JAMES MADISON UNIVERSITY

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No. **UCPJMU7141**

This contract entered into this 25th day of March 2025, by Assura, Inc., hereinafter called the "Contractor" and Commonwealth of Virginia, James Madison University called the "Purchasing Agency".

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

SCOPE OF CONTRACT: The Contractor shall provide the services to the Purchasing Agency as set forth in the Contract Documents.

PERIOD OF PERFORMANCE: From April 1, 2025 through March 30, 2026 with nine (9) one-year renewal options.

The contract documents shall consist of:

(1) This signed form;

(2) The following portions of the Request for Proposal FDC-1220 dated December 17, 2024:
- (a) The Statement of Needs,
- (b) The General Terms and Conditions,
- (c) The Special Terms and Conditions together with any negotiated modifications of those Special Conditions;
- (d) Addendum One, dated January 10, 2025;
- (e) Addendum Two, dated January 16, 2025.

(3) The Contractor's Proposal dated January 30, 2025 and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
- (a) Negotiations Summary, dated March 17, 2025.

IN WITNESS WHEREOF, the parties have caused this Contract to be duly executed intending to be bound thereby.

CONTRACTOR:	PURCHASING AGENCY:
By: _____ (Signature)	By: _____ (Signature)
Karen L. Cole (Printed Name)	Doug Chester (Printed Name)
Title: Chief Executive Officer	Title: Buyer Senior

Rev. 5/12/21

JAMES MADISON UNIVERSITY

RFP # FDC-1220
Information Technology Security Auditing Services
Negotiation Summary for Assura, Inc.
March 17, 2025

1. Parties agree that items within this Negotiation Summary modify RFP #FDC-1220 and the Contractor's response to RFP #FDC-1220 and that this Negotiation Summary takes precedence in conflict.

2. Contractor agrees that all exceptions taken within their initial response to RFP #FDC-1220 that are not specifically addressed within this negotiation are null and void.

3. The pricing schedule is as follows:

Pricing for Auditing Services	Off-site	On-site*
External Vulnerability Scanning	$203.06	$221.11
Wireless Network Assessment	$203.06	$221.11
Firewall and Router Security Assessment	$338.44	$361.00
Server Configurations Assessment	$338.44	$361.00
Database Architecture Security Assessment	$338.44	$361.00
Network Scanning Process Assessment	$203.06	$221.11
Web Application Security Assessment	$338.44	$361.00
Active Directory Security Assessment	$338.44	$361.00
Penetration Testing	$203.06	$221.11
Telecommunications	$338.44	$361.00
(flat fee hourly rate that includes all billables/travel)		

4. The University may also request that these services be provided as a fixed-fee project, as would be mutually agreed to prior to services being rendered, with deliverables billed upon completion of milestones.

5. The University may also request that these services be provided as a monthly subscription service, as would be mutually agreed to prior to services being rendered, with deliverables determined by monthly service requirements.

6. Contractor has disclosed all potential fees. Additional charges will not be accepted without mutual written agreement between parties, e.g., contract modification and/or change order.

James Madison University
Information Technology Security Auditing Services
RFP# FDC-1220
January 30, 2025

Proposal Submitted To:

Doug Chester, Buyer Senior
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Building
Harrisonburg, VA 22807
www.jmu.edu

Contact: Karen Cole, CISA, CRISC, CBCP, MBCI
Email: karen.cole@assurainc.com
Phone: (804) 767-4521

PREPARED BY

ASSURA®

Cybersecurity uncompromised.

ASSURA, INC. | 7330 STAPLES MILL ROAD | #292 | RICHMOND, VA | 23228

ASSURAINC.COM

Cybersecurity uncompromised.

7330 Staples Mill Road, Suite 292
Richmond, VA 23228
Telephone: 804-672-8714
Toll Free: 855-9NOHACK

January 30, 2025

Mr. Doug Chester, Buyer Senior
Commonwealth of Virginia
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Building
First Floor, Suite 1023
Harrisonburg, VA 22807

RE: Request for Proposal # FDC-1220 Information Technology Security Auditing Services

Mr. Chester,

We appreciate the opportunity to submit our response to RFP #FDC-1220 for Information Technology Security Auditing Services. Having had the privilege of working with James Madison University (JMU) for over the past six years, we value the trust you have placed in us to deliver outstanding cybersecurity services. We are excited about the potential to continue supporting JMU and other Virginia Association of State and College University Purchasing Professionals (VASCUPP) organizations in their mission to proactively identify and mitigate security vulnerabilities.

JMU's commitment to robust security practices, as reflected by the efforts of the Audit and Management Services (AMS) and this RFP, underscores a dedication to protecting critical systems and data. We share this commitment and bring a proven track record of industry expertise and tailored solutions to support your organization's evolving needs.

Our proposal highlights the exceptional capabilities and value we have consistently delivered to JMU, along with the expertise we can bring to other VASCUPP institutions. Thank you for considering our submission, and we look forward to the opportunity to continue to build on our strong partnership in protecting educational and government organizations!

If you have any questions or if I may be of assistance, please do not hesitate to contact me at (804) 767-4521 or karen.cole@assurainc.com

Sincerely,

Karen L. Cole
CEO

TABLE OF CONTENTS

1.0 RFP ACKNOWLEDGEMENTS

REQUEST FOR PROPOSAL

RFP# FDC-1220

Issue Date: December 17, 2024
Title: Information Technology Security Auditing Services
Issuing Agency: Commonwealth of Virginia
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Building
First Floor, Suite 1023
Harrisonburg, VA 22807

Period of Contract: From Date of Award Through One Year (Renewable)

Sealed Proposals Will Be Received Until 2:00 PM on January 30, 2025 for Furnishing The Services Described Herein. (See Special Terms & Conditions "D. Late Proposals")

SEALED PROPOSALS MAY BE MAILED, EXPRESS MAILED, SUBMITTED IN eVA OR HAND DELIVERED DIRECTLY TO THE ISSUING AGENCY SHOWN ABOVE.

All Inquiries For Information And Clarification Should Be Directed To: Doug Chester, Buyer Senior, Procurement Services, chestefd@jmu.edu; 540-568-4272; (Fax) 540-568-7935 not later than five business days before the proposal closing date.

NOTE: THE SIGNED PROPOSAL AND ALL ATTACHMENTS SHALL BE RETURNED.

In compliance with this Request for Proposal and to all the conditions imposed herein, the undersigned offers and agrees to furnish the goods/services in accordance with the attached signed proposal or as mutually agreed upon by subsequent negotiation.

Name and Address of Firm:

7330 Staples Mill Road

#292

Richmond, VA 23228

By: DocuSigned by: Karen Cole 52AE0F655128412... *(Signature)*

Name: Karen L. Cole *(Please Print)*

Date: January 30, 2025

Title: Chief Executive Officer

Web Address: www.assurainc.com

Phone: 804-767-4521

Email: Karen.cole@assurainc.com

Fax #: 804-672-6442

ACKNOWLEDGE RECEIPT OF ADDENDUM: #1 DS kl #2 DS kl #3____ #4____ #5____ (please initial)

SMALL, WOMAN OR MINORITY OWNED BUSINESS:

☑ YES; ☐ NO; *IF YES* ⇒⇒ ☑ SMALL; ☑ WOMAN; ☐ MINORITY ***IF MINORITY:*** ☐ AA; ☐ HA; ☐ AsA; ☐ NW; ☑ Micro

Note: This public body does not discriminate against faith-based organizations in accordance with the *Code of Virginia*, § 2.2-4343.1 or against an offeror because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment.

Rev. 9/2/2024

2.0 MAPPING OF RFP REQUIREMENTS

Section	Section Title	RFP Section V Mapping and Description	Proposal Page Number
1	RFP Acknowledgements	• Maps to V.B.1 • RFP Cover Sheet and All Addenda Acknowledgements	3
3	Goods and Services Plan and Methodology	• Maps to V.B.2 • Response to Statement of Needs	5
4	Firm Overview and Qualifications	• Maps to V.B.3 • Response to Expertise, Qualifications, and Experience of Firm • Resumes of Key Personnel	33
5	Offeror Data Sheet	• Maps to V.B.4 • Attachment A from RFP	37
6	Small Business Subcontracting Plan	• Maps to V.B.5 • Assura SWaM Certification	38
7	VASCUPP Sales	• Maps to V.B.6 •	40
8	Proposed Cost	• Maps to V.B.7 • Pricing Schedule	41
9	Additional Information	• Maps to V.A.3.C • Additional Material	43

3.0 GOODS AND SERVICES PLAN AND METHODOLOGY

James Madison University (JMU) continues to exemplify excellence in higher education, as evidenced by its significant rise in national rankings. In the latest report by The Wall Street Journal, JMU climbed 82 spots to secure the No. 70 position among the best colleges in the United States. This ascent reflects the University's dedication to providing exceptional learning opportunities, career preparation, and character development.

In the realm of cybersecurity, JMU has been a pioneer since being recognized as one of the original seven National INFOSEC Education and Training Program centers in the United States. This prestigious designation by the National Security Agency and the Department of Homeland Security honors universities that demonstrate academic excellence in information assurance education. Building on this legacy, JMU's 100% online Master's in Computer Science with a concentration in Cybersecurity is ranked among the best online graduate programs in the nation. Designed for working professionals, this highly technical program is one of the most comprehensive in the country.

JMU's forward-thinking approach is further demonstrated by its development of statewide contract vehicles that streamline the procurement of cybersecurity services for members of the Virginia Association of State College and University Purchasing Professionals (VASCUPP) and other government entities. These initiatives underscore JMU's commitment to safeguarding not only its own students, staff, sensitive data, and critical systems but also those of its colleagues across Virginia.

Assura is pleased to provide this response to RFP# FDC-1220 Information Technology Security Auditing Services, demonstrating our unparalleled knowledge in delivering security assessment and testing services, superior work quality, outstanding results, and reasonably priced options to meet all of JMU and VASCUPP's security audit needs.

Statement of Needs

Assura is proud to bring a team of experienced and highly certified professionals to meet the cybersecurity needs of JMU and VASCUPP members. Since our founding in 2007, Assura has built a reputation for delivering exceptional security assessment and testing services to Virginia government agencies and institutions of higher education. Our commitment to excellence is reflected in our practice of engaging only certified personnel with credentials tailored to the specific work being performed. These certifications include the following and many others:

- **CISSP** – Certified Information Systems Security Professional (ISACA)
- **CISM** – Certified Information Security Manager (ISACA)
- **CISA** – Certified Information Systems Auditor (ISACA)
- **CEH** – Certified Ethical Hacker (EC-Council)
- **CRISC** – Certified in Risk and Information Systems Control
- **Security+** – Security Certification (CompTIA)

What sets Assura apart is our unwavering commitment to excellence. We are the only firm to offer **AuditArmor® Guarantee** and **AuditArmor® Audit Defense,** provide assurances that reduce risk and ensure peace of mind:

- **AuditArmor® Guarantee** is our 100% guarantee that all work we deliver is fully compliant with identified standards and regulations and will withstand the scrutiny of any audit. If any aspect of our work is deemed noncompliant, we fix it at no cost.
- **AuditArmor® Audit Defense** ensures that we will work directly with auditors and regulators to defend the integrity of our work and prevent unwarranted findings—at no additional cost for services we have provided.

At Assura, we believe that selecting a cybersecurity partner should be the least risky part of securing your systems. With a proven track record, unmatched expertise, and innovative guarantees, we stand ready to deliver results that exceed expectations while protecting your organization from unnecessary risks.

The remainder of this section details how Assura's services address the needs of JMU and VASCUPP members.

3.1 C.1.A: EXTERNAL VULNERABILITY ASSESSMENT

Cybercriminals are relentless, constantly scanning for **unpatched security flaws and weak system configurations** to exploit. Is the organization staying one step ahead? Vulnerability assessments answer this common question.

At Assura, we don't just **find vulnerabilities**—we **prioritize and remediate them before attackers can exploit them.** Through our **one-time vulnerability assessments** or our **Vulnerability Management-as-a-Service (VMaaS)**, we take a **risk-based approach** to protecting your organization, ensuring that **critical security weaknesses are identified, analyzed, and addressed with expert guidance.**

Our **VMaaS solution** goes beyond traditional scanning. Each client is assigned a **dedicated service concierge** from our **Offensive Security Operations (OSO) team**, providing:

- ☑ **Continuous vulnerability scanning** across your entire infrastructure.
- ☑ **In-depth reports** with clear explanations of findings.
- ☑ **Monthly strategy calls** to review trends and prioritize fixes based on real-world attack risks.
- ☑ **The "attacker's eye view"** of your environment, ensuring you see what cybercriminals see.

With support for leading security tools like **Tenable Vulnerability Management, Veracode, Snyk, Acunetix, and Burp Suite Pro**, Assura's service covers **everything from device and application discovery to compliance scoring and software misconfigurations**.

We **seamlessly integrate with your IT and DevSecOps workflows**, leveraging **Nucleus**, a **cloud-based vulnerability intelligence platform** powered by **Mandiant threat intelligence**. This ensures:

- **Automated prioritization** of vulnerabilities based on risk level and business impact.
- **Real-time alerts** to IT teams for critical security gaps.
- **A single-pane-of-glass dashboard** for full visibility into vulnerability management.

Our **OSO Concierge Team** works hand-in-hand with your security and IT operations teams to **configure workflows, train staff, and ensure seamless integration with existing security processes**.

Our detailed approach is listed below.

One of the most common means that threat actors use to compromise an organization's security is taking advantage of systems with lingering security flaws and weak configurations. Through either a one-time vulnerability assessment or with Assura's Vulnerability Management-as-a-Service (VmaaS), we take a risk-based approach to keep the bad guys from finding and exploiting those weaknesses, prioritizing the vulnerabilities that matter the most.

Either as a project or with VmaaS, our services include ongoing vulnerability scans, detailed vulnerability reports, a guided explanation of what it all means, and more. Each VMaaS client is assigned a dedicated service concierge from our Offensive Security Operations team. Our expert will facilitate a monthly conference to highlight trends and make treatment recommendations for the client. These added insights provide the client with an "attacker's eye view" of their attack surface.

Assura's project or VMaaS services utilize scanning tools such as Tenable Vulnerability Management, which Assura can provide as part of the service. We can also use data from dozens of other vulnerability identification tools, such as Veracode, Snyk, Acunetix, and Burp Suite Pro. The scope of our scans includes:

- Device and application discovery;
- Vulnerability identification and scoring; and
- Compliance assessment and scoring.

