls as a pillar of zero-trust network architecture.

THE SECURANCE WAY...

- ▶ Incorporates understanding of the role of the firewall and how it is administered.
- ▶ Includes evaluation of more than just firewall rules.
- ▶ Provides consultation on opportunities to optimize the firewall.

....DELIVERS EXTRA VALUE TO YOU.

- ▶ Securance ensures that the firewall serves as an effective first layer of defense configured to prevent unauthorized access or a network breach.

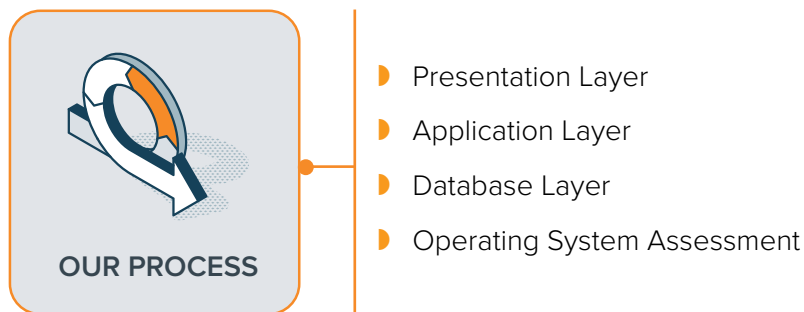


SECURANCE APPROACH AND METHODOLOGY

Enterprise Application Assessment

Securance has conducted enterprise application assessments for clients across all major industries, including UMW's industry, in our 23 years of cybersecurity service. A proper enterprise application integrates computer systems within an organization so all work and core business processes (e.g., sales, accounting, finance, human resources, manufacturing) can be coordinated.

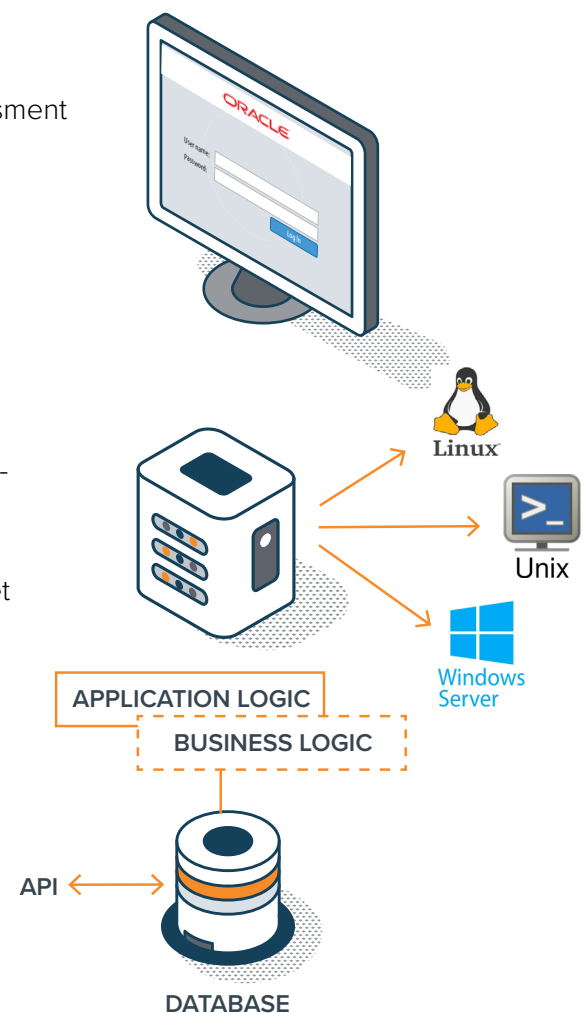
Securance's methodology for assessing overall enterprise application security includes analyzing all layers of the application, including presentation, application business logic, database store, and operating system, as well as the IT general controls that govern UMW's environment.



Presentation Layer

The presentation layer refers to what UMW presents to the world on the Internet or intranet. Keeping this layer separate from others allows the existing interfaces or design to be updated without making any changes to the backend layers. As most current applications are browser-based, either Internet or intranet-facing, our testing approach follows Open Worldwide Application Security Project (OWASP) standards. We will assess UMW's Internet | intranet-facing applications using the following tools with unauthenticated and authenticated testing and manual and automated procedures.

- ▶ Securance may use the following tools to test UMW's presentation layer:
 - Burp Suite
 - NStalker
 - OWASP ZAP
 - Tenable
 - WebInspect



SECURANCE APPROACH AND METHODOLOGY

Enterprise Application Assessment (continued)

Application Layer

The application layer is the layer with which users interact, and serves to exchange information between applications running on other computers.

Securance will work with UMW to ensure that its application is configured effectively to reduce possible risks. If the application is internally developed, we will review its system development methodology to identify any inherent weaknesses in the system development life cycle (SDLC) and project management methodology. We will determine if the application is founded on best practices for coding, and we will ensure that:

- ▶ High-risk functions are restricted to authorized users and reviewed by management.
- ▶ Adequate segregation of duties is established.
- ▶ Application controls are effective.
- ▶ Cross-validation rules are established.
- ▶ Configurable application control and tolerance settings that address risks pertaining to the validity, completeness, and accuracy of master data are properly adjusted.

Database Layer

At the database layer, we will perform an administration and configuration analysis to identify administrative risks and technical vulnerabilities. Securance's methodology for conducting a database-specific security assessment is flexible and built around the unique usage of the application supported by the database. Our approach involves:

- ▶ Assessing the administrative practices supporting the database.
- ▶ Assessing the general controls supporting the database environment.
- ▶ Identifying weaknesses in database design schema, technical vulnerabilities, and entry points through which unauthorized users could gain direct access to the database to extract or insert data.
- ▶ Assessing the system to determine how it may have been affected by any of the discovered database security risks.
- ▶ The database review includes assessments of the following universal database controls, as well as MySQL, Microsoft SQL and Oracle specific controls:
 - Accounts with no password
 - Agent jobs privilege escalation
 - Application-specific DB-related buffer overflows
 - Automated table auditing
 - Blank password
 - Blank password for well-known login
 - Comparisons against industry average and leading practices
 - Console password not set.
 - Database account management
 - Default passwords
 - Default password for well-known login
 - Disabled accounts

SECURANCE APPROACH AND METHODOLOGY

Enterprise Application Assessment (continued)

- Easily guessed passwords
- Easily guessed passwords on sensitive accounts
- Extended stored proc privilege upgrade
- Latest service pack I hot fix not applied
- Look for permissions granted to view the linked table
- Password attack
- Password same as login name
- PL I SQL injection
- Proxy password in secure registry key
- Permissions on sensitive tasks
- Public can create agent jobs
- Several DBCC buffer overflows
- Several parameter buffer overflows
- Slammer I Sapphire Worm
- Temporary stored procedures bypass permissions
- XSTATUS backdoor

Securance may use tools like Application Detective and Tenable, as well as manual procedures, to carry out the database layer assessment.