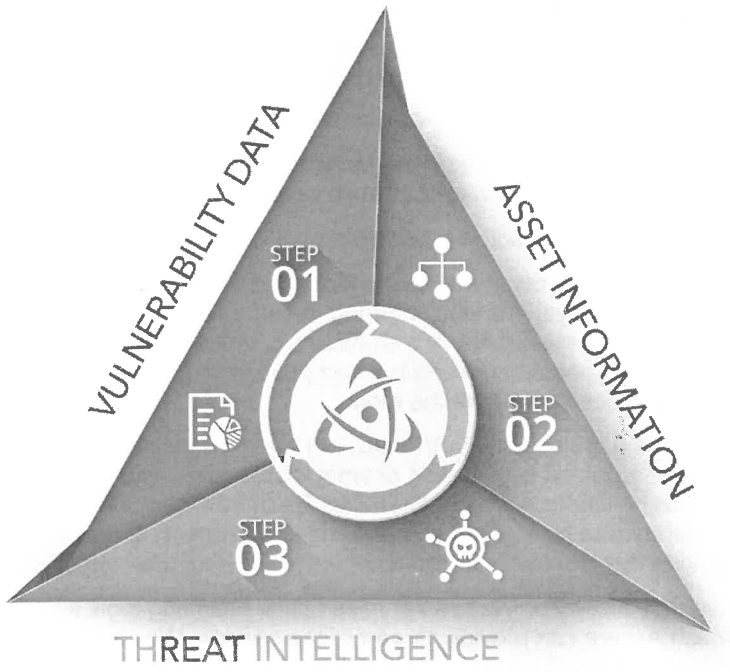
Our service not only uncovers security flaws from outdated software, but it also uncovers insecure hardware and software configurations, such as variances from Center for Internet Security Benchmark controls, and application-level flaws, such as injection, cross-site scripting, and request forgery vulnerabilities. We can also integrate static code analysis tools to identify and manage vulnerabilities in custom applications and third-party libraries such that they integrate seamlessly with each client's system development life cycle, change control, and release management practices.

Each vulnerability is then scored using the Common Vulnerabilities Scoring System (CVSS) or the Common Weaknesses Scoring System (CWSS).

Once a vulnerability is identified and scored, we work with the client's security and IT operations to confirm the vulnerabilities and assist them with expert guidance for remediation on a prioritized basis. We also have the means of configuring our system to automatically alert IT operations of a critical vulnerability through their service management platform. Vulnerabilities are then mapped to the client's asset inventory, with critical assets scheduled for remediation of high-impact vulnerabilities first.

All vulnerabilities are ingested and reported into Nucleus, a cloud-based vulnerability intelligence and management platform. Nucleus automatically enriches all vulnerability data using enterprise-class vulnerability and threat intelligence powered by Mandiant. By combining the aggregation, analytics, and vulnerability management orchestration capabilities already provided within Nucleus with the insight and intelligence provided by the Mandiant team, practitioners can accelerate the vulnerability prioritization and triage process using automation at scale and have the data they need to rapidly make confident decisions and accurately assess the risk of vulnerabilities. Nucleus combines all the asset information, vulnerability data from scanning tools, and threat intelligence into one single platform for vulnerability teams to eliminate laborious manual data analysis, accelerate decision-making and prioritization, and remove major pain points that exist for all organizations trying to mature their vulnerability management programs.

In a single pane of glass, Nucleus correlates all organizational asset information, vulnerability data from the network, application, cloud and container scanning tools, org charts, system hierarchies, and three complete feeds of vulnerability intelligence so practitioners can assess what matters most. Nucleus normalizes the data, enabling teams to evaluate, triage, prioritize, and remediate much faster and with greater precision.



Assura's OSO Concierge works with the client to fully configure and customize Nucleus, set up all integrations and workflows, determine remediation priorities, and train the client on its use.

At the client's option, we can report on the status of vulnerability remediation and newly identified vulnerabilities at a pace that is right for the organization.

3.2 C.1.B: WIRELESS NETWORK ASSESSMENT

Wireless networks are a **critical entry point** for attackers. **Misconfigurations, weak encryption, rogue access points, and signal leakage can expose an organization to cyber threats**. Assura's comprehensive Wireless Network Assessment is designed to **uncover security gaps, validate defenses, and provide actionable solutions**—before attackers find them.

Our four-phase methodology **ensures full visibility into the wireless environment**, delivering in-depth insights and technical expertise to keep the organization secure.

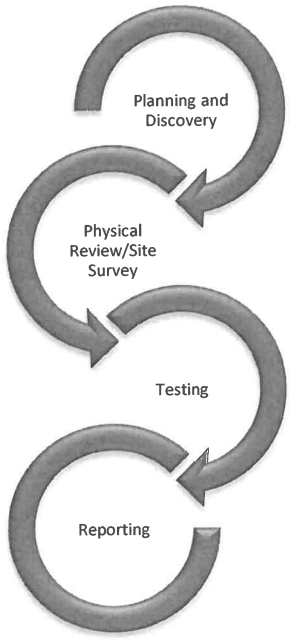
Assura's **Wireless Network Assessment** identifies hidden threats, tests an organization's defenses, and provides clear, actionable recommendations to **help lock down the network**.

Our detailed approach is listed below.

Planning & Discovery

Before beginning testing, we conduct a brief meeting with the client to review and acknowledge the assessment or penetration testing rules of engagement, confirm the project scope and testing timeline, identify specific testing objectives, document any testing limitations or restrictions, and answer any questions related to the project.

Assura begins each assessment by performing a walkthrough of all in-scope facilities in order to enumerate advertised and hidden wireless networks and the physical location of access points. After this phase, Assura generates a wireless network inventory that lists the wireless network name, encryption, and associated access point MAC address. Assura then confirms all in-scope wireless networks with the client's team, including MAC addresses and SSIDs. This assists in confirming the presence or absence of rogue access points.



Physical Review/Site Survey

Assura uses the inventory generated during the Planning & Discovery phase to locate and inspect access points that may be in publicly accessible locations. If found, Assura inspects the access point for open console or ethernet ports and validates if they provide access to sensitive networks or to the management console of the access point. Using several high-gain antennas, our testers walk the perimeter of the network and track the various wireless signals throughout the organization. Additionally, the tester will walk outside of the facility and continue to collect signals. This allows the tester to correlate whether a particular access point is within the client's network or a nearby network. The tester will then determine whether the wireless signal is significantly leaking outside of sensitive areas that could allow an attacker to target the wireless network from nearby locations. In addition to taking an inventory of available SSIDs and measuring signal strength, the tester will also be searching for rogue access points within the building.

Testing

For any networks that use WEP, WPA, WPA2-PSK, or WPA3-PSK encryption, Assura passively monitors wireless traffic and captures authentication information. Assura uses captured authentication traffic to attempt an offline brute force attack to determine if the passphrase is sufficiently strong. For any networks that use a weak passphrase or don't use encryption, Assura associates with the wireless network and performs the following tasks:

- Collect basic network information including internal network range, DHCP / DNS configurations, external IP address, and filtering on network traffic (e.g. URL filtering, malware filtering, port blocking).
- Determine other network ranges that may be accessible from the attached network.
- Determine if client isolation is enabled on the network.
- Determine if broadcast filtering is enabled on the network.
- Check if network infrastructure management services are accessible from the network such as access point management interfaces or router SSH/telnet ports.
- Determine if corporate assets are accessible from the network by monitoring traffic.
- Determine if unencrypted traffic discloses sensitive information (e.g. SNMP strings, usernames, passwords).

Optionally, Assura can perform active testing, including:

- "Evil Twin" attacks. This testing is used to validate if endpoints are properly configured to validate the access point their associating with. If vulnerable this will result in gaining access to authentication information for endpoints or users.
- Use social engineering techniques to advertise similarly named wireless networks with crafted captive portal pages designed to capture username and passwords from employees.
- Vulnerability scans performed against any associated networks. This identifies systems that could potentially be attacked and used to gain further access into the environment.
- LLMNR/NBT-NS poisoning attacks on any associated network to potentially gain authentication information of other systems on the network.

Reporting

The wireless testing report provides:

- An overview of the scope of the testing
- Testing methodology
- Signal heat maps of client SSIDs that identify areas of signal or SSID leakage
- Inventory of discovered access points and SSIDs and protective mechanisms
- Findings and recommendations to correct identified vulnerabilities

Assura also provides an executive-level out-brief as part of its reporting.

3.3 C.1.C: FIREWALL AND ROUTER SECURITY ASSESSMENT

Firewalls and routers are the **first line of defense** against cyber threats—but are they configured to protect the organization effectively? **Misconfigurations, outdated firmware, and weak security policies can leave the network exposed, making it an easy target for attackers.**

At Assura, we take **a proactive approach** to firewall and router security. Our **comprehensive security assessment** evaluates the network devices against **industry best practices, regulatory standards, and real-world attack methodologies** to uncover vulnerabilities before they become an issue.

With our in-depth **three-phase methodology**, we ensure firewall and router configurations are **aligned with security policies, optimized for performance, and hardened against cyber threats.** Our assessment provides the organization with:

- ☑ **A clear view of security gaps** in device configurations, access control lists, and routing policies.
- ☑ **Identification of unsupported or end-of-life devices** that pose security risks.
- ☑ **Vulnerability analysis** of software, firmware, and configuration settings.
- ☑ **Assessment of authentication controls**, including passwords, multifactor authentication, SSH keys, and SNMP configurations.
- ☑ **Evaluation of security benchmarks**, including CIS and DISA STIG compliance.
- ☑ **Scored security metrics** to measure your compliance against industry best practices.

At the conclusion of our assessment, Assura delivers a **detailed security report** with a prioritized roadmap for remediation, ensuring a network remains secure against evolving threats. Protect firewalls and routers with Assura's expert-driven security assessment—before attackers find the gaps.

Our detailed approach is listed below.

Assura's firewall and router configuration security assessments analyze and evaluate the following security-related components:

- Identification of available support by OEMs including end-of-life devices or devices where end-of-life is imminent;
- Ports, protocols, and services permitted by policy to be routed through the firewall or router;
- Access control list alignment with policies to ensure that data flows are enforced per approved configurations;
- Vulnerable configurations, software, and firmware;
- Configuration security of the device itself in accordance with Center for Internet Security benchmarks and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs);
- Use of a dedicated management Virtual Local Area Network (VLAN) to isolate access to management functions;
- Credentials and keys such as passwords, multifactor authentication, SSH keys, and Simple Network Management Protocol (SNMP) strings are provisioned, implemented, and managed in accordance with best practices;
- OS/firmware patch level to identify any open security or functionality issues;
- AAA (centralized authentication, authorization, and audit) on all devices;
- Other configuration-related items (e.g., URL filtering, content inspection, and Intrusion Prevention System configuration) for Unified Threat Management devices and
- Other items as identified or scoped.

Assura's methodology for firewall and router security assessments consists of three phases, as described below:

Artifact Review

Assura reviews artifacts such as device security policies, configuration standards, approved ports, protocols, and services, and approved data flows.

Analysis and Evaluation

In this step, Assura reviews the configurations for conformance with the artifacts in the prior step. We do this through manual inspection of configurations, interviews with network administrators, and through the use of automated tools such as Tenable Vulnerability Management and CIS-CAT to identify variances from industry best practices as well as other weak configurations or vulnerabilities. We then provide a score of each device's security so that the client has concrete metrics to show compliance with industry practices.

Reporting

The firewall and router security reports provide:

- An overview of the scope of the assessment
- Inventory of assessed devices, including name, make, model, serial number, operating system version, and primary IP address
- Testing methodology
- Detailed identification of gaps between organizational policy and approved configurations and recommendations for correction
- Detailed identification of vulnerabilities and recommendations for correction

Assura also provides an executive-level out-brief as part of its reporting.

3.4 C.1.D: SERVER CONFIGURATION ASSESSMENT

Servers are the **backbone of the IT infrastructure**, housing critical data and applications that keep the organization running. But **misconfigurations, outdated software, and weak security controls** can leave them vulnerable to cyberattacks, downtime, and compliance failures.

At Assura, we take a **proactive approach to server security** by conducting in-depth **configuration assessments** to identify **hidden vulnerabilities, policy misalignments, and security gaps** before they can be exploited. Our methodology evaluates **on-premises, cloud-based, and virtualized environments** to ensure that servers are **configured securely and compliant with industry best practices** such as **CIS benchmarks and DISA STIGs**.

With Assura's **comprehensive assessment**, organizations gain:

- ☑ **Full visibility into security risks** across operating systems, applications, and network configurations.
- ☑ **End-of-life identification** to mitigate risks from outdated or unsupported server versions.
- ☑ **Cloud security best practice validation**, including **encryption, access management, and security services** for IaaS environments.
- ☑ **Access control and authentication analysis**, ensuring **strong credential management and multifactor authentication**.
- ☑ **Advanced security control validation**, including **firewall, EDR, malware defense, and intrusion detection**.
- ☑ **OS and firmware patch-level verification** to identify **unpatched vulnerabilities**.

At the end of our assessment, we provide a **detailed security report** with a **prioritized action plan** to close security gaps, along with an **executive-level briefing** to translate findings into actionable business decisions.

Our detailed approach is listed below.

Assura's server configuration assessments are similar to its firewall and router configuration security assessments, which analyze and evaluate the following security-related components:

- Identification of available support by OEMs including end-of-life devices or devices where end-of-life is imminent;
- If the server is a hypervisor host, support by the hypervisor OEM, including end-of-life versions or versions where end-of-life is imminent;
- If the server is in a cloud Infrastructure-as-a-Service (IaaS) provider, security best practices for the cloud tenant such as encrypted volumes, Identity and Access Management keys and roles, and use of security services provided by the IaaS provider (e.g., Amazon Guard Duty and Security Hub);
- Approved software and functions for the server;
- Ports, protocols, and services permitted by policy to be processed by the server;
- Access control list alignment with policies to ensure that data flows are enforced per approved configurations;
- Configuration security of the server and services (e.g., IIS, Apache, SQL, Oracle, etc.) in accordance with Center for Internet Security benchmarks and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs);
- Use of malware defense, Host-based Intrusion Detection/Prevention, firewall, and Endpoint Detection and Response (EDR);
- Use of a dedicated management Virtual Local Area Network (VLAN) to isolate access to management functions such as IPMI ports;
- Credentials and keys such as passwords, multifactor authentication, SSH keys are provisioned, implemented, and managed in accordance with best practices;

- OS/firmware patch level to identify any open security or functionality issues; and
- Other items.

Assura's methodology for server configuration assessments consists of three phases, as described below:

Artifact Review

Assura reviews artifacts such as device security policies; configuration standards; approved server roles; approved ports, protocols, and services; and approved data flows.

Analysis and Evaluation

In this step, Assura reviews the configurations for conformance with the artifacts in the prior step. We do this through manual inspection of configurations, interviews with system administrators, and the use of automated tools such as Tenable Vulnerability Management and CIS-CAT to identify variances from industry best practices as well as other weak configurations or vulnerabilities. We then provide a score of each device's security so that the client has concrete metrics to show compliance with industry practices.

Reporting

The server security reports provide:

- An overview of the scope of the assessment
- Inventory of assessed devices, including name, make, model, serial number, operating system version, and primary IP address
- Testing methodology
- Detailed identification of gaps between organizational policy and approved configurations and recommendations for correction
- Detailed identification of vulnerabilities and recommendations for correction

Assura also provides an executive-level out-brief as part of its reporting.

3.5 C.1.E: DATABASE ARCHITECTURE SECURITY ASSESSMENT

Databases hold the crown jewels of the organization—student, citizen, or client information; intellectual property; financial records; and mission-critical data. But are they truly secure? **Misconfigurations, excessive permissions, weak encryption, and poor monitoring** can leave databases vulnerable to breaches, insider threats, and regulatory non-compliance.

At Assura, we specialize in **database security assessments** that go beyond basic vulnerability scans. We **analyze the full architecture of your databases**, ensuring that **data is segmented, protected, and accessed securely**—whether the databases are on-premises, in the cloud, or fully managed services like **Amazon RDS or Microsoft Azure Databases**.

Our **comprehensive security review** includes:

- ☑ **End-of-life risk identification** – Ensuring database software is supported and up to date.
- ☑ **Access control analysis** – Validating **database roles, permissions, and authentication** to prevent unauthorized access.
- ☑ **Data segmentation & regulatory compliance** – Evaluating **logical and physical separation** to align with compliance frameworks.
- ☑ **Backup & replication assessments** – Ensuring **high availability and disaster recovery readiness**.
- ☑ **Data protection verification** – Reviewing **encryption, hashing, masking, and tokenization** techniques.
- ☑ **Production data security** – Identifying improper use of **real data in non-production environments**.
- ☑ **Audit & logging configuration** – Ensuring complete visibility into database activity.
- ☑ **Threat monitoring & detection** – Assessing defenses against **data-layer attacks, exfiltration, and insider threats**.

We use **industry-leading tools** like **Tenable Vulnerability Management, Oracle DBSAT, and SQL Server's Vulnerability Assessment** to perform deep security evaluations.

Assura's team of **database security experts** works closely with administrators to provide:

- **Detailed reports** with **prioritized recommendations** to fix security gaps.
- **A full inventory of assessed databases**, their configurations, and associated risks.
- **An executive-level briefing**, translating technical findings into actionable business insights.

Assura's **Database Architecture Security Assessment** gives organizations the confidence that their most valuable assets are safe.

Our detailed approach is listed below.

Assura conducts database architecture security assessments to review the way that databases are constructed, data is protected, database segmentation, data is accessed, and how databases are monitored. We conduct assessments of databases built on Oracle, Microsoft SQL Server, MySQL, PostgreSQL, NoSQL, MongoDB, MariaDB, and others. We can do

assessments of traditional DBMS installations or on fully managed services such as Amazon Relational Database Service (RDS) or Microsoft Azure Databases. We do assessments for databases, data warehouses, and data lakes as well as security of BLOB storage such as in Amazon Simple Storage Service (S3) buckets.

Our assessments analyze and evaluate the following security-related components:

- Identification of available support by OEMs including end-of-life software or software where end-of-life is imminent;
- Database roles and account permissions;
- Data segmentation (logical and physical) based on regulatory and policy requirements;
- Availability including backup and replication;
- Data protection such as hashing, encryption, masking, and tokenization;
- Use of production data in non-production environments;
- Auditing and logging;
- Configuration compliance with best practices such as CIS Benchmarks;
- Monitoring for data-layer attacks, exfiltration, and misuse of data; and
- Other items.

We use tools such as Tenable Vulnerability Management, the Oracle Database Security Assessment Tool (DBSAT), and the SQL Vulnerability assessment capabilities built into SQL Server Management Studio.

Assura's methodology for database architecture security assessments consists of three phases, as described below:

Artifact Review

Assura reviews artifacts such as data security policies; business impact analysis; data classifications; configuration standards; and approved data flows.

Analysis and Evaluation

In this step, Assura reviews the configurations for conformance with the artifacts in the prior step. We do this through manual inspection of configurations, interviews with database administrators, and through the use of automated tools.

Reporting

The server security reports provide:

- An overview of the scope of the assessment
- Inventory of assessed databases
- Assessment methodology
- Detailed identification of gaps between organizational policy and approved configurations and recommendations for correction
- Detailed identification of vulnerabilities and recommendations for correction

Assura also provides an executive-level out-brief as part of its reporting.

3.6 C.1.F: NETWORK SCANNING PROCESS ASSESSMENT

Networks are under constant attack—**but are the vulnerabilities known?** Misconfigured devices, outdated software, and **exposed services** create **entry points for attackers** looking to breach defenses. **Without proper visibility, an organization could be one scan away from exploitation.**

Assura's **proven four-phase network scanning process** identifies **critical security weaknesses before cybercriminals do**, delivering actionable insights to **harden defenses and reduce the attack surface**. Unlike basic automated scans, this approach combines **advanced scanning tools with expert analysis** to separate real threats from false positives, ensuring **only the most relevant vulnerabilities demand attention**.

Assura's Network Scanning Process

- ☑ **Planning for Precision:** The scan is tailored to the organization's environment, ensuring no sensitive systems are impacted while capturing **all critical network assets**.
- ☑ **Smart, Non-Destructive Scanning:** Using leading scanning tools, **unnecessary services, vulnerable software, and active exploits** are identified—without disrupting operations.
- ☑ **Expert-Led Analysis:** Assura's cybersecurity specialists **validate findings, eliminate false positives, and identify trends** that indicate deeper security risks.
- ☑ **Actionable, Executive-Level Reporting:** Each assessment includes **two reports**:
  - 📌 **Executive Report** – A high-level summary of **critical vulnerabilities, security trends, and prioritized recommendations** for leadership teams.
  - 📌 **Detailed Assessment Report** – A technical deep dive with **CVSS-based risk scoring, impact assessments, and step-by-step remediation guidance** tailored to the organization's environment.

With Assura's **network scanning service**, organizations receive more than just raw data—**they gain clear, prioritized insights that strengthen defenses before attackers can strike.** Our detailed approach is listed below. Strengthen network security with Assura's expert-driven network scanning assessment.

Our detailed approach is listed below.

Assura uses a proven four-phase process to conduct network scanning:

Planning

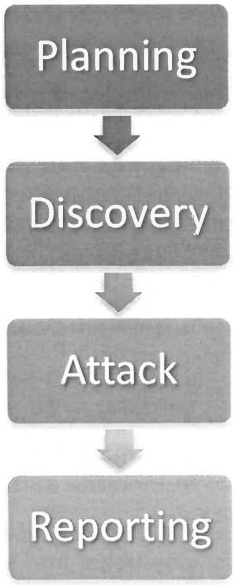
The Planning phase is where Assura obtains targeting information from the client. This includes IP addresses of specific devices and/or network/subnetwork addresses. We also request that the client provide us with a list of devices and/or subnets/VLANs known to be sensitive to scanning so that they can be excluded from scanning or scanned separately with the production support staff for those devices on standby in case an issue arises.

Scanning

In the Scanning phase, Assura configures the scanning software tools with the targets and ensures that only non-destructive scanning is performed. The scanners will then identify known vulnerabilities using signature patterns. The purpose of these scans is to identify unnecessary services, unusual use, vulnerable software, and active vulnerabilities. Assura will not attempt to exploit any of the vulnerabilities identified in this activity.

Analysis

The Analysis phase is where Assura uses its expertise to identify critical vulnerabilities that need to be reported immediately, identify potential false positives[1]; and identify patterns and trends that need to be highlighted in the Reporting phase. The team will also map identified services to server functions in order to properly identify which running services are superfluous, increase the attack surface of the device, and/or pose a high risk.



Reporting

The Reporting phase consists of developing and delivering two reports:

1. An Executive Report that provides a management-level overview of the results of the assessment including key findings such as critical vulnerabilities and trends, and recommendations for remediation. Recommendations may include software updates, configuration changes, process changes, additional training for IT personnel or a combination of those.
2. A Detailed Assessment Report that provides in-depth information about each vulnerability along with a Common Vulnerability Scoring System (CVSS) base score. Assura uses CVSS scores because they provide an easy-to-understand metric that represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments and expresses the potential impacts to confidentiality, integrity, and availability of data. If warranted, Assura may also calculate the temporal and environmental scores in order to better communicate the magnitude of risk in the context of the client's IT environment and threat landscape. The report also provides detailed information about how to remediate each vulnerability.

[1] While every attempt will be made to identify and discard "false positive" results through post-test review of the data, additional "false positives" may be revealed as the client and Assura conduct further analysis to address identified weaknesses.

3.7 C.1.G: WEB APPLICATION SECURITY ASSESSMENT

Web applications and APIs are prime targets for cyber threats. **Misconfigurations, broken access controls, and unpatched vulnerabilities** can expose sensitive data and disrupt operations. **Assura's Web Application and API Penetration Testing goes beyond basic scans—identifying and exploiting real-world attack paths to strengthen defenses before adversaries do.**

The Assura Advantage: More Than Just Automated Testing

Many penetration tests rely too heavily on automated tools, **missing business logic flaws, chained vulnerabilities, and nuanced security weaknesses**. Assura takes a **hybrid approach**, combining **commercial and open-source tools** like Burp Suite, Nuclei, SQLmap, and Dirsearch with extensive **manual testing** by experienced security professionals.

This **hands-on testing process** uncovers weaknesses that automation alone cannot detect—**from insecure authentication flows to subtle misconfigurations that allow privilege escalation or data exfiltration**. Each engagement evaluates **both unauthenticated and authenticated attack scenarios**, simulating real-world insider threats and assumed breach conditions.

Testing Aligned with Industry Standards

Assura's penetration testing methodology is grounded in **OWASP ASVS, NIST SP 800-115, PCI-DSS, and PTES**, ensuring comprehensive coverage across:

✓ **Web Application Security:** Authentication, access control, session management, encryption, error handling, business logic, API endpoints, and more.
✓ **API Security:** Authentication & authorization protocols, input validation, cryptographic handling, improper data sanitization, and transport security.
✓ **Critical Vulnerability Frameworks:** OWASP Top 10, CWE/SANS Top 25, and custom test cases tailored to the organization's specific risks.

Harden applications and APIs with **Assura's expert-driven penetration testing.**

Our detailed approach is listed below.

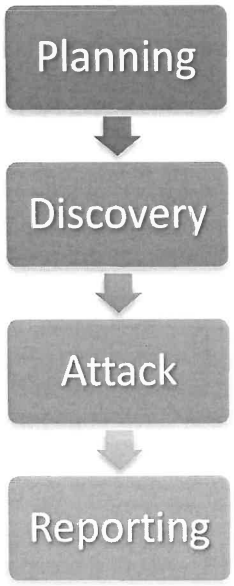
Assura's approach to web application and API penetration combines automated testing (where safe) with extensive manual testing techniques to deliver a comprehensive assessment. Our methodology leverages both commercial and open-source tools, such as Burp Suite, Nuclei, SQLmap, and Dirsearch, to identify vulnerabilities such as cross-site scripting, SQL injection attacks, insecure direct object references, and much more.

Assura goes beyond automated testing with in-depth, hands-on inspection of applications and APIs to uncover and exploit subtle flaws, including misconfigurations, insecure storage of sensitive data, business logic flaws, and other chained vulnerabilities that often evade detection by automated scanners. Our engagements evaluate web applications from both an unauthenticated and authenticated (insider threat/assumed breach) perspective, ensuring vulnerabilities such as privilege escalation, lateral movement, and data segmentation are identified.

Assura's web application and API penetration testing align with well-known standards, including OWASP ASVS, NIST SP 800-115, PCI-DSS, and PTES. Key components of our assessments include looking for vulnerabilities in the following areas:

- Web Applications:
  - Architecture, design, and threat modelling
  - Authentication
  - Session management
  - Access control
  - Malicious input handling
  - Cryptography at rest
  - Error handling and logging
  - Data protection

  - Communications
  - HTTP security configuration
  - Malicious controls
  - Business logic
  - File and resources
  - Mobile
  - Web services
  - Configuration
- API
  - Protocols for Authentication and Authorization
  - REST services are stateless
  - Access Control
  - Input validation
  - Output encoding
  - Cryptography
  - Message Integrity
  - Confidentiality
  - HTTP Return Code
  - Improper Data Sanitization
  - Insecure Direct Object Reference
  - Insufficient Transport Layer Security
  - Sensitive Data Exposure
  - Weak Server-Side Security
  - Improper Key Handling
  - Inconsistent API Functionality
  - Security Misconfiguration
- OWASP Top 10
- CWE/SANS Top 25
- Custom test cases based on application and business functions.



Assura's methodology for web application security assessment consists of four phases, as described below:

Planning

The Planning stage is where we develop a Rules of Engagement (ROE) document. The ROE acts as a guide for the conduct of the test. Each ROE document addresses:

- The test window (i.e., dates and times that testing is authorized)
- Prerequisites (e.g., systems operating normally)
- Test methodologies and tools, their potential impact to operations, and mitigations that will be put into place to minimize impact or recover from potentially unwanted impact
- Test parameters (e.g., authorized test activities)
- IP address(es) where testing originates
- List of applications to be tested (by URL)
- Handling of sensitive information to prevent unauthorized disclosure
- Destruction of sensitive information that comes into the possession of the test team
- Methods and timing for reporting sensitive information
- Process for halting operations
- A de-confliction process, and
- Contact information for key personnel from all involved organizations, including the Assura Technical Point of Contact, who will be available 24/7 throughout the test window

Each Rules of Engagement document will be executed by an authorized executive of Assura and an authorized signatory from the client.

Discovery

The Discovery stage is where Assura conducts reconnaissance activities by reviewing available documentation, manually crawling and interacting with the application or API, and automated tools such as Burp Suite or file and directory discovery tools.

Attack

In the Attack stage, Assura attempts to exploit potential vulnerabilities that were uncovered in the Discovery stage. We will use a combination of automated and manual means in order to exploit the identified vulnerabilities and defeat/bypass security controls in order to identify application weaknesses and test whether the application addresses common vulnerabilities.

This stage represents the bulk of our effort in conducting a penetration test. One of the ways that we ensure that we are maximizing our time and enhancing our chances of success is to verify the results of automated scanning with manual techniques for the vulnerabilities or combination of vulnerabilities that present the highest likelihood of exploitability (sometimes a combination of "low" vulnerabilities can be used in concert to achieve a big payoff; this is called vulnerability chaining). We then use this information as the basis of a plan of attack.

Each successful attack is fully documented with supporting evidence and detailed recommendations or remediation. This means that client personnel will not have to chase false positives or spend days, weeks or months of precious time researching remediation options – we do that "homework" for you.

Reporting

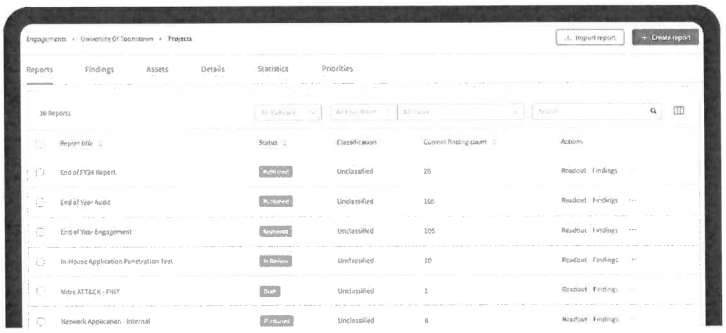
The Reporting stage is where raw data becomes information. The detailed findings and evidence gathered in the Discovery and Attack stages will be reported. Each exploitable weakness will be assigned a severity rating of Critical, High, Medium, Low, or Informational based on Likelihood and Impact, along with a CVSS score.

For each identified weakness, Assura will recommend detailed remediation steps. This could include the application of security patches, changing a system setting (or set of settings), implementing/modifying a compensating control, or modifying application code (right down to the function call). For each finding where it is possible, Assura will provide references to real-world attacks and research, MITRE ATT&CK framework tactics and techniques, and MITRE CWE identifiers relevant to the finding.