API Assessment

Application Programming Interfaces (API) act as an intermediary layer that processes data transfers between systems, allowing companies to open their application data and functionality to external third-party developers, business partners, and internal departments within their companies. Our API assessment includes:

- ▶ Evaluating the security of both ends of UMW's API connection.
- ▶ Performing manual manipulation testing.
- ▶ Assessing UMW's data integrity controls.

Operating System Assessment

The operating system is the environment in which an application runs. If not properly patched and updated, it will accrue vulnerabilities and leave application security susceptible to compromise. Our assessment is designed to ensure the organization's servers maintain a stable and secure environment and effective controls and policies to deter both physical and Internet-based malicious attacks.

THEIR APPROACH

- ▶ Includes limited, if any, assessment of database, API, and OS security.

THE SECURANCE WAY...

- ▶ Includes database-specific testing to identify risks.
- ▶ Includes API-specific testing performed to identify data leakage and integrity.
- ▶ Incorporates operating system-specific assessments.

....DELIVERS EXTRA VALUE TO YOU.

- ▶ No risk, threat, or vulnerability is missed.
- ▶ UMW will know exactly how to secure the entire application environment.

SECURANCE APPROACH AND METHODOLOGY

Enterprise Application Assessment (continued)

We will evaluate each server operating system (OS) that hosts a presentation layer, application layer, and database layer for:

- ▶ OS-level vulnerabilities.
- ▶ Configuration aligned with UMW's standards and best practices.
- ▶ The following are included in our operating system analysis:
 - Windows Server Review:
 - 50+ security option settings
 - Account policy (if applicable)
 - Account policy settings (if applicable)
 - Accounts with no password
 - Change | patch management
 - Comparisons against industry average and leading practice
 - Connected servers and workstations
 - Customer-selected registry key values
 - Directory rights and privileges
 - Disabled accounts
 - Discretionary access controls
 - Event logging (if applicable)
 - Group management
 - Group policy objects (GPO) and links
 - Network connections
 - Network shares
 - OS-specific vulnerability management (if applicable)
 - Overall structure
 - RAS dial-in
 - Security updates, patches, and hot fixes
 - Services and drivers installed
 - Trusted and trusting servers
 - User administration
 - User management
 - UNIX | Linux Server Review:
 - Accounts with expired dates
 - All password related settings
 - Change | patch management
 - Comparisons against industry leading practice
 - Current network connections
 - Disabled usernames
 - Discrepancies in password | shadow password files
 - Files with Word writable permissions
 - FTP access
 - Group administrators
 - Groups and group members
 - Guest account management
 - Last logins
 - Login retries
 - Network services enabled
 - OS specific vulnerability management
 - Password shadowing
 - Passwords 30 days or older
 - Permissions on sensitive files and directories
 - Redundant groups and members
 - Rot account management and control
 - SUID and SGID permissions
 - System login script file
 - System search paths
 - System wide security settings
 - Trivial passwords
 - Trusted hosts
 - Use and control of "r" commands
 - Use of Telnet and high-risk protocols
 - User administration
 - Usernames, UIDs, and home directory
 - Users allowed to login remotely
 - Users with administrative status

SECURANCE APPROACH AND METHODOLOGY

Enterprise Application Assessment (continued)

In addition to performing a comprehensive review of the enterprise application, our approach also includes an assessment of the supporting IT general controls.

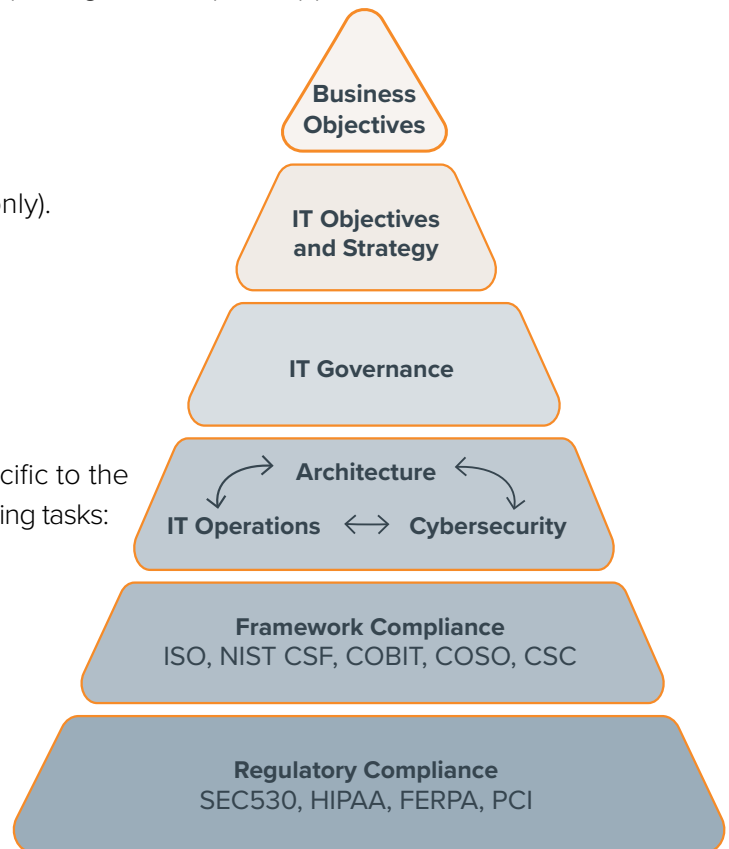
We will assess the IT general controls supporting the application environment and compare them to UMW's preferred framework or the National Institute of Standards and Technology (NIST) framework. The most common IT processes supporting an enterprise application include:

- ▶ Batch job scheduling.
- ▶ Password controls.
- ▶ Patch management.
- ▶ Physical security (on-premises applications only).
- ▶ Program change management.
- ▶ System and data backup.
- ▶ System and data recovery.
- ▶ User provisioning.