Each report includes the following:

- Executive Summary is written to be understandable by non-technical personnel and suitable for 3rd party consumption.
- Detailed technical report aimed at technical personnel with sufficient detail to fully understand the strengths and weaknesses demonstrated by the test. The full report includes:
    - Detailed description of each finding.
    - Recommendations and best practices to remediate or mitigate the risks associated with the finding.
    - References for each finding.
    - Steps-to-Reproduce for each finding to help clients safely re-create the vulnerability on their own and prove exploitation.
    - Evidence for each finding, which typically consists of sanitized screenshots but may also include output of a command or other knowledge obtainable only through exploitation.

Following the penetration test:



- Clients are provided access to Assura's online vulnerability management platform, where reports, asset information, and all findings are documented. Here, clients can assign and track remediation efforts for findings and request retesting for findings.
- Our team meets with all clients to discuss the outcome of the penetration test in an in-person or virtual briefing. Both technical and executive briefings are available to all clients.
- After the organization receives the draft copy of the report it will have 10 business days to request changes and provide commentary. Clients also have 60 calendar days to request retesting at no additional charge from the date the client receives the draft report. After the 60 days have lapsed, Assura will generate an updated report that reflects the progress the organization has made in that time.
- Clients maintain access to reports online for 1 year from the engagement start date.
- Any "0-day" vulnerabilities found in commercial software within the Client's environment will be reported by Assura to the vendor and MITRE/the National Vulnerability Database for remediation and tracking.
    - Assura adopted a responsible disclosure policy in late 2021 to assist clients with the difficulty of getting commercial software developers to fix newly found vulnerabilities. That policy and several Assura's CVEs can be found here: https://assura.atlassian.net/wiki/spaces/VULNS/overview

3.8 C.1.H: ACTIVE DIRECTORY SECURITY ASSESSMENT

Active Directory (AD) is the **heart of an organization's identity and access management**, making it a prime target for cybercriminals. **One misconfiguration, over-permissioned account, or exposed credential can open the door to privilege escalation, lateral movement, and full domain compromise.**

Assura's **Active Directory Security Assessment** provides a **real-world attacker's perspective**, identifying **hidden weaknesses before they can be exploited**. This assessment **simulates an insider threat scenario**, leveraging **pre-existing credentials to uncover privilege escalation paths, credential exposure risks, and attack vectors** that could be used to take control of the network.

By using **cutting-edge tools** like **BloodHound, PurpleKnight, and custom attack scripts**, Assura doesn't just **find vulnerabilities**—it **demonstrates how attackers can exploit them and provides expert-driven remediation strategies** to eliminate those risks.

How Assura Protects Active Directory:

✓ **Exposes misconfigured permissions, ACLs, and delegation settings** that enable privilege escalation.
✓ **Detects weak password policies, Kerberoasting, and AS-REProasting vulnerabilities** that attackers can leverage for credential theft.
✓ **Identifies Azure AD misconfigurations** that create security gaps in hybrid environments.
✓ **Simulates real-world attack paths** using **lateral movement and domain persistence techniques** to assess true exploitability.
✓ **Delivers clear, actionable guidance** with **step-by-step remediation strategies** mapped to **MITRE ATT&CK and industry best practices**.

Assura's AD Security Assessment provides the insights needed to secure identities, lock down permissions, and prevent breaches before they happen.

Our detailed approach is listed below.

Assura's Active Directory Security Assessments focus on identifying weaknesses that could lead to account or system compromise. Our assessments adopt an assumed breach perspective, leveraging pre-existing credentials to emulate insider threat scenarios. By utilizing advanced tools like BloodHound, PurpleKnight, and custom scripts, we evaluate users, groups, ACLs, policies, computers, and Azure Active Directory for exploitable flaws. Our engagements provide a detailed view of attack paths and privilege escalation opportunities within your Active Directory environment.

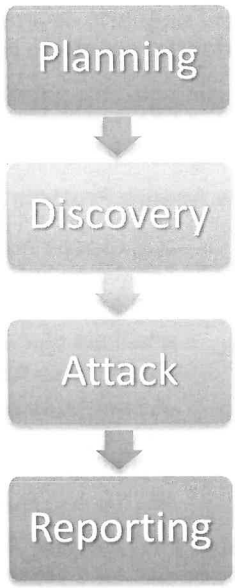
Assura's methodology aligns with modern standards and best practices for securing Active Directory to ensure comprehensive coverage. Key areas of focus during Active Directory assessments include:

- Misconfigured permissions and ACLs
- Over-permissions accounts and groups
- Insecure delegation settings
- Credential exposure (e.g., clear-text passwords, cached credentials)
- Kerberoasting and AS-REProasting opportunities
- Weak password policies
- Excessive permissions in hybrid identity environments
- Azure Active Directory misconfigurations
- Other issues that could enable privilege escalation, lateral movement, or domain compromise

Planning

The Planning stage is where we develop a Rules of Engagement (ROE) document. The ROE acts as a guide for the conduct of the test. Each ROE document addresses:

- The test window (i.e., dates and times that testing is authorized)
- Prerequisites (e.g., systems operating normally, credentials)
- Test methodologies and tools, their potential impact on operations, and mitigations that will be put into place to minimize impact or recover from potentially unwanted impact
- Test parameters (e.g., authorized test activities)
- IP address(es) where testing originates
- List of domains and environments to be tested
- Handling of sensitive information to prevent unauthorized disclosure
- Destruction of sensitive information that comes into the possession of the test team
- Methods and timing for reporting sensitive information
- Process for halting operations
- A de-confliction process, and
- Contact information for key personnel from all involved organizations, including the Assura Technical Point of Contact, who will be available 24/7 throughout the test window



Each Rules of Engagement document will be executed by an authorized executive of Assura and an authorized signatory from the client.

Discovery

The Discovery stage focuses on reconnaissance and data collection within the Active Directory environment. This includes:

- Gathering information on users, groups, ACLs, and policies
- Mapping attack paths using BloodHound or other tools
- Assessing hybrid Azure AD configurations for privilege escalation risks
- Identifying credential exposure through analysis and scanning tools

Attack

In the Attack stage, Assura actively exploits identified vulnerabilities to demonstrate the potential impact of a compromise. Using manual techniques and tools like NetExec, MimiKatz, and custom scripts, we test for:

- Privilege escalation (e.g., escalating from a standard user to a domain administrator)
- Lateral movement (e.g., via Pass-the-Hash or Pass-the-Ticket attacks)
- Credential harvesting
- Exploitation of over-permissioned accounts or misconfigured delegation rights
- Abuse of Azure AD configurations, such as consented permissions and application roles

This stage represents the bulk of our effort in conducting a penetration test and we conduct this stage just as a real attacker would. One of the ways that we ensure that we are maximizing our time and enhancing our chances of success is to verify the results of automated scanning with manual techniques for the vulnerabilities or combination of vulnerabilities that present the highest likelihood of exploitability (sometimes a combination of "low" vulnerabilities can be used in concert to achieve a big payoff; known as vulnerability chaining). We then use this information as the basis of a plan of attack.

Each successful attack is meticulously documented with evidence, remediation recommendations, and references to the MITRE ATT&CK framework and best practices. This ensures that clients can address findings effectively without spending time chasing false positives or conducting extensive research.

During the attack stage, the client's attack detection capabilities may also be challenged.

Reporting

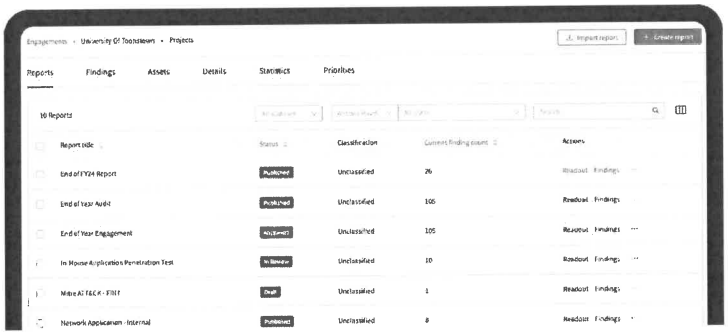
The Reporting stage is where raw data becomes information. The detailed findings and evidence gathered in the Discovery and Attack stages will be reported. Each exploitable weakness will be assigned a severity rating of Critical, High, Medium, Low, or Informational based on Likelihood and Impact, along with a CVSS score.

For each identified weakness, Assura will recommend detailed remediation steps. This could include the application of security patches, changing a system setting (or set of settings), implementing/modifying a compensating control, or modifying application code (right down to the function call). For each finding, where it is possible, Assura will provide references to real-world attacks and research, MITRE ATT&CK framework tactics and techniques, and MITRE CWE identifiers relevant to the finding.

Each report includes the following:

- Executive Summary is written to be understandable by non-technical personnel and suitable for 3rd-party consumption.
- Detailed technical report aimed at technical personnel with sufficient detail to fully understand the strengths and weaknesses demonstrated by the test. The full report includes:
    - Detailed description of each finding.
    - Recommendations and best practices to remediate or mitigate the risks associated with the finding.
    - References for each finding.
    - Steps-to-Reproduce for each finding to help clients safely re-create the vulnerability on their own and prove exploitation.
    - Evidence for each finding which typically consists of sanitized screenshots but may also include output of a command or other knowledge only obtainable only through exploitation.

Following the penetration test:



- Clients are provided access to Assura's online vulnerability management platform, where reports, asset information, and all findings are documented. Here, clients can assign and track remediation efforts for findings and request retesting for findings.
- Our team meets with all clients to discuss the outcome of the penetration test in an in-person or virtual briefing. Both technical and executive briefings are available to all clients.
- After the organization receives the draft copy of the report, it will have 10 business days to request changes and provide commentary. Clients also have 60 calendar days to request retesting at no additional charge from the date the client receives the draft report. After the 60 days have lapsed, Assura will generate an updated report that reflects the progress the organization has made in that time.
- Clients maintain access to reports online for 1 year from the engagement start date.

- Any "0-day" vulnerabilities found in commercial software within the Client's environment will be reported by Assura to the vendor and MITRE/the National Vulnerability Database for remediation and tracking.
    - Assura adopted a responsible disclosure policy in late 2021 to assist clients with the difficulty of getting commercial software developers to fix newly found vulnerabilities. That policy and several Assura's CVEs can be found here: https://assura.atlassian.net/wiki/spaces/VULNS/overview

3.9 C.1.I: PENETRATION TESTING

Cyber threats are constantly evolving, and organizations must stay ahead by **proactively identifying security weaknesses before adversaries can exploit them**. Assura's **penetration testing services provide real-world attack simulations** that go beyond automated scanning—leveraging **human expertise, advanced toolsets, and industry-recognized methodologies** to uncover vulnerabilities **across networks, applications, cloud environments, and infrastructure**.

Unlike generic testing, Assura's approach is **highly customized** to meet each organization's unique security challenges. Whether **external or internal penetration testing, black-box, grey-box, or white-box assessments**, Assura's methodology is based on **NIST SP 800-115, PTES, and OSSTMM**, ensuring a **rigorous, standards-based approach** that aligns with framework and regulatory requirements such as **NIST, PCI-DSS, HIPAA, and ISO 27001**.

Why Assura's Penetration Testing Stands Out

✓ **Tailored to Organizational Needs** – Every engagement is customized based on threat models, compliance requirements, and business-critical assets.
✓ **Beyond Automated Scanning** – Combining **advanced automation with hands-on exploitation** to uncover chained vulnerabilities and business logic flaws.
✓ **Realistic Threat Emulation** – Assessing security from an **attacker's perspective**, including **social engineering, lateral movement, and privilege escalation**.
✓ **Clear, Actionable Reporting** – Delivering **detailed technical findings, strategic remediation guidance, and executive summaries** for informed decision-making.
✓ **End-to-End Support** – Providing **attack path visualization, retesting options, and ongoing advisory services** to ensure remediation effectiveness.

From **external and internal network penetration tests** to **cloud security assessments, Wi-Fi penetration testing, and red teaming exercises**, Assura delivers a **comprehensive, intelligence-driven security assessment** that empowers organizations to **mitigate risks before they become breaches**.

Our detailed approach is listed below.

Whether internal or external, white, grey box, or black box, no matter the target type; and no matter if the test strictly focuses on technical testing or includes social engineering, Assura uses a penetration testing methodology based on a combination of National Institute of Standards and Technology (NIST) Special Publication 800-115, The Penetration Testing Execution Standard (PTES), and The Open Source Security Testing Methodology Manual (OSSTMM).

Before the test

We have a conversation with clients to find out what is more important to their organization and discuss our process:

- Each engagement is tailored to meet the client's needs and concerns.
- Our engagements both leverage advanced automation frameworks and hands on keyboard testing, human testing as opposed to only hands-off tool scanning.
- Where appropriate, we discuss the threat model that organizations are looking to emulate to ensure that testing is aligned with what the environment must defend against.
- All information is captured in the Rules of Engagement, which guides how the test is to be conducted.

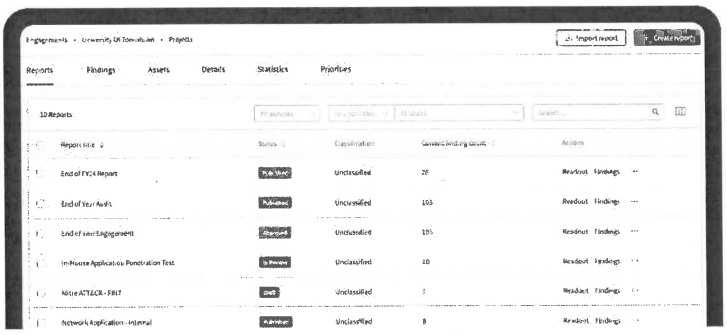
During the test

Assura maintains open lines of communication with clients based on their desired level of communication and comfort level with the penetration testing engagement.

After the test

Assura develops a full report that includes an executive summary, all technical findings, steps to reproduce, and recommendations for each finding reported. Additionally, Assura will include supplemental documents such as open-source intelligence gathered during the penetration test, social engineering campaign outcomes (if included in the engagement), and strategic recommendations for the organization:

Access to penetration test management platform:



- Assura provides a web interface to the report where clients can review vulnerabilities and assets, track remediation efforts, and request retesting of vulnerabilities.
- Client organizations will have visibility into the attack paths that Assura develops to paint a picture of how a real-world threat actor could move through your environment.