Our assessment of these processes will be specific to the target enterprise application and include the following tasks:

- ▶ Obtain and review supporting IT policies, procedures, standards, and guidelines.
- ▶ Interviews with technology administrators and I or IT process owners.
- ▶ Identification of controls stipulated in policy documentation and comparison to UMW's desired control framework(s).
- ▶ Performance of test of design to ensure our understanding of the controls to be tested.
- ▶ Discuss and confirmation of the results of the test of design.
- ▶ Use of IT security and audit tools to perform specialized testing.
- ▶ Online and real-time review of technical configuration settings.
- ▶ Analysis of collected documents, technical reports, and other audit evidence.
- ▶ Sample testing to opine on the operating effectiveness of controls.
- ▶ Completing our issue tracker for all potential findings.
- ▶ Immediate review with UMW's IT staff of any potential finding deemed Urgent or Critical.
- ▶ Discussion and confirmation of potential findings with UMW's IT staff and key stakeholders.

These tasks will complete our Enterprise Application assessment and inform our actionable findings and observations.



SECURANCE APPROACH AND METHODOLOGY

Enterprise Application Assessment (continued)

THEIR APPROACH

- Focuses on the application-specific controls only.

THE SECURANCE WAY...

- Assesses the entire application stack.
- Includes supporting IT general controls.
- Incorporates technical testing where appropriate.

...DELIVERS EXTRA VALUE TO YOU.

- A comprehensive assessment report of every risk and technical vulnerability within the application environment.

(The remainder of this page has been deliberately left blank.)



SECURANCE APPROACH AND METHODOLOGIES

Microsoft File and Print Server Assessment

The server's operating system is the environment in which an application runs. If not properly patched and updated, it will accrue vulnerabilities and leave application security susceptible to compromise. Our assessment is designed to ensure the organization's servers maintain a stable environment and effective controls and policies to deter both physical and Internet-based malicious attacks.



We will evaluate the Windows operating system (OS), including the presentation layer, application layer, and database layer for:

- ▶ OS-level vulnerabilities.
- ▶ Configuration aligned with UMW's standards and best practices.
- ▶ The following are included in our operating system analysis:
 - **Windows Server Review:**
 - 50+ security option settings
 - Account policy (if applicable)
 - Account policy settings (if applicable)
 - Accounts with no password
 - Change I patch management
 - Comparisons against industry average and leading practice
 - Connected servers and workstations
 - Customer-selected registry key values
 - Directory rights and privileges
 - Disabled accounts
 - Discretionary access controls
 - Event logging (if applicable)
 - Group management
 - Group policy objects (GPO) and links
 - Network connections
 - Network shares
 - OS-specific vulnerability management (if applicable)
 - Overall structure
 - RAS dial-in
 - Security updates, patches, and hot fixes
 - Services and drivers installed
 - Trusted and trusting servers
 - User administration
 - User management

THEIR APPROACH

- ▶ Focuses on server-specific controls only.

THE SECURANCE WAY...

- ▶ Assesses the entire server environment and any associated application stack(s).
- ▶ Includes supporting IT general controls.
- ▶ Includes technical testing where appropriate.

....DELIVERS EXTRA VALUE TO YOU.

- ▶ Securance provides comprehensive assessment report of every risk and technical vulnerability within the server environment.

SECURANCE APPROACH AND METHODOLOGIES

Microsoft File and Print Server Assessment (continued)

In addition to performing a comprehensive review of the server OS, our approach also includes an assessment of the supporting IT general controls.

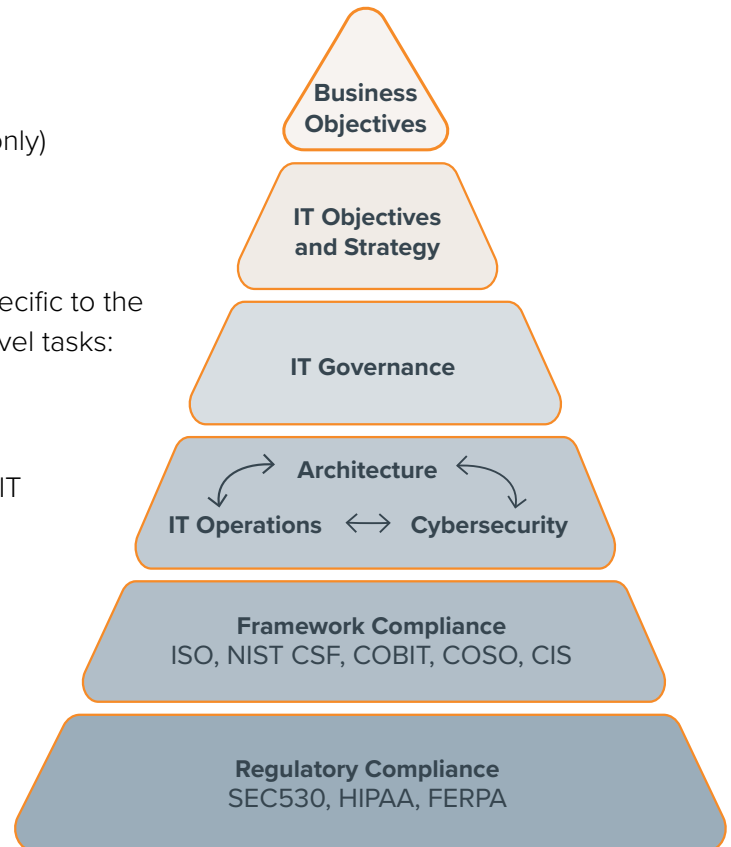
We will assess the IT general controls supporting the server environment and compare them to UMW's preferred framework or the National Institute of Standards and Technology (NIST) framework. The most common IT processes supporting servers include:

- ▶ Password controls
- ▶ Patch management
- ▶ Physical security (on-premise applications only)
- ▶ System recovery
- ▶ User provisioning

Our assessment of these processes will be specific to the target server and include the following high-level tasks:

- ▶ Obtain and review supporting IT policies, procedures, standards, and guidelines.
- ▶ Interview technology administrators and or IT process owners.
- ▶ Identify controls stipulated in policy documentation and compare to UMW's desired control framework(s).
- ▶ Use IT security and audit tools to perform specialized testing.
- ▶ Perform online and real-time review of technical configuration settings.
- ▶ Analyze collected documents, technical reports, and other audit evidence.
- ▶ Complete our Issue Tracker document for all potential findings.
- ▶ Immediately review any potential finding deemed urgent or critical with {RFP Client}'s IT staff.
- ▶ Discuss and confirm potential findings with {RFP Client}'s IT staff and key stakeholders.