- Assura will provide the full penetration test report along with an executive summary report suitable for executives and third parties.
- Our team meets with clients to discuss the outcome of the penetration test in an in-person or virtual briefing. Both technical and executive briefings are available.
- After the organization receives the draft copy of the report, it will have 10 business days to request changes and provide commentary. Clients will also have 60 calendar days to request retesting at no additional charge from the day they receive the draft report. After the 60 days have lapsed, Assura will generate an updated report that reflects the progress the organization has made in that time.
- The organization will maintain access to reports online for 1 year from the engagement start date.
- Any "0-day" vulnerabilities found in commercial software within the Client's environment will be reported by Assura to the vendor and MITRE/the National Vulnerability Database for remediation and tracking.
- Assura adopted a responsible disclosure policy in late 2021 to assist clients with the difficulty of getting commercial software developers to fix newly found vulnerabilities. That policy and several Assura's CVEs can be found here: https://assura.atlassian.net/wiki/spaces/VULNS/overview

Penetration Test Types

External Network Penetration Test

The Assura penetration testing team assigned to the engagement carries out a penetration test that aligns to a custom methodology which draws from and meets the requirements of PCI- DSS, HIPAA, NIST SP 800-115, OSSTMM, and the Pentest Standard. Depending on the needs of the client, Assura aligns testing methodologies to any regulatory, contractual, or custom requirements through the creation of custom test cases.

Stages of the External Network Penetration Test include:

- OSINT – Open-Source Intelligence Gathering takes three primary forms as part of an evolutionary process – passive, semi-passive, and active. The purpose of OSINT is to help paint the picture of what the organization does, who works there, what technology is in place, what service providers and business partners exist, etc. to gain insight into the best avenues of attack.
- Footprinting – In this stage, Assura is focused on gathering information about the IP range

and/or DNS names available for attack. Activities include "whois" lookups, BGP looking glass reconnaissance, port scanning, DNS brute forcing, enumeration of services and versions, mapping web sites, and initial identification of potential vulnerabilities.

- Vulnerability Analysis – Assura utilizes automated vulnerability scanning tools such as Nmap's scripting engine, Nessus Professional, Invicti, WPScan, etc. to identify what we generally refer to as "low hanging fruit". Those are the vulnerabilities which are easily identifiable by an adversary with limited resources and skills. This information is used as input into furthering our manual penetration testing.
- Manual Assessment and Exploitation – At this stage, Assura's penetration testers focus on the specific services which may be vulnerable to attacks based on the information gathered in previous stages. Manual assessment may include traffic inspection and manipulation in tools such as BurpSuite or via Wireshark for non-web protocols. From there, Assura develops custom test cases and exploits to demonstrate the impact of the vulnerability in your environment. All steps to reproduce the exploit are included in AttackForge and the formal report.

Internal Network Penetration Test

The Assura penetration testing team assigned to the engagement executes a penetration test that aligns to a custom methodology which draws from and meets the requirements of PCI- DSS, HIPAA, NIST SP 800-115, OSSTMM, and the Pentest Standard. Depending on the needs of the client, Assura will align testing methodologies to any regulatory, contractual, or custom requirements through the creation of custom test cases.

Stages of the Internal Network Penetration Test include:

- Logistics – Due to the sensitive nature of internal networks, Assura works with the client to determine what systems are in-scope for testing and what systems should be tested but considered "fragile". Additionally, Assura works with the client to determine lockout policies to avoid user experience issues and ensure that the penetration test team is covering all areas of the network desired by the client.
- Enumeration – In this stage, Assura is focused on gathering information about the IP range and Domain through LDAP reconnaissance, packet captures, port scanning, DNS reconnaissance and brute forcing, enumeration of services and versions, mapping internal web sites, and initial identification of potential vulnerabilities.
- Vulnerability Analysis – Assura utilizes automated vulnerability scanning tools such as Nmap's scripting engine, Nessus Professional, BurpSuite Professional, WPScan, etc. to identify what we generally refer to as "low hanging fruit". Those are the vulnerabilities which are easily identifiable by an adversary with limited resources and skills. This information is used as input into furthering our manual penetration testing.
- Manual Assessment and Exploitation – At this stage, Assura's penetration testers focus on the specific services which may be vulnerable to attacks based on the information gathered in previous stages. Manual assessment may include traffic inspection and manipulation in tools such as BurpSuite or via Wireshark for non-web protocols. From there, Assura develops custom test cases and exploits to demonstrate the impact of the vulnerability in the context of your environment. All steps to reproduce the exploit are included in AttackForge and the formal report.

Wi-Fi Penetration Testing

Assura's Wi-Fi penetration tests ensure that your organization is utilizing best practices for Wi- Fi security such as the latest encryption technology, strong passwords, and adequate network segmentation.

- Reconnaissance – Assura reviews the SSIDs in scope, discovers any additional or hidden SSIDs, then identifies the Wi-Fi protocols in use to determine the applicable attacks.
- Exploitation – Assura utilizes techniques to obtain pre-shared keys for "cracking" to obtain plain text passwords. This includes:
    - De-auth attacks

- PMKID capture
- Rouge Access Point
- WPS brute force attacks and "pixie dust" attacks
- Username Capture and EAP-Brute forcing for WPA Enterprise environments

If Assura is then able to access the network after obtaining the pre-shared key, Assura validates that the Wi-Fi network is appropriately segmented from other networks based on the SSID's intended use-case. Specifically, we ensure that the guest network (if in place) cannot be used to access sensitive networks.

Cloud Penetration Test and Cloud Conformity Audit

Assura's Cloud Penetration Tests and Cloud Conformity Audits are based on the application of traditional penetration testing techniques combined with Trend Micro's Cloud Conformity Standards which contain 750+ best practices for your AWS, Microsoft Azure, and Google Cloud environments. The client receives a thorough understanding of how exposed their cloud environment is to attacks and what configuration changes the organization can make to better fortify that environment against future attack.

- Reconnaissance – Assura reviews any initially provided documentation and reviews the scope of the Cloud environment to ensure adequate coverage. Assura performs external scope discovery exercises to reveal the publicly available attack surface such as Virtual Machines, Storage, APIs, Authentication points, etc. This step ensures that we ensure that we have identified the potential attack surface, which also verifies that we have adequate access during the audit.
- Component Enumeration – At this phase, the Assura penetration tester assigned to perform the Cloud Conformity Standards audit authenticates to the environment using the provided credentials. The tester then gets acclimated to the environment and determines which test cases within the Cloud audit are applicable.
- Automated Component Configuration Review – Optionally, Assura can utilize Tenable.io to conduct a Cloud Configuration review based on CIS best practices. This step is only performed based on the client's desire to have their environment scanned in addition to the manual audit.
- Manual Assessment and Configuration Review – Assura's penetration testers utilize the Cloud Conformity Standards to identify weak security configurations and recommend enhancements. The team also attempts to exploit potential vulnerabilities in the services discovered during reconnaissance to demonstrate the impact and tie that finding back to the standard.
- Architectural Design and Custom Test Cases Review – It is not uncommon that once we are inside of a client's environment, we discover service integrations or configurations that may not be covered by any automated scan or audit standard. When Assura's penetration test team encounter a unique design concept or see a potentially misconfigured integration, we work with the client's team to determine the impact and report this accordingly.

3.10 C.1.J: TELECOMMUNICATIONS

Voice over IP (VoIP) and telecommunications systems **power modern business communications**, but **misconfigurations, weak security controls, and unpatched vulnerabilities** can turn them into prime targets for cybercriminals. **Attackers exploit weaknesses in VoIP infrastructure to intercept calls, manipulate call data, commit toll fraud, and even eavesdrop on confidential conversations.** Without proactive security assessments, organizations risk compromised communications, financial loss, and reputational damage.

Assura's **Telecommunications Penetration Testing** provides a **real-world attack simulation** to uncover and remediate security gaps **before they can be exploited**. Using **advanced penetration testing techniques and tools such as Nmap, Metasploit, rtpbreak, and siparmyknife**, Assura's experts assess **VoIP implementations, network segmentation, authentication mechanisms, encryption standards, and overall system resilience** against modern threats.

Why Assura's Telecommunications Security Testing Stands Out

✓ **Comprehensive VoIP Security Assessment** – Identifies vulnerabilities in **SIP proxies, unencrypted communications, voicemail security, and RTP injection risks**.
✓ **Real-World Attack Simulation** – Tests for **man-in-the-middle attacks, credential theft, call manipulation, and unauthorized access**.
✓ **Tailored Methodology** – Aligns with **industry standards and best practices**, ensuring security assessments match the organization's specific VoIP infrastructure.
✓ **Actionable Insights & Expert Remediation** – Provides **detailed reports with prioritized vulnerabilities, exploitation proof, and remediation strategies** for rapid security improvements.
✓ **Continuous Support & Retesting** – Offers **remediation validation, ongoing vulnerability tracking, and strategic recommendations** to fortify defenses over time.

From **VoIP security testing to full-scale telecommunications infrastructure assessments**, Assura delivers a **proactive, intelligence-driven security approach** that helps organizations **secure their communications, prevent fraud, and maintain confidentiality. Strengthen VoIP security with Assura's Telecommunications Penetration Testing.**

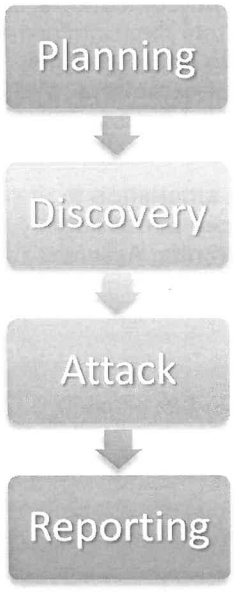
Our detailed approach is listed below.

Telecommunications penetration testing, such as identifying exploitable weaknesses in Voice Over IP (VoIP) implementations, helps to identify areas where communication confidentiality can be compromised as well as leaving an organization open to call tracking, call data manipulation, toll fraud, and other scams. Assura's telecommunications assessments are similar to traditional penetration tests where the VoIP infrastructure is attacked. We use tools such as Nmap, Metasploit, rtpbreak, siparmyknife, and others. Our telecommunications assessments analyze and evaluate the following security-related components:

- Identification of available support by OEMs including end-of-life devices, software, and firmware or devices, software, and firmware where end-of-life is imminent
- Unpatched vulnerabilities in VoIP infrastructure equipment
- Uncredentialed access to Session Initiation Protocol (SIP) proxies
- Weak credentials to SIP proxies
- Use of unencrypted communications with SIP proxies
- Vulnerability to man-in-the-middle attacks to decode G.711 traffic and eavesdrop on communications
- RTP injection
- Voicemail attacks
- Adequate network segmentation
- Quality of Service (QoS), and
- Others

Planning

The Planning stage is where we develop a Rules of Engagement (ROE) document. The ROE act as a guide for the conduct of the test. Each ROE document addresses:



- The test window (i.e., dates and times that testing is authorized)
- Prerequisites (e.g., systems operating normally)
- Test methodologies and tools, their potential impact to operations, and mitigations that will be put into place to minimize impact or recover from potentially unwanted impact
- Test parameters (e.g., authorized test activities)
- IP address(es) where testing originates
- List of applications to be tested (by URL)
- Handling of sensitive information to prevent unauthorized disclosure
- Destruction of sensitive information that comes into the possession of the test team
- Methods and timing for reporting sensitive information
- Process for halting operations
- A de-confliction process, and
- Contact information for key personnel from all involved organizations, including the Assura Technical Point of Contact, who will be available 24/7 throughout the test window

Each Rules of Engagement document will be executed by an authorized executive of Assura and an authorized signatory from the client.

Discovery

The Discovery stage is where Assura conducts reconnaissance activities using automated tools such as Nmap and Metasploit's SIP enumerator.

Attack

In the Attack stage, Assura attempts to exploit potential vulnerabilities that were uncovered in the Discovery stage. We will use a combination of automated and manual means in order to exploit the identified vulnerabilities and defeat/bypass security controls in order to identify weaknesses that permit account compromise, access to unauthorized information, injection of code, and other weaknesses.

This stage represents the bulk of our effort in conducting a penetration test and we conduct this stage just as a real attacker would. One of the ways that we ensure that we are maximizing our time and enhancing our chances of success is to verify the results of automated scanning with manual techniques for the vulnerabilities or combination of vulnerabilities that present the highest likelihood of exploitability (sometimes a combination of "low" vulnerabilities can be used in concert to achieve a big payoff). We then use this information as the basis of a plan of attack.

Each successful attack is fully documented with supporting evidence and detailed recommendations or remediation. This means that client personnel will not have to chase false positives or spend days, weeks or months of precious time researching remediation options – we do that "homework" for you.

During the attack stage, the client's attack sensing and warning capability may also be challenged.

Reporting

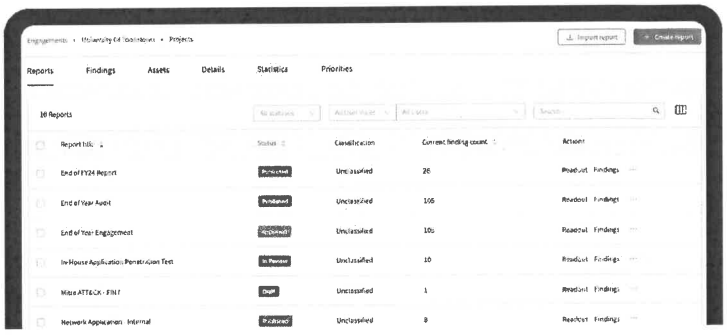
The Reporting stage is where raw data becomes information. The detailed findings and evidence gathered in the Discovery and Attack stages will be reported. Each exploitable weakness will be assigned a severity rating of Critical, High, Medium, Low, or Informational based on Likelihood and Impact, along with a CVSS score.

For each identified weakness, Assura will recommend detailed remediation steps. This could include the application of security patches, changing a system setting (or set of settings), implementing/modifying a compensating control, or modifying application code (right down to the function call). For each finding, where it is possible, Assura will provide references to real-world attacks and research, MITRE ATT&CK framework tactics and techniques, and MITRE CWE identifiers relevant to the finding.

Each report includes the following:

- Executive Summary is written to be understandable by non-technical personnel and suitable for 3rd-party consumption.
- Detailed technical report aimed at technical personnel with sufficient detail to fully understand the strengths and weaknesses demonstrated by the test. The full report includes:
    - Detailed description of each finding.
    - Recommendations and best practices to remediate or mitigate the risks associated with the finding.
    - References for each finding.
    - Steps-to-Reproduce for each finding to help clients safely re-create the vulnerability on their own and prove exploitation.
    - Evidence for each finding, which typically consists of sanitized screenshots but may also include the output of a command or other knowledge obtainable only through exploitation.

Following the penetration test:



- Clients are provided access to Assura's online vulnerability management platform, where reports, asset information, and all findings are documented. Here, clients can assign and track remediation efforts for findings and request retesting for findings.
- Our team meets with all clients to discuss the outcome of the penetration test in an in-person or virtual briefing. Both technical and executive briefings are available to all clients.
- After the organization receives the draft copy of the report it will have 10 business days to request changes and provide commentary. Clients also have 60 calendar days to request retesting at no additional charge from the date the client receives the draft report. After the 60 days have lapsed, Assura will generate an updated report that reflects the progress the organization has made in that time.
- Clients maintain access to reports online for 1 year from the engagement start-date.
- Any "0-day" vulnerabilities found in commercial software within the Client's environment will be reported by Assura to the vendor and MITRE/the National Vulnerability Database for remediation and tracking.
    - Assura adopted a responsible disclosure policy in late 2021 to assist clients with the difficulty of getting commercial software developers to fix newly found vulnerabilities. That policy and several Assura's CVEs can be found here: https://assura.atlassian.net/wiki/spaces/VULNS/overview

4.0 FIRM OVERVIEW AND QUALIFICATIONS

Founded in 2007, **Assura** was built on a simple yet powerful mission: **securing the future—one client at a time.** With a vision to **democratize cybersecurity**, we firmly believe that **data security should be a right, not a privilege**. Our unwavering commitment to this belief has fueled over a decade of growth, enabling us to provide **cutting-edge, enterprise-grade cybersecurity solutions** to organizations of all sizes, including those with limited budgets.