These tasks will complete our server assessment and inform our actionable findings and observations.



PROJECT TIMELINE

The table below outlines each step in our IT audit 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 UMW.

IT Auditing Services	Week 1	Week 2	Resources
Kick-off Meeting			Paul Ashe UMW PM
Prepare Client Assistance Memo			SC Consultants
Respond to Client Assistance Request			UMW Staff
Review Client Assistance Request			SC Consultants
External Network Vulnerability Assessment and Penetration Test — Value Add			
Perform information gathering of public information			SC Consultants
Perform vulnerability scanning			SC Consultants
Analyze results to remove false positives			Paul Ashe
Review results of scan with UMW			SC Consultants
Identify hosts to attempt to exploit and confirm with UMW			1 SC Consultants UMW PM
Perform exploit testing			SC Consultants
Extend testing to escalate privileges and move laterally in environment			SC Consultants
Review results with UMW			2 SC Consultants
Active Directory (AD) Assessment			
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 UMW's PM			3 Paul Ashe UMW PM
Core Switch Configuration Review			
Interview device administrator			SC Consultants

PROJECT TIMELINE

IT Auditing Services	Week 2	Week 3	Week 4	Week 5	Resources
Core Switch Configuration Review (continued)					
Analyze device configuration file					SC Consultants
Assess results of analysis					Paul Ashe UMW PM
DNCP DNS Assessment					
Verify scope settings					SC Consultants
Assess performance, availability, and failover					SC Consultants
Evaluate security, logging, and monitoring					SC Consultants
Firewall Configuration Assessment					
Interview firewall administrator					SC Consultants UMW Staff
Analyze firewall configuration					SC Consultants
Assess results of configuration analysis					SC Consultants
Enterprise Application Assessments (Titanium, AMAG, CAD)					
Gain an understanding of the application in scope					SC Consultants
Review system documentation, technical controls, and security practices					SC Consultants
Interview personnel responsible for security of the application					SC Consultants UMW Staff
Test enterprise application controls					SC Consultants
Review the design and operating effectiveness of supporting IT general controls					SC Consultants
TLS WAN Assessment					
Map WAN structure; confirm TLS certificates and protocol version					SC Consultants
Assess performance, load balancing, and failover configurations					SC Consultants
Assess firewall rules, VPN encryption, and access control lists					SC Consultants
Microsoft File and Print Server Assessment					
Assess UMW's build and configuration standards					SC Consultants
Interview system administrator					SC Consultants UMW Staff

PROJECT TIMELINE

IT Auditing Services	Week 5	Week 6	Resources
Microsoft File and Print Server Assessment (continued)	5		
Perform vulnerability scan of the operating system (OS)			SC Consultants
Perform configuration scan and analysis of OS			SC Consultants
Analyze results of scanning			SC Consultants
Review results with system administrator			Paul Ashe UMW Staff
Draft Management Report		6	SC Consultants
Review Management Report with UMW's Key Stakeholders			Paul Ashe UMW Stakeholders
Review Final Report and Hold Exit Conference			Paul Ashe UMW PM

PROJECT MANAGEMENT

Securance is dedicated to performing the audits 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:




**CLICK
ON THUMBNAIL
TO VIEW THE
STATUS REPORT**

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 UMW. 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 UMW and Securance.
- ▶ **Work Plan:** Within one week of receiving the notice to proceed, Securance will submit a detailed work plan for UMW'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, UMW'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.



SECURANCE
CONSULTING

Advantage
Insight AI

Status Report

ABC University

IT Security Audit

Project Detail

Project Manager

Paul Ashe – Securance (paula@securanceconsulting.com)

Project Manager

John Doe, IT Manager (jdoe@ABC_University.gov)

Reporting Weekend

Thursday, July 26, 2025

Project Due Date

December 15, 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 Completed
Phase I Project Tasks Schedule			
1. IT Security Policies, Practices, and Procedures Review	Completed	100%	100%
2. VA: Internal Network	Completed	100%	100%
3. VA: External Network	Completed	100%	100%
4. VA: Wireless Network (price for 4 controllers)	Completed	100%	100%
5. VA: Host-Based Security: Operating System	Ongoing		
6. VA: Host-Based Security: Virtual Host Servers			
7. VA: Host-Based Security: Database System	Ongoing		
8. VA: Web Application Testing (price for sample of 10 applications)	Completed	100%	100%

PROJECT MANAGEMENT



Shared Tasks

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

- ▶ **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 UMW's IT environment.

These factors will be looked at as a whole and discussed with AMS 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 AMS. The use of this tracker helps to avoid unwanted surprises and I or disputes over findings.

- ▶ **Continuous Improvement:** We will invite UMW employees to shadow our consultants as they execute technical engagements. Additionally, to ensure continuous improvement of UMW'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 23 years of experience conducting more than 3,000 IT audits, delivering project success on time and on budget.