ASSURA™
Cybersecurity uncompromised.

ISO 27001:2022 Certified & Committed to the Highest Standards of Security

Assura is **ISO 27001:2022 certified**, demonstrating our commitment to **maintaining the highest levels of information security and risk management.** This certification reinforces our dedication to **delivering services that meet internationally recognized security standards**, ensuring that our clients' sensitive data and systems remain **protected against evolving cyber threats**.

Affordable, High-Impact Cybersecurity for Education & Government

Assura understands that **institutions of higher education and government organizations play a vital role in shaping America's future**—yet they often struggle with budget constraints when it comes to cybersecurity. That's why we deliver **cost-effective, high-impact security solutions** that **protect mission-critical systems and sensitive data** from today's most sophisticated cyber threats.

By partnering with **James Madison University (JMU) and other VASCUPP organizations**, Assura helps ensure that **students, faculty, and staff operate in a secure digital environment**, free from the risks of **data breaches, ransomware, and malicious cyber threats.**

A Proven Team of Certified Cybersecurity Experts

Since day one, **Assura has set the standard for cybersecurity excellence** by employing **only highly certified professionals** in every service area. Our team holds top industry certifications, ensuring that clients receive **best-in-class security assessments, penetration testing, managed security services, and compliance consulting** that align with the latest industry frameworks, including **ISO 27001:2022, NIST, PCI-DSS, HIPAA, and OWASP**.

Why Organizations Trust Assura

- ✓ **18 years of cybersecurity excellence** – Providing **trusted security solutions since 2007**.
- ✓ **Mission-driven approach** – Focused on **protecting clients from evolving cyber threats, not just checking compliance boxes**.
- ✓ **Cost-effective solutions** – Ensuring **higher education institutions and government agencies** can access top-tier security without budgetary roadblocks.
- ✓ **Certified cybersecurity professionals** – No junior staff, no unqualified personnel—**only proven industry experts**.
- ✓ **ISO 27001:2022 Certified** – Ensuring **best-in-class information security management**.
- ✓ **Comprehensive security services** – Offering **penetration testing, vulnerability management, cloud security assessments, compliance consulting, and more**.

BARR CERTIFICATIONS
ISO 27001:2022

At Assura, we don't just **protect data**—we **protect futures**. Whether securing **higher education, government, healthcare, or private sector organizations**, Assura remains **committed to delivering cutting-edge, accessible cybersecurity solutions that empower institutions to thrive in a digitally connected world.**

4.1 SOCIO-ECONOMIC AND CERTIFICATION OVERVIEW

Assura is a **Richmond, Virginia-based, woman-owned cybersecurity advisory and managed services firm** that is **trusted by government agencies, universities, and private organizations** to provide cutting-edge security solutions. As a **certified Small, Woman-, and Minority-Owned (SWaM) and Disadvantaged Business Enterprise (DBE)** (Certification #661749) by the **Virginia Department of Small Business and Supplier Diversity**, Assura brings **exceptional value, diversity-driven innovation, and top-tier cybersecurity expertise** to every engagement.

CERTIFIED SWaM Small, Women and Minority-Owned
Supplier Diversity Strengthens the Commonwealth
by the Virginia Department of Small Business & Supplier Diversity

A Fast-Growing, Nationally Recognized Cybersecurity Leader

- **Inc. 5000 Honoree – Four Years Running & Poised for a Fifth in 2025!**
  Assura has been named to the **Inc. 5000 list of America's fastest-growing private companies for four consecutive years** and is on track to earn this prestigious recognition for a **fifth consecutive year in 2025**. This sustained growth is a testament to **our industry-leading expertise, client trust, and commitment to delivering top-tier cybersecurity services**.
- **Top 1% of Women-Owned Firms in the U.S.**
  Assura has been **recognized by the U.S. Women's Chamber of Commerce as being in the top 1% of women-owned firms nationwide**. This prestigious ranking was achieved through a rigorous evaluation of **business assets, leadership structure, and operational excellence**—further demonstrating Assura's **strong management, financial stability, and superior service delivery**.

The Competitive Advantage of Working with a Certified SWaM & DBE Firm

Partnering with a **SWaM and DBE-certified business** offers organizations **a strategic advantage in meeting diversity procurement goals** while also ensuring they receive **best-in-class cybersecurity services**. Assura's certifications **enhance supplier diversity initiatives** while providing **direct access to high-quality cybersecurity consulting and managed services** through streamlined procurement processes.

A Trusted Cybersecurity Partner for Higher Education & Government

In 2020, Assura was awarded the first **James Madison University (JMU) Information Technology Security Auditing Services contract**, enabling **higher education institutions and government agencies** to leverage **a simplified, cost-effective procurement vehicle** for world-class cybersecurity services. Over the past six years, **numerous universities and government organizations** have benefited from this contract, utilizing Assura's expertise for **cybersecurity planning, risk management, compliance, and managed security services**.

Why Choose Assura?

- ✓ **Inc. 5000 Fastest-Growing Company** – Recognized **four years in a row and poised for a fifth in 2025**.
- ✓ **SWaM & DBE Certified** – Supporting supplier diversity initiatives while delivering top-tier cybersecurity services.
- ✓ **Nationally Recognized Leader** – Ranked among the **top 1% of women-owned firms** in the U.S. for operational excellence.
- ✓ **Proven Experience – Successfully serving higher education institutions, government agencies, and enterprises** for 18 years.
- ✓ **Streamlined Procurement** – Easy access to Assura's services through **pre-established contracts and certifications**.
- ✓ **Unmatched Cybersecurity Expertise** – Offering **penetration testing, vulnerability management, compliance consulting, cloud security, and managed services**.

Organizations **don't just gain a cybersecurity provider when they partner with Assura**—they gain a **trusted, high-performance security ally committed to securing their future and strengthening supplier diversity initiatives**.

4.2 CONTRACT PERSONNEL

At Assura, excellence isn't just a goal—it's the standard. To ensure unparalleled service quality, we have assigned our most experienced, highly certified cybersecurity professionals to oversee this contract and deliver top-tier security solutions to James Madison University (JMU) and VASCUPP member organizations.

Our leadership team is committed to selecting the best resources for each engagement, carefully matching industry-leading experts with the unique needs of every request. This guarantees that clients receive the highest level of expertise, precision, and innovation while we remain on time, on budget, and exceeding expectations at every stage.

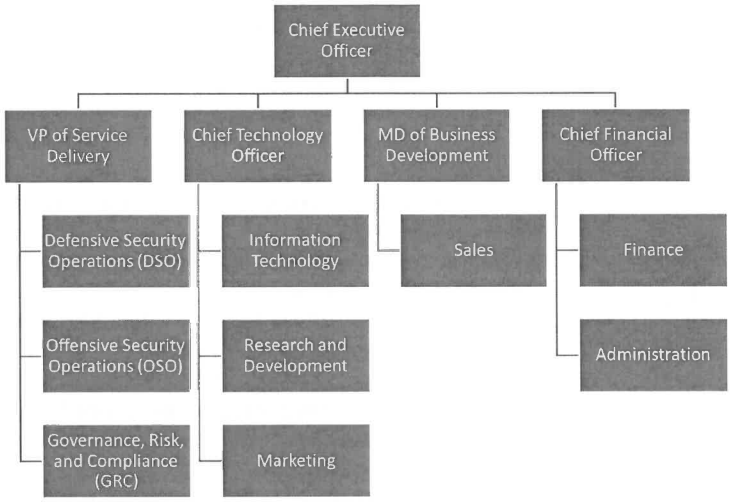
By leveraging deep industry experience, cutting-edge methodologies, and a customer-centric approach, the Assura team ensures that JMU and VASCUPP organizations benefit from:

- **Industry-Leading Expertise** – Our professionals hold top industry certifications, including CISSP, CISM, CEH, and OSCP – to name a few!
- **Decades of Real-World Experience** – The team comprises seasoned security professionals with extensive backgrounds in higher education, government, and private sector cybersecurity.
- **Proven Problem-Solvers** – Every engagement is led by experts who know how to tackle complex security challenges efficiently and effectively.
- **Commitment to Excellence** – The team is highly detail-oriented, results-driven, and passionate about delivering outstanding cybersecurity outcomes.
- **Clear Communication & Collaboration** – Our professionals excel at working with IT teams, executives, and stakeholders to provide actionable security insights without unnecessary technical jargon.

The following section outlines the highly skilled leadership team permanently assigned to this contract, ensuring JMU and VASCUPP organizations have direct access to elite cybersecurity professionals ready to support their security needs.

Leadership

Co-founder and CEO Karen Cole, CISA, CRISC, CBCP, MBCI, leads the company and holds ultimate responsibility for all services provided. She brings extensive knowledge of regulatory and client requirements for Virginia state and local governments, colleges, and universities. Ms. Cole is supported by a team of professionals dedicated to delivering high-quality services that exceed client expectations and requirements.



Service Delivery Team

Brett Bajcsi, a cybersecurity practitioner with 20 years of experience, leads our Service Delivery team. He is supported by Nick Berrie, Managing Director of Offensive Security Operations, David Mizell, Director of Defensive Security Operations, and Jonathon Neel, Director of Governance, Risk and Compliance Services. Each team oversees advisory and managed services.

Technology Team

Joshua Cole, our Chief Technology Officer, selects and integrates best-in-class cybersecurity and IT tools to meet the needs of our practitioners and clients. He directs the IT staff and services, working closely with partners to implement new functionality or enhancements with minimal operational impact. His team also includes our marketing group, which communicates service and technology updates clearly and professionally, tailoring messages to users with different levels of technical expertise.

Business Development Team

Kay Powers leads our Business Development team, collaborating with Service Delivery to engage current and potential clients. Her responsibilities include account management, service check-ins, and contract oversight. She is ultimately accountable for all account management activities. She and the Business Development team will manage all organizations utilizing this contract.

Finance and Administration

John Cox, our Chief Financial Officer, oversees fiscal and administrative management, maintaining accuracy and efficiency in financial operations.

Full resumes for these professionals are available upon request.

5.0 OFFEROR DATA SHEET

ATTACHMENT A

OFFEROR DATA SHEET

TO BE COMPLETED BY OFFEROR

1. QUALIFICATIONS OF OFFEROR: Offerors must have the capability and capacity in all respects to fully satisfy the contractual requirements.

2. YEARS IN BUSINESS: Indicate the length of time you have been in business providing these types of goods and services.

   Years 18 Months 0

3. REFERENCES: Indicate below a listing of at least five (5) organizations, either commercial or governmental/educational, that your agency is servicing. Include the name and address of the person the purchasing agency has your permission to contact.

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #
REDACTED			
REDACTED			
REDACTED			
REDACTED			
REDACTED			

4. List full names and addresses of Offeror and any branch offices which may be responsible for administering the contract.

   7330 Staples Mill Road, #292, Richmond, VA 23228

5. RELATIONSHIP WITH THE COMMONWEALTH OF VIRGINIA: Is any member of the firm an employee of the Commonwealth of Virginia who has a personal interest in this contract pursuant to the CODE OF VIRGINIA, SECTION 2.2-3100 – 3131?
   [ ] YES [×] NO

   IF YES, EXPLAIN:_____

6.0 SMALL BUSINESS CONTRACTING PLAN

Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Offeror Name: Assura, Inc. **Prepare Name:** Karen L. Cole, CEO

Date: January 30, 2025

Is your firm a **Small Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes X No_____

If yes, certification number: 661749 Certification date: 7-8-2016

Is your firm a **Woman-owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes X No_____

If yes, certification number: 661749 Certification date: 7-8-2016

Is your firm a **Minority-Owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes____ No X

If yes, certification number: _____ Certification date: _____

Is your firm a **Micro Business** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes X No_____

If yes, certification number: 661749 Certification date: 7-8-2016

Instructions: *Populate the table below to show your firm's plans for utilization of small, women-owned and minority-owned business enterprises in the performance of the contract. Describe plans to utilize SWAMs businesses as part of joint ventures, partnerships, subcontractors, suppliers, etc.*

Small Business: "Small business " means a business, independently owned or operated by one or more persons who are citizens of the United States or non-citizens who are in full compliance with United States immigration law, which, together with affiliates, has 250 or fewer employees, or average annual gross receipts of $10 million or less averaged over the previous three years.

Woman-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more women who are U.S. citizens or legal resident aliens, or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more women, and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified women-owned businesses are also a small business enterprise.**

Minority-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more minorities or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more minorities and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified minority-owned businesses are also a small business enterprise.**

Micro Business is a certified Small Business under the SWaM Program and has no more than twenty-five (25) employees **AND** no more than $3 million in average annual revenue over the three-year period prior to their certification.

All small, women, and minority owned businesses must be certified by the Commonwealth of Virginia Department of Small Business and Supplier Diversity (SBSD) to be counted in the SWAM program. Certification applications are available through SBSD at 800-223-0671 in Virginia, 804-786-6585 outside Virginia, or online at http://www.sbsd.virginia.gov/ (Customer Service).

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B (CNT'D)

Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Procurement Name and Number: Information Technology (IT) Security Auditing Services

Date Form Completed: 1/30/2025

Listing of Sub-Contractors, to include, Small, Woman Owned and Minority Owned Businesses for this Proposal and Subsequent Contract

Offeror / Proposer:

Assura, Inc. (Firm)

7330 Staples Mill Rd., #292, Richmond, VA 23228 (Address)

Karen L. Cole/804-767-4521 (Contact Person/No.)

Sub-Contractor's Name and Address	Contact Person & Phone Number	SBSD Certification Number	Services or Materials Provided	Total Subcontractor Contract Amount (to include change orders)	Total Dollars Paid Subcontractor to Date (to be submitted with request for payment from JMU)
Not Applicable as Assura is SWaM certified.	N/A	N/A	N/A	N/A	N/A

(Form shall be submitted with proposal and if awarded, again with submission of each request for payment)

RETURN OF THIS PAGE IS REQUIRED

7.0 VASCUPP SALES

REDACTED

Note: All client names and corporate financial details are considered proprietary and confidential.

8.0 PROPOSED COST

As detailed in Section 3: Goods and Services Plan and Methodology, services can be purchased as managed services or advisory projects. Billing can be a monthly flat fee for managed services, a fixed-fee with milestone billing for projects, or time and materials. For managed services and fixed-fee engagements, a detailed service quote will be developed based on variables such as network assets, testing targets, and types of functionality in the environment. For engagements that are based solely on time and materials, the following labor categories will be utilized.