UMW RESOURCES NEEDED TO COMPLETE THE PROJECT

When a contract or statement of work is executed, there are specific items Securance will need to perform the project. To ensure that UMW gets 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 UMW'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 UMW staff
- ▶ Access to technical staff (if needed) during the length of the technical testing (very little time needed)
- ▶ Access to staff who have been identified for interviews during the length of the project (approximately one hour each)
- ▶ Immediate access on a part-time basis to a cybersecurity staff member who can assist with questions (if needed)

Logical and Other Access Requests

- ▶ IP addresses relevant to the project (external and internal network penetration testing only)
- ▶ User IDs and passwords for web applications | operating systems (if needed)
- ▶ Authority to access network components and operating systems (if needed)

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

Rules of Engagement Memo (for vulnerability assessments and penetration testing only; please see an example on pages 44–45)

Office Space for On-Site Work (As Needed)

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

UMW RESOURCES NEEDED TO COMPLETE THE PROJECT

Securance Consulting

2024 University of Mary Washington Client Assistance Request

Location:

No.	Phase I	Request 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.	
11	External Network	Please provide all available network diagrams. The more detailed the better.	
23	Firewall	Please provide the brand, version and firmware version of the firewalls to be assessed.	
24	Firewall	Please provide the contact information for the firewall administrator.	
25	Firewall	Please provide copies of the firewall config files.	
26	Router	Please provide the brand, version and firmware version of the routers/switches to be assessed.	
27	Router	Please provide the contact information for the router/switch administrator. This is typically the network engineer.	
28	Router	Please provide copies of the router/switch configuration files.	

UMW RESOURCES NEEDED TO COMPLETE THE PROJECT



MEMORANDUM

DATE: UMW_____ (version 1.0)
TO: [RFP Client's Project Management]
FROM: Securance LLC
RE: Security Assessment Rules of Engagement (RoE) - SAMPLE

This memo represents the mutually agreed upon RoE for the upcoming network security assessment.

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

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	
o Project Manager Name	
o Project Manager Email Address	
o Project Manager Mobile Phone	
o Project Manager Office/Lab Phone	
20. Security Engineer Contact Information	
o Consultant Name	
o Consultant Email Address	
o Consultant Mobile Phone	
o Consultant Office/Lab Phone	

By: _____ Title: _____
Securance: Please Sign Please Type

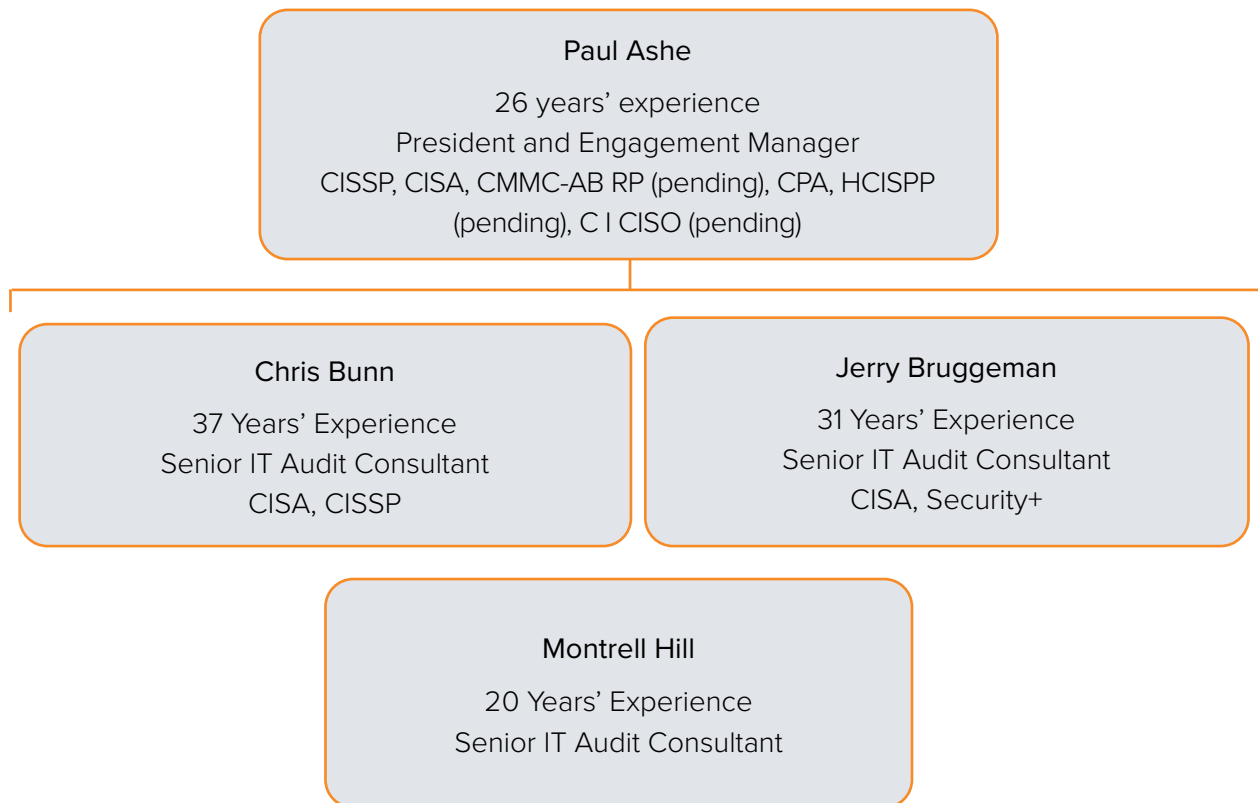
Name: _____ Date: _____
Please Type Please Type

By: _____ Title: _____
Client Project Manager: Please Sign Please Type

Name: _____ Date: _____
Please Type Please Type

SECURANCE'S DEDICATED PROJECT TEAM

The expertise and experience of the key personnel listed below align with UMW's scope of work and requirements. If any of these consultants are unavailable when work starts, Securance will propose an equally experienced substitute for approval. Securance only employs senior-level consultants; no junior-level consultants will be assigned to UMW's project.



SECURANCE'S DEDICATED PROJECT TEAM

Resumes — Key Personnel

PAUL ASHE

27 YEARS OF IT AUDIT 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 23 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 IT audits, reviews, and technology-specific vulnerability assessments and penetration tests for clients in nearly every industry and is an expert in implementing and assessing security frameworks.

RELEVANT EXPERIENCE

- ▶ Active Directory Reviews
- ▶ Computer-Aided Dispatch (CAD) System Reviews
- ▶ DNCP | DNS Reviews
- ▶ Enterprise | Web Application Testing
- ▶ Firewall | Router Configuration Reviews
- ▶ Identity and Access Management Reviews
- ▶ Internal | External | Wireless Network Security
- ▶ IT Governance
- ▶ Project Management
- ▶ TLS | WAN Reviews
- ▶ Vulnerability Assessments

RELEVANT EXPERTISE

- ▶ **Project Management:** Paul has led Securance engagements from kick-off to final report for 23 years.
- ▶ **IT Security Audits:** Paul helps clients identify technical and operational risks and vulnerabilities, develops prioritized remediation recommendations, and guides organizations to focus their resources in the right areas and make informed decisions about IT risk management.
- ▶ **Data Security:** Paul is skilled in helping organizations protect the confidentiality, integrity, and availability of their critical data.

SECURANCE'S DEDICATED PROJECT TEAM

Resumes — Key Personnel (continued)

RELEVANT ACHIEVEMENTS

- ▶ **Atlanta Public Schools** Identified opportunities to improve the configurations of application and database technologies and provided actionable recommendations; created an audit plan that prioritizes and informs the scope of future IT audit activities.
- ▶ **City and County of San Francisco** Conducted IT security audits including network penetration testing, supplier portal testing, and web application security assessments.
- ▶ **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 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 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.
- ▶ **Georgia Institute of Technology (Georgia Tech)** Performed vulnerability assessments of the University's external network and web applications and delivered a detailed remediation roadmap.
- ▶ **Henrico County Public Schools** identified critical vulnerabilities in the internal network and validated the need for continuing security awareness training.
- ▶ **Matanuska-Susitna Borough** Helped identify vulnerabilities within firewall, router | switch, and server configurations; reviewed domain and enterprise application security administration; assessed logging and monitoring processes; assessed security tool feature configuration for multiple technologies.
- ▶ **Radford University** Strengthened the University's security posture by identifying vulnerabilities in its firewall configuration and recommending the implementation of an on-premises security operations center.
- ▶ **Riverside University Health System** Reduced vulnerabilities within the internal network, web application, operating system, and databases and developed a remediation plan that prioritized risks, estimated costs, timelines, and resources needed to attain full HIPAA compliance.
- ▶ **Rowan University** Validated the overall security of the University's network architecture and identified physical security and the need for router | switch firmware updates as potential risks.

SECURANCE'S DEDICATED PROJECT TEAM

Resumes — Key Personnel (continued)

CHRIS BUNN

37 YEARS OF IT AUDIT EXPERIENCE

Senior IT Audit Consultant | Securance Consulting



EDUCATION

Master of Science

Management Information Systems

Bachelor of Science

Computer Science for Business

PROFESSIONAL CREDENTIALS

- ▶ Certified Information Systems Security Professional (CISSP)
- ▶ Certified Information Systems Auditor (CISA)

Chris is an expert in IT assessments, from best-practice standards to cloud security reviews. His expertise in evaluating security, assessing and remediating potential threats, and resolving issues caused by internal and external cyber attacks has benefited numerous educational institutions and other government entities.

RELEVANT EXPERIENCE

- ▶ Computer-Aided Dispatch (CAD) System Reviews
- ▶ Data | Information Security
- ▶ Enterprise Application Assessments
- ▶ IT Audits
- ▶ IT Governance
- ▶ Microsoft File and Print Server Reviews
- ▶ Network Device Security Reviews
- ▶ Process and Practice Improvement
- ▶ Vulnerability Assessments and Penetration Testing

RELEVANT EXPERTISE

- ▶ **Network Device Security:** Chris excels at identifying and exploiting vulnerabilities in networks, routers, switches, and firewalls and providing actionable remediation recommendations to address each specific vulnerability.
- ▶ **Enterprise Application Assessments:** Chris evaluates student management software and other enterprise applications for security compliance, performance, and alignment with business needs, helping organizations optimize their IT operations and minimize risks.

SECURANCE'S DEDICATED PROJECT TEAM

Resumes — Key Personnel (continued)

RELEVANT ACHIEVEMENTS

- ▶ **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** Delivered detailed mapping to the HIPAA Privacy, Security, and Breach Notification Rule code sections and provided actionable recommendations to help the City avoid civil penalties.
- ▶ **City of Pasadena** Analyzed each specific IT operation and process by NIST CSF function, category, sub-category, and tier and provided a roadmap with detailed recommendations to improve the City's IT security and control posture.
- ▶ **City of Peoria** Identified financial exposure related to data loss and developed a three-year audit program and roadmap for long-term improvement
- ▶ **City of Phoenix** In addition to identifying and helping to remediate vulnerabilities in the City's networks, servers, databases, firewalls, and routers, secured funding for a 24 | 7 | 365 security operations center.
- ▶ **Colorado Department of Human Services** Provided a detailed remediation roadmap to expediently attain full compliance with HIPAA; recommended they maintain their covered entity status and sign BAAs with all county-level social and human service departments.
- ▶ **North Dakota Public Employee Retirement System** Identified medium-risk vulnerabilities and offered actionable remediation recommendations, including the implementation of a program management policy to solidify program change policies.
- ▶ **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.
- ▶ **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.
- ▶ **University at Buffalo** Improved the operating effectiveness of critical IT processes, including change management, user provisioning, physical and environmental security, disaster recovery, data backups, and security awareness training to prepare the organization for HIPAA compliance.
- ▶ **Village of Niles** Initiated development of policies, SOPs, cross-training, and a technology steering committee and reduced key person risk by matching staff to appropriate tasks.
- ▶ **Village of Orland Park** Mapped assessment findings to CJIS requirements and NIST CSF controls and then streamlined IT operations by improving the Village's governance documentation.
- ▶ **Washington State Investment Board** Reduced key-person risk by 90 percent and reduced financial exposure from non-compliance with State Office of the CIO's policies.