Below is the starting hourly rate for each labor category broken. ***Assura offers substantial discounts from these rates depending on the scope and size of the project, as well as early payment terms.***

Labor Category	MSRP	Discount	VASCUPP Pricing
C-Level Executive - Off-site	$600.00	5.00%	$570.00
C-Level Executive - Onsite	$650.00	5.00%	$617.50
Digital Forensics Investigator - Off-site	$300.00	5.00%	$285.00
Digital Forensics Investigator - Onsite	$325.00	5.00%	$308.75
Digital Forensics Lead - Off-site	$350.00	5.00%	$332.50
Digital Forensics Lead - Onsite	$375.00	5.00%	$356.25
Digital Forensics Senior - Off-site	$375.00	5.00%	$356.25
Digital Forensics Senior - Onsite	$400.00	5.00%	$380.00
Senior Analyst - Off-site	$225.00	5.00%	$213.75
Senior Analyst- Onsite	$245.00	5.00%	$232.75
Senior Analyst - Off-site	$285.00	5.00%	$270.75
Senior Analyst - Onsite	$305.00	5.00%	$289.75
Analyst - Off-site	$195.00	5.00%	$185.25
Analyst- Onsite	$210.00	5.00%	$199.50
Principal Defensive Security Operations - Off-site	$370.00	5.00%	$351.50
Principal Defensive Security Operations - Onsite	$395.00	5.00%	$375.25
Principal Digital Forensics - Off-site	$400.00	5.00%	$380.00
Principal Digital Forensics - Onsite	$425.00	5.00%	$403.75
Principal GRC - Off-site	$295.00	5.00%	$280.25
Principal GRC - Onsite	$325.00	5.00%	$308.75
Principal Offensive Security Operations - Off-site	$325.00	5.00%	$308.75
Principal Offensive Security Operations - Onsite	$350.00	5.00%	$332.50
Security Engineering - Off-site	$375.00	5.00%	$356.25
Security Engineering - Onsite	$400.00	5.00%	$380.00
Penetration Tester - Off-site	$200.00	5.00%	$190.00
Penetration Tester - Onsite	$225.00	5.00%	$213.75
Penetration Tester Lead - Off-site	$225.00	5.00%	$213.75
Penetration Tester Lead - Onsite	$250.00	5.00%	$237.50
Penetration Tester Senior - Off-site	$300.00	5.00%	$285.00
Penetration Tester Senior - Onsite	$325.00	5.00%	$308.75
Project Manager - Off-site	$190.00	5.00%	$180.50
Project Manager - Onsite	$205.00	5.00%	$194.75

Labor Category	MSRP	Discount	VASCUPP Pricing
Security Engineer - Off-site	$300.00	5.00%	$285.00
Security Engineer - Onsite	$375.00	5.00%	$356.25
Security Engineer Lead - Off-site	$375.00	5.00%	$356.25
Security Engineer Lead - Onsite	$400.00	5.00%	$380.00
Security Engineer Senior - Off-site	$375.00	5.00%	$356.25
Security Engineer Senior - Onsite	$400.00	5.00%	$380.00
Senior Project Manager - Off-site	$205.00	5.00%	$194.75
Senior Project Manager - Onsite	$220.00	5.00%	$209.00
SOC Analyst/Engineer - Off-site	$200.00	5.00%	$190.00
SOC Analyst/Engineer - Onsite	$225.00	5.00%	$213.75
SOC Analyst/Engineer Lead - Off-site	$225.00	5.00%	$213.75
SOC Analyst/Engineer Lead - Onsite	$250.00	5.00%	$237.50
SOC Analyst/Engineer Senior - Off-site	$300.00	5.00%	$285.00
SOC Analyst/Engineer Senior - Onsite	$325.00	5.00%	$308.75

9.0 ADDITIONAL INFORMATION

Although this was not specifically requested in the RFP, Assura submits the following services for inclusion in the contract.

9.1 WORKSTATION AND MOBILE DEVICE RISK ASSESSMENT

Endpoints—**workstations, laptops, and mobile devices—are prime targets for cyber threats**. A single misconfiguration or unpatched vulnerability can provide attackers with an entry point, putting sensitive data and systems at risk. **Assura's Endpoint Risk Assessment ensures that every device is properly secured, hardened against attacks, and aligned with industry best practices and compliance standards.**

Cutting-Edge Assessment for Maximum Protection

Our team takes a **deep-dive, hands-on approach** to evaluating endpoint security configurations by scanning prototype configuration images with advanced security tools like **Nessus**. These assessments identify vulnerabilities, validate security policies, and ensure compliance with **client-specific standards** and **industry frameworks** such as **Center for Internet Security (CIS) benchmarks**.

Advanced Security Configuration Analysis

Assura's security professionals extract and analyze **critical security settings** to ensure endpoints are configured securely and operating at peak defense capability. Our approach includes:

✓ **Policy Compliance Verification** – Gathering detailed security configurations using tools such as gpresult /v and exporting security settings from **secpol.msc**.

✓ **Enterprise Mobility Management (EMM) Integration** – Ensuring endpoint configurations align with **client-deployed security policies and controls**.

✓ **Vulnerability & Configuration Auditing** – Identifying security gaps through advanced scanning techniques and expert manual review.

Comprehensive Malware Prevention & Endpoint Security Checks

Our assessment ensures that critical **endpoint security software**—such as **malware protection, host-based intrusion prevention systems, and firewalls**—is properly configured and fully operational. We verify that these essential security controls are:

- ✓ **Running the latest software versions** to defend against evolving threats.
- ✓ **Automatically downloading updated signature files** to detect new malware strains.
- ✓ **Configured for real-time monitoring and reporting of malicious activity.**

Actionable Insights & Expert Recommendations

Following the assessment, Assura delivers a **detailed security report** that includes:

- **Assessment results mapped to security requirements** (compliance policies, security baselines, and best practices).
- **Actionable recommendations** for configuration improvements, enhanced controls, and additional security measures.
- **Clear guidance** on strengthening workstation and mobile device security to minimize the attack surface.

Secure Endpoints, Reduce Risk, Protect Your Organization

With cyber threats constantly evolving, **organizations can't afford weak or misconfigured endpoints. Assura's Endpoint Risk Assessment empowers IT and security teams with the visibility and guidance needed to ensure that every device is fully secured, compliant, and resilient against cyber threats.**

9.2 INFORMATION SECURITY PROGRAM (GRC) ASSESSMENTS

Understanding and managing risk is the foundation of a strong information security program. Without comprehensive, standards-based risk assessments, organizations are left vulnerable to compliance failures, security gaps, and evolving cyber threats. Assura specializes in delivering high-value, in-depth Governance, Risk, and Compliance (GRC) focused risk assessments that empower organizations to identify, prioritize, and mitigate risks efficiently and effectively. These services can provide remediation support upon request as either an advisory project or as a managed service.

Risk Assessments Aligned with Industry Standards

Assura's risk assessments evaluate information security programs and critical systems against the most widely recognized security and compliance frameworks, including:

✓ **National Institute of Standards and Technology (NIST) Special Publication 800-53** – A comprehensive security and privacy control framework used across government and regulated industries.
✓ **NIST Cybersecurity Framework (CSF)** – A risk-based approach to managing cybersecurity that enhances resilience and regulatory alignment.
✓ **International Organization for Standardization (ISO) 27001:** Information Security Management Systems (ISMS) – The gold standard for security program management and continuous risk assessment.
✓ **Cybersecurity Maturity Model Certification (CMMC)** – A Department of Defense (DoD)-mandated framework for evaluating contractor cybersecurity readiness.
✓ **Payment Card Industry Data Security Standard (PCI DSS)** – A critical framework for protecting payment data and maintaining financial security compliance.

Beyond these industry frameworks, organizations must also conduct periodic risk assessments for:

- **Sensitive Systems** – Identifying vulnerabilities in mission-critical assets.
- **IT Disaster Recovery** – Ensuring resilience in the face of cyberattacks and system failures.
- **Third-Party Risk Management** – Assessing vendor and supply chain security risks to prevent external threats from impacting internal operations.

Delivering Actionable, Business-Focused Risk Assessments
A successful risk assessment isn't just about compliance—it's about enabling organizations to make informed business decisions that strengthen security, reduce risk, and drive operational success. Assura's cybersecurity experts provide:

✓ **In-Depth Risk Identification & Analysis** – Uncovering security weaknesses across people, processes, and technology.
✓ **Clear, Actionable Recommendations** – Delivering real-world guidance to mitigate risks without disrupting business operations.
✓ **Compliance Alignment & Future-Readiness** – Ensuring organizations meet current regulatory requirements while preparing for future security challenges.

Strengthen Security, Reduce Risk, and Ensure Compliance with Assura's Expert Risk Assessments
Organizations can't afford to guess when it comes to risk. Assura's comprehensive, business-aligned risk assessments provide the insights needed to proactively mitigate threats, enhance compliance, and protect critical assets.

Please see the following page for a full overview of the Virtual ISO service available to JMU and VASCUPP-authorized contract users.

The age of Democratizing Cybersecurity® is here.

At Assura we believe cybersecurity isn't a privilege, it's a right.

That's why we offer scalable solutions that fit the budget for any organization and will work hard to make sure you have the protection you need. We deliver world-class cybersecurity to organizations guaranteed to meet or exceed compliance regulations.

How does Virtual ISO™ solve your security and compliance challenges?

- We map out a fully functional and compliant program, then build it together
- You're guided through all program management decisions
- You decide how your organization will run the business end of cybersecurity
- All the unsexy work of documentation will be taken care of by your Virtual ISO™ team
- Your IT experts implement the necessary technical safeguards
- We work closely with your IT folks to make sure your system is secure
- Once the program is in place we continue to keep it maintained and compliant going forward
- Users are trained in security practices to help defend against attacks
- We take on cybersecurity planning activities such as system security plans if applicable
- In the unfortunate event of a cyber incident, we advise on how to handle it

What do you get with Virtual ISO™?

- Fractional Chief Information Security Officer (CISO)
- Security policies, standards, and guidelines
- Security processes, procedures, and plans
- Business Impact Analysis
- Security awareness training
- Security and compliance assessments
- Risk assessments
- Third-party vendor oversight
- Secure system development
- Investigate and lead response to security breaches
- Recurring compliance activities management
- Audit defense with AuditArmor™

JAMES MADISON UNIVERSITY

Request for Proposal

RFP# FDC-1220

Information Technology Security Auditing Services

December 17, 2024

James Madison University will be closed from December 20, 2024 – January 1, 2025

VIRGINIA ASSOCIATION OF STATE COLLEGE & UNIVERSITY PURCHASING PROFESSIONALS

VASCUPP

ANSWER/INQUIRY SUBMISSION FORM

DEADLINE FOR SUBMISSION OF QUESTIONS: Wednesday, January 8, 2025 @ 5:00 p.m.

****PROCEDURE FOR SUBMITTING QUESTIONS****

All questions and inquiries shall be formally submitted on this document. Questions shall be submitted in writing and shall reference, whenever possible, the Page, Section, and Item number within the Statement of Needs specifications of this document that the question is in reference to.

Questions shall be submitted to Doug Chester at the following e-mail address: chestefd@jmu.edu.

Answers to all questions received will be issued through a written addendum (if applicable) and become a part of the permanent record of this solicitation.

Date: _____

Project Location: James Madison University
Project # & Title: FDC-1220 Information Technology Security Auditing Services

The following question concerns: (indicate)

RFP Document: Section (number) _____, Page _____, Paragraph _____,

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Question submitted by:

_____

Name Organization E-mail Address

REQUEST FOR PROPOSAL
RFP# FDC-1220

Issue Date: **December 17, 2024**

Title: **Information Technology Security Auditing Services**

Issuing Agency: **Commonwealth of Virginia**
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Building
First Floor, Suite 1023
Harrisonburg, VA 22807

Period of Contract: From Date of Award Through One Year (Renewable)

Sealed Proposals Will Be Received Until 2:00 PM on January 21, 2025 for Furnishing The Services Described Herein. (See Special Terms & Conditions "D. Late Proposals")

SEALED PROPOSALS MAY BE MAILED, EXPRESS MAILED, SUBMITTED IN eVA, OR HAND DELIVERED DIRECTLY TO THE ISSUING AGENCY SHOWN ABOVE.

All Inquiries For Information And Clarification Should Be Directed To: Doug Chester, Buyer Senior, Procurement Services, chestefd@jmu.edu; 540-568-4272; (Fax) 540-568-7935 not later than five business days before the proposal closing date.

NOTE: THE SIGNED PROPOSAL AND ALL ATTACHMENTS SHALL BE RETURNED.
In compliance with this Request for Proposal and to all the conditions imposed herein, the undersigned offers and agrees to furnish the goods/services in accordance with the attached signed proposal or as mutually agreed upon by subsequent negotiation.

Name and Address of Firm:

_____

_____

_____

By: _____
(Signature)

Name: _____
(Please Print)

Date: _____ Title: _____

Web Address: _____ Phone: _____

Email: _____ Fax #: _____

ACKNOWLEDGE RECEIPT OF ADDENDUM: #1_____ #2_____ #3_____ #4_____ #5_____ (please initial)

SMALL, WOMAN OR MINORITY OWNED BUSINESS:
ÿ YES; ÿ NO; ***IF YES*** ⇒⇒ ÿ SMALL; ÿ WOMAN; ÿ MINORITY ***IF MINORITY***: ÿ AA; ÿ HA; ÿ AsA; ÿ NW; ÿ Micro

Note: This public body does not discriminate against faith-based organizations in accordance with the *Code of Virginia*, § 2.2-4343.1 or against an offeror because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment.

REQUEST FOR PROPOSAL

RFP # FDC-1220

TABLE OF CONTENTS

I. PURPOSE

The purpose of this Request for Proposal (RFP) is to solicit sealed proposals from qualified sources to enter into a contract to provide Information Technology (IT) Security Auditing Services for James Madison University (JMU), an agency of the Commonwealth of Virginia. Initial contract shall be for one (1) year with an option to renew for four (4) additional one-year periods.

II. BACKGROUND

James Madison University (JMU) is a comprehensive public institution in Harrisonburg, Virginia with an enrollment of approximately 22,000 students and approximately 4,000 faculty and staff. There are over 600 individual departments on campus that support seven (7) academic divisions. The University offers over 120 majors, minors, and concentrations. Further information about the University can be found at the following website: www.jmu.edu.

The mission of James Madison University's Audit and Management Services (AMS) is to assist the university's management and the JMU Board of Visitors by providing independent, objective assurance and consulting services designed to add value and improve university operations.

A. Internal accounting controls are adequate and effective in promoting efficiency and in protecting the assets of the University.
B. Financial statements and reports, whether for internal or external use, comply with established policies, generally accepted accounting principles, and/or other applicable rules and regulations both State and Federal.
C. Operational policies promote the well-being of the University and are effective and enforced to the end that operational efficiency and effectiveness are achieved.
D. Adequate standards of business conduct are being observed.
E. Internal control over information security activities, either internal or as provided by the fiscal agent and other contractors, is sufficient to reasonably ensure efficient, accurate, and complete processing of University data with due regard to security.
F. Contractors who are providing services to the University are doing so in a manner in accordance with all contract provisions.
G. Contractor billings conform to the predetermined formats and contain sufficient information to fully support University evaluation and payment.
H. University data in the hands of contractors is maintained in a secure and efficient manner according to formal backup, disaster and data recovery plans.