SECURANCE'S DEDICATED PROJECT TEAM

Resumes — Key Personnel (continued)

PRIOR ACHIEVEMENTS

- ▶ **East West Bank** | 2012 | Senior Information Security Consultant | Responsible for execution of compliance and risk management projects within the Information Security department of the IT division; developed an IT risk management framework for national and international operations; developed and implemented IT policies and procedures, vendor risk management program, and daily monitoring procedures of critical and high-risk applications and platforms.
- ▶ **Experis Finance/Accretive Solution** | 2006–2011 | Senior Risk Advisory Services Consultant | Managed and executed IT audits for various organizations across industries. Audit topics included regulatory compliance, data governance, general computer controls, business continuity, enterprise application controls and security, and process improvement.
- ▶ **University of Florida** | 2005–2006 | IT Audit Manager | Planned, supervised, and conducted audits of enterprise applications, data warehouse and reporting systems, financial systems, operations, advisory services, and other projects undertaken by the Office of Audit and Compliance Review; supervised and performed HIPAA compliance audits.
- ▶ **BDO Seidman LLP** | 2003–2005 | IT Audit Manager | Member of the BridgeMark risk consulting and advisory services practice; responsible for SAP business intelligence (BI) and governance | risk | compliance advisory services for mySAP ERP with NetWeaver, PeopleSoft, and other service-oriented architecture ERP systems; responsible for project management in technology risk and security, business process improvement, BI and advanced analytics, regulatory compliance, and internal IT audits.
- ▶ **Computer Sciences Corporation** | 2000–2003 | IT Audit Supervisor | Responsible for the management and execution of service organization (SOC Type II), compliance, internal information system, and pre- and post-implementation audits.
- ▶ **Ernst & Young LLP** | 1997–2000 | IT Audit Manager | Member of Information Systems Assurance and Advisory Services (ISAAS) practice; responsible for service organization, general computer controls, IT process reviews, information security engagements, application control consulting, and internal IT audits.
- ▶ **Lockheed Martin** | 1994–1997 | IT Audit Supervisor | Performed risk-focused audits of enterprise applications and platforms, system implementations, the enterprise network, engineering online security, and eCommerce security.
- ▶ **SunTrust Bank** | 1987–1994 | IT Audit Supervisor | Responsible for audits of computer operations, networks, information security policies, enterprise applications, and telecommunications.
- ▶ **Blue Cross and Blue Shield of Florida** | 1984–1987 Senior IT Auditor | Supervised reviews of information systems and controls.

SECURANCE'S DEDICATED PROJECT TEAM

Resumes — Key Personnel (continued)

JERRY BRUGGEMAN

32 YEARS OF IT AUDIT EXPERIENCE

Senior IT Audit 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, networking, IT administration, and IT security. He has helped create and maintain robust information security programs for large organizations in both the private and public sectors, including the U.S. military. Jerry has significant experience conducting internal audits and technical testing for educational institutions and other government organizations.

RELEVANT EXPERIENCE

- ▶ Active Directory Reviews
- ▶ Cybersecurity Assessment
- ▶ Database Assessments
- ▶ DNCP | DNS Reviews
- ▶ Enterprise and Web Application Security
- ▶ Firewall and IDS | IPS Deployment
- ▶ IT Audits
- ▶ Microsoft File and Print Server Reviews
- ▶ Network Assessments, e.g., Internal | External | Wireless
- ▶ TLS | WAN Reviews
- ▶ Vulnerability Assessments and Penetration Testing

RELEVANT EXPERTISE

- ▶ **Vulnerability Assessments | Penetration Testing:** Jerry is an ethical hacker with a passion for penetration testing, cyber security, and information security. His exceptional ability to think like a hacker and probe for security vulnerabilities helps organizations enhance their security postures and protect against potential threats.
- ▶ **Enterprise Application Assessments:** Jerry is an expert in evaluating all aspects of an application's environment, from the presentation layer to the supporting IT general controls. He enhances the reliability of applications and protects organizations by helping to prevent unauthorized access, data leaks, DDoS and injection attacks, ransomware, and other security risks.

SECURANCE'S DEDICATED PROJECT TEAM

Resumes — Key Personnel (continued)

RELEVANT ACHIEVEMENTS WITH SECURANCE

- ▶ **Albemarle County** Provided Cybersecurity as a Service (CSaaS) consulting to the county on an as needed basis.
- ▶ **Atlanta Public Schools** Performed a database security audit; reviewed a Microsoft SQL cluster.
- ▶ **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.
- ▶ **Lea County** Reviewed critical IT governance documents including incident response and disaster recovery plans, and assessed IT service and staffing performance against best practices, and lead the remediation of technical vulnerabilities.
- ▶ **Milwaukee Metropolitan Sewerage District** Conducted network penetration tests.
- ▶ **Newport News Public Schools** Performed vulnerability assessment and penetration testing.
- ▶ **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.
- ▶ **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.

SECURANCE'S DEDICATED PROJECT TEAM

Resumes — Key Personnel (continued)

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.
- ▶ **U.S. Air Force Weather Agency** | 2002–2005 | Lead Infrastructure /Information Assurance Technician | Led and trained team responsible for administering and managing the weather network.

SECURANCE'S DEDICATED PROJECT TEAM

Resumes — Key Personnel (continued)

MONTRELL HILL

20 YEARS OF IT AUDIT EXPERIENCE

Senior IT Audit Consultant | Securance Consulting



EDUCATION

Bachelor of Science

Business Computer Information
Systems

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

RELEVANT EXPERIENCE

- ▶ Cybersecurity
- ▶ Database Security
- ▶ External | Internal Vulnerability Assessments and Penetration Testing
- ▶ Firewall Configuration Reviews
- ▶ Identity and Access Management Reviews
- ▶ IT Audits
- ▶ Network Security
- ▶ Router | Switch Configuration Reviews

RELEVANT EXPERTISE

- ▶ **Network Security:** Montrell excels at identifying and exploiting vulnerabilities in networks, routers, switches, and firewalls.
- ▶ **IT Audits:** Montrell is an expert at assessing the security of organizations' IT architectures and the supporting policies and procedures. He provides objective assessments of the effectiveness of an organization's risk management, processes, and governance.

SECURANCE'S DEDICATED PROJECT TEAM

Resumes — Key Personnel (continued)

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 for improving the overall efficiency and performance of the 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.

REFERENCES

Securance has decades of experience providing UMW's requested services. Below is the contact information of three clients for which Securance has recently performed similar projects. We encourage UMW 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
Radford University	Dawnetta (Dawn) L. Taylor, Audit Manager dtaylor96@radford.edu	- IT security auditing and network assessments - Data center audit (Please see the case study on page 8.)
City of Richmond	Rochelle Carter, Management Analyst Rochelle.Carter@rva.gov 804.646.5632	- Enterprise application security review - Network device configuration reviews - Network vulnerability assessments - Phishing campaign security awareness training - Cybersecurity assessment (Please see the case study on page 9.)
Henrico County Public Schools	Michael Gillespie mgillespie@henrico.k12.va.us 804.328.5200 ext. 85426	- Cybersecurity as a Service (CSaaS) - Firewall configuration review - Internal network vulnerability assessment and penetration testing - Social engineering testing - Wireless network review (Please see the case study on page 10.)

PROPOSED FEES

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

Project Scope Item	Line Item Fee
Active Directory Assessment	\$3,168
Core Switch Configuration Review (2 switches)	\$2,112
DHCP DNS Assessment	\$1,584
Firewall Configuration Review (Fortinet —2 firewalls)	\$3,168
TLS WAN Assessment	\$2,112
Microsoft File and Print Server Review	\$3,168
Titanium Assessment	\$11,880
AMAG Assessment	\$9,240
CAD Assessment	\$9,240
Internet Security Review (External Network Vulnerability Assessment and Penetration Test) — Value Add	~~\$3,168~~
Status Reporting — Value Add	~~\$3,168~~
Project Management — Value Add	~~\$1,584~~
Subtotal	\$56,760
Value Add Price Reduction	~~\$7,920~~
Total	\$48,840

**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 UMW will **NOT** be billed for expenses such as mileage, meals, and incidentals.

PROPOSED FEES

To provide UMW 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 effort will be less than proposed. This could result in significant savings to UMW.
- ▶ 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 UMW.
- ▶ UMW'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 UMW personnel, or unavailability of documentation occur, Securance will determine their effect on the engagement scope, timing, and fees and promptly notify UMW of any such changes. Securance will not proceed with any changes or additions to the scope of work without UMW's explicit written approval.

Hourly Rate

Securance's cost proposal is based on an hourly rate of \$132, 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.

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.

PROPOSED FEES

For Securance, this is not just another project. It is an opportunity to help your team solve problems, exceed your goals, and pursue our mutual passion for UMW's long-term success.

After reviewing your needs and taking the time to understand your organization, we believe we are the best fit for this opportunity, and **we want to partner with you!**

We are offering the following free value adds as one way to demonstrate our desire to work with you and the lasting value brought by the Securance advantage.

Deliverable	Value
Internet Security Review (External Network Vulnerability Assessment Penetration Test)	In order to demonstrate our commitment to UMW, we will provide a vulnerability assessment and penetration test of the external network at no additional cost. For more information, please see our methodology beginning on page 14.
Project Management	At no additional charge, we will oversee the progress of the City's project from beginning to end. Our proven project management methodology has been used successfully for organizations across the country.
Status Reporting	Securance recognizes the importance of ongoing communication with the City. To guarantee that work remains on schedule and that all potential issues are quickly addressed, we will issue biweekly status reports and review them with the City during status meetings.

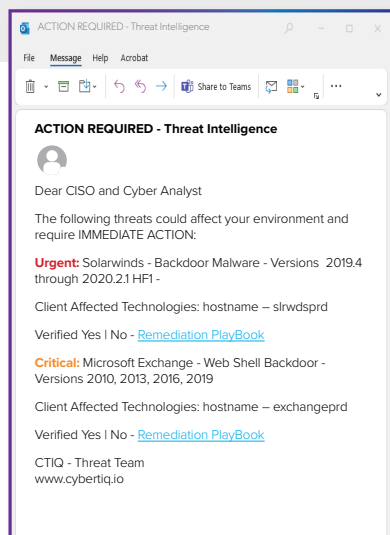
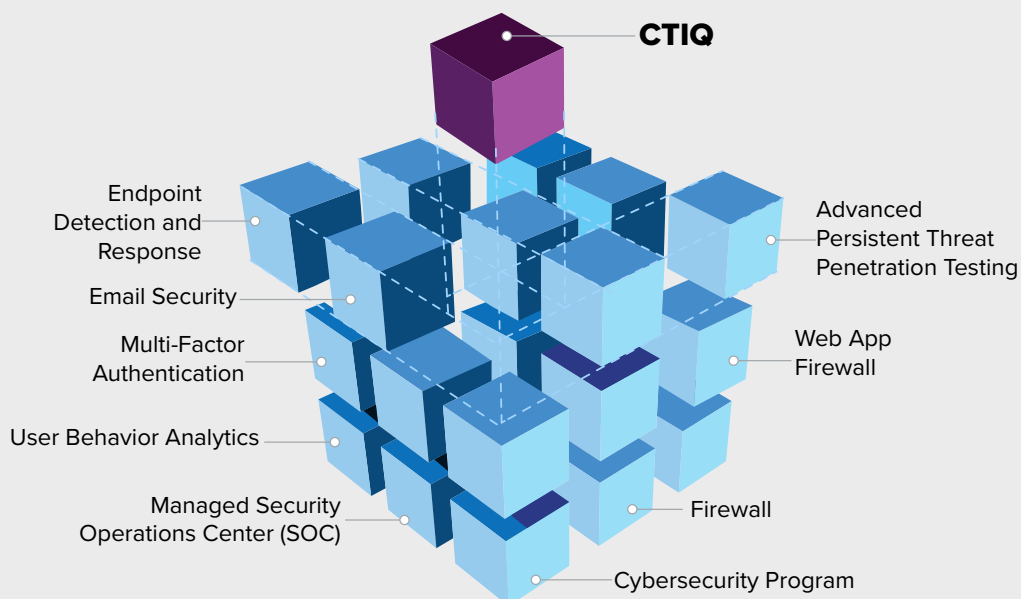
If you have questions or would like additional information, do not hesitate to contact us. We want to make sure you have everything you need to make your decision.

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

THE GROWING CHALLENGE IN CYBERSECURITY



REVOLUTIONIZE YOUR CYBER DEFENSE WITH AI-POWERED INTELLIGENCE



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



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