III. SMALL, WOMAN-OWNED AND MINORITY PARTICIPATION

It is the policy of the Commonwealth of Virginia to contribute to the establishment, preservation, and strengthening of small businesses and businesses owned by women and minorities, and to encourage their participation in State procurement activities. The Commonwealth encourages contractors to provide for the participation of small businesses and businesses owned by women and minorities through partnerships, joint ventures, subcontracts, and other contractual opportunities. Attachment B contains information on reporting spend data with subcontractors.

IV. STATEMENT OF NEEDS

A. James Madison University desires to contract with qualified firms to provide expertise and a range of services to support technologies used by the University. The contractor shall serve on special projects as a technology expert when requested and as needed. Reports shall be provided back to the University summarizing options and providing recommendations. The contractor shall serve as a technology advisor to understand, communicate, and propose solutions as requested. The contractor shall serve as a resource for research, implementation, troubleshooting, and other technical tasks to support the efforts of James Madison University Information Technology (JMU IT) staff. Functional consultants shall be represented by the Contractor as experts in the tasks and functions assigned. The University reserves the right to accept or reject any proposed or assigned consultant, without cause, at any time during the duration of the contract.

B. The selected contractor(s) shall supply professionally certified staff, at hourly rates, qualified to perform IT Security Audits at the direction of the Director of Internal Audit and Management Services. James Madison University does not guarantee any work will be assigned to the selected contractor(s). If multiple awards are issued because of this solicitation, JMU reserves the right to select the contractor who, in their sole opinion, is best suited for each particular project on a project-by-project basis.

C. The University's AMS requires, at a minimum, the following supplemental support for its IT auditing functions:

1. Describe your company's plan to provide certified professional staff to perform a wide range of IT audits of various IT activities and processes under the direction of the Director or staff of AMS. The list below includes audits currently performed by University personnel or by the staff of contractors performing under formal statement of work agreements with the University.*

    a. External Vulnerability Scanning
    b. Wireless Network Assessment
    c. Firewall and Router Security Assessment
    d. Server Configurations Assessment
    e. Database Architecture Security Assessment
    f. Network Scanning Process Assessment
    g. Web Application Security Assessments
    h. Active Directory Security Assessment
    i. Penetration Testing
    j. Telecommunications

    **Definition of Term – Certified Professional is defined as holding current Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified Information Systems Manager (CISM), Microsoft Certified Professional (MCP), Cisco Certified Network Associate (CCNA), Information Systems Security Management Professional (ISSMP).*

2. Describe your company's history in working with any institutions of higher education, especially those within the Commonwealth of Virginia.

    Specific scope requirements and deliverables will be included in an individual statement of work (SOW) for each separate project.

D. Billing Rate:

The Offeror shall provide an off-site hourly rate broken down by position type for the proposed services and a flat fee onsite hourly rate that includes all billables (e.g., travel, lodging, etc.). Pricing for all other products and services shall also be included.

E. Additional Information

1. The number of FTEs could vary for each project; however, most projects can be completed by one person if that person has the expertise.

2. For each project, the contractor is expected to provide project management for the work agreed upon in the statement of work.

3. The contractor will be paid according to the statement of work developed for a given project. If applicable, JMU will issue a 1099 to the contractor for the amount paid in the calendar year.

4. The statement of work for each project will outline the expected hours and projected timeline.

5. A statement of work will be developed with a selected contractor for each project. The contractor is expected to provide project management, personnel, and any licensed software necessary for the work agreed upon in the statement of work.

6. JMU follows ISO 27002 for security framework guidance and networking equipment compliance, along with industry-standard best practices.

7. The overall contract may be awarded to multiple companies as needed to ensure that JMU has the expertise to support our audit plan. Each project will then be contracted separately with a selected contractor. A pre-audit conference is conducted to develop the scope of work for each project. The contractor then submits a proposal for the project with an estimate of the project's hours (and total cost). Approval of the proposal by AMS and the issuance of a purchase order to authorize the work create the contract for the project.

   The examples of IT audits listed in IV.C.1. and below are typical audits of short duration (two days to two months). Each audit is considered a separate project and may be awarded to a contractor based on a specific statement of work agreement. Projects are scheduled based on the needs of the university, peak system usage times, and contractor availability. The statement of work for each project will outline the project's scope, the expected hours, and projected timeline. For each project, the statement of work will be developed with input from the selected contractor, IT, and JMU Audit and Management Services. The contractor will be expected to provide project management, personnel, and any licensed software necessary for the work agreed upon in the statement of work.

   Depending upon the project, the work may be done entirely off-site or require on-site testing with off-site report writing and follow-up.

V. PROPOSAL PREPARATION AND SUBMISSION

A. GENERAL INSTRUCTIONS

To ensure timely and adequate consideration of your proposal, offerors are to limit all contact, whether verbal or written, pertaining to this RFP to the James Madison University Procurement Office for the duration of this Proposal process. Failure to do so may jeopardize further consideration of Offeror's proposal.

ELECTRONIC OR PAPER SUBMISSIONS MAY BE ACCEPTED FOR THIS PROPOSAL. INSTRUCTIONS BELOW FOR OFFEROR'S CHOSEN METHOD (A. ELECTRONIC SUBMISSION or B. PAPER RESPONSE).

1. RFP Response: In order to be considered for selection, the **Offeror shall submit a complete response to this RFP**; and shall submit to the issuing Purchasing Agency:

   a. **ELECTRONIC SUBMISSION**:

      i. ELECTRONIC RESPONSES SUBMITTED THROUGH eVA WILL BE ACCEPTED. **Emailed responses will not be accepted.** Please see below, "eVA Procurement Website and Registration" for additional information on registration. It is the responsibility of the Supplier to ensure their proposal and all required documentation is properly completed, readable, and uploaded to eVA. Suppliers should allow sufficient time to account for any technical difficulties they may encounter during online submission or uploading of the documents. In the event of any technical difficulties, Suppliers shall contact the eVA Customer Care Center at 1-866-289-7367 or via email at eVACustomerCare@DGS.virginia.gov.

      ii. eVA Procurement Website and Registration The Commonwealth's procurement portal, eVA, located at http://www.eva.virginia.gov, provides information about Commonwealth solicitations and awards. Suppliers shall be registered in eVA in order submit a proposal to this

RFP. To register with eVA, select "Register Now" on the eVA website homepage, http://www.eva.virginia.gov. For registration instructions and assistance, as well as instructions on how to submit proposals and accept orders please select "I Sell to Virginia". Suppliers are encouraged to check this site on a regular basis and, in particular, prior to submission of proposals to identify any amendments to the RFP that may have been issued.

iii. Electronic Responses submitted through eVA shall be in WORD format or searchable PDF of the entire proposal, INCLUDING ALL ATTACHMENTS. PDFs must be submitted in an unlocked format. Any proprietary information should be clearly marked in accordance with Section V.4.e below.

b. **PAPER SUBMISSIONS:**

i. **One (1) original** and **three (3) copies** of the entire proposal, INCLUDING ALL ATTACHMENTS. Any proprietary information should be clearly marked in accordance with V.4.e. below.

ii. **One (1) electronic copy in WORD format or searchable PDF** (*flash drive*) of the entire proposal, INCLUDING ALL ATTACHMENTS. Any proprietary information should be clearly marked in accordance with 3.f. below.

iii. Each copy of the proposal should be bound or contained in a single volume where practical. All documentation submitted with the proposal should be contained in that single volume.

iv. See additional information in Section VIII.C, *IDENIFICATION OF PROPSAL ENVELOPE*.

2. Should the proposal contain **proprietary information**, **provide one (1) redacted copy of the proposal** and all attachments with **proprietary portions removed or blacked out**. This copy should be clearly marked *"Redacted Copy"* on the front cover. The classification of an entire proposal document, line-item prices, and/or total proposal prices as proprietary or trade secrets is not acceptable. JMU shall not be responsible for the Contractor's failure to exclude proprietary information from this redacted copy.

   No other distribution of the proposal shall be made by the Offeror.

3. The version of the solicitation issued by JMU Procurement Services, as amended by an addenda, is the mandatory controlling version of the document. Any modification of, or additions to, the solicitation by the Offeror shall not modify the official version of the solicitation issued by JMU Procurement services unless accepted in writing by the University. Such modifications or additions to the solicitation by the Offeror may be cause for rejection of the proposal; however, JMU reserves the right to decide, on a case-by-case basis in its sole discretion, whether to reject such a proposal. If the modification or additions are not identified until after the award of the contract, the controlling version of the solicitation document shall still be the official state form issued by Procurement Services.

4. Proposal Preparation

   a. Proposals shall be signed by an authorized representative of the Offeror. All information requested should be submitted. Failure to submit all information requested may result in the purchasing agency requiring prompt submissions of missing information and/or giving a lowered evaluation of the proposal. Proposals which are substantially incomplete or lack key information may be rejected by the purchasing agency. Mandatory requirements are those required by law or regulation or are such that they cannot be waived and are not subject to negotiation.

   b. Proposals shall be prepared simply and economically, providing a straightforward, concise description of capabilities to satisfy the requirements of the RFP. Emphasis should be placed on completeness and clarity of content.

c. Proposals should be organized in the order in which the requirements are presented in the RFP. All pages of the proposal should be numbered. Each paragraph in the proposal should reference the paragraph number of the corresponding section of the RFP. It is also helpful to cite the paragraph number, sub letter, and repeat the text of the requirement as it appears in the RFP. If a response covers more than one page, the paragraph number and sub letter should be repeated at the top of the next page. The proposal should contain a table of contents which cross references the RFP requirements. Information which the offeror desires to present that does not fall within any of the requirements of the RFP should be inserted at the appropriate place or be attached at the end of the proposal and designated as additional material. Proposals that are not organized in this manner risk elimination from consideration if the evaluators are unable to find where the RFP requirements are specifically addressed.

d. As used in this RFP, the terms "must", "shall", "should" and "may" identify the criticality of requirements. "Must" and "shall" identify requirements whose absence will have a major negative impact on the suitability of the proposed solution. Items labeled as "should" or "may" are highly desirable, although their absence will not have a large impact and would be useful, but are not necessary. Depending on the overall response to the RFP, some individual "must" and "shall" items may not be fully satisfied, but it is the intent to satisfy most, if not all, "must" and "shall" requirements. The inability of an offeror to satisfy a "must" or "shall" requirement does not automatically remove that offeror from consideration; however, it may seriously affect the overall rating of the offeror' proposal.

e. Each copy of the proposal should be bound or contained in a single volume where practical. All documentation submitted with the proposal should be contained in that single volume.

f. Ownership of all data, materials and documentation originated and prepared for the State pursuant to the RFP shall belong exclusively to the State and be subject to public inspection in accordance with the Virginia Freedom of Information Act. Trade secrets or proprietary information submitted by the offeror shall not be subject to public disclosure under the Virginia Freedom of Information Act; however, the offeror must invoke the protection of Section 2.2-4342F of the Code of Virginia, in writing, either before or at the time the data is submitted. **The written notice must specifically identify the data or materials to be protected and state the reasons why protection is necessary. The proprietary or trade secret materials submitted must be identified by some distinct method such as highlighting or underlining and must indicate only the specific words, figures, or paragraphs that constitute trade secret or proprietary information. The classification of an entire proposal document, line-item prices and/or total proposal prices as proprietary or trade secrets is not acceptable. Marking an entire proposal as confidential or attempts to prevent disclosure of pricing information by designating it as confidential, proprietary or trade secret will be ignored.**

5. Oral Presentation: Offerors who submit a proposal in response to this RFP may be required to give an oral presentation of their proposal to James Madison University. This provides an opportunity for the Offeror to clarify or elaborate on the proposal. This is a fact-finding and explanation session only and does not include negotiation. James Madison University will schedule the time and location of these presentations. Oral presentations are an option of the University and may or may not be conducted. Therefore, proposals should be complete.

B. SPECIFIC PROPOSAL INSTRUCTIONS

Proposals should be as thorough and detailed as possible so that James Madison University may properly evaluate your capabilities to provide the required services. Offerors are required to submit the following items as a complete proposal:

1. Return RFP cover sheet and all addenda acknowledgements, if any, signed and filled out as required. (Electronic signature shall be accepted, i.e. Adobe Sign, DocuSign, etc.)

2. Plan and methodology for providing the goods/services as described in Section IV. Statement of Needs of this Request for Proposal.

3. A written narrative statement to include, but not be limited to, the expertise, qualifications, and experience of the firm and resumes of specific personnel to be assigned to perform the work.

4. Offeror Data Sheet, included as *Attachment A* to this RFP.

5. Small Business Subcontracting Plan, included as *Attachment B* to this RFP. Offeror shall provide a Small Business Subcontracting plan which summarizes the planned utilization of Department of Small Business and Supplier Diversity (SBSD)-certified small businesses which include businesses owned by women and minorities, when they have received Department of Small Business and Supplier Diversity (SBSD) small business certification, under the contract to be awarded as a result of this solicitation. This is a requirement for all prime contracts in excess of $100,000 unless no subcontracting opportunities exist.

6. Identify the amount of sales your company had during the last twelve months with each VASCUPP Member Institution. A list of VASCUPP Members can be found at: www.VASCUPP.org.
7. Proposed Cost. See Section X. Pricing Schedule of this Request for Proposal.

VI. EVALUATION AND AWARD CRITERIA

A. EVALUATION CRITERIA

Proposals shall be evaluated by James Madison University using the following criteria:

		Points
1.	Quality of products/services offered and suitability for intended purposes	25
2.	Qualifications and experience of Offeror in providing the goods/services	25
3.	Specific plans or methodology to be used to perform the services	20
4.	Participation of Small, Women-Owned, & Minority (SWaM) Businesses	10
5.	Cost	20
		100

B. AWARD TO MULTIPLE OFFERORS: Selection shall be made of two or more offerors deemed to be fully qualified and best suited among those submitting proposals on the basis of the evaluation factors included in the Request for Proposals, including price, if so stated in the Request for Proposals. Negotiations shall be conducted with the offerors so selected. Price shall be considered, but need not be the sole determining factor. After negotiations have been conducted with each offeror so selected, the agency shall select the offeror which, in its opinion, has made the best proposal, and shall award the contract to that offeror. The Commonwealth reserves the right to make multiple awards as a result of this solicitation. The Commonwealth may cancel this Request for Proposals or reject proposals at any time prior to an award, and is not required to furnish a statement of the reasons why a particular proposal was not deemed to be the most advantageous. Should the Commonwealth determine in writing and in its sole discretion that only one offeror is fully qualified, or that one offeror is clearly more highly qualified than the others under consideration, a contract may be negotiated and awarded to that offeror. The award document will be a contract incorporating by reference all the requirements, terms and conditions of the solicitation and the contractor's proposal as negotiated.

VII. GENERAL TERMS AND CONDITIONS

A. PURCHASING MANUAL: This solicitation is subject to the provisions of the Commonwealth of Virginia's Purchasing Manual for Institutions of Higher Education and Their Vendors and any revisions thereto, which are hereby incorporated into this contract in their entirety. A copy of the manual is available for review at the purchasing office. In addition, the manual may be accessed electronically at http://www.jmu.edu/procurement or a copy can be obtained by calling Procurement Services at (540) 568-3145.

B. APPLICABLE LAWS AND COURTS: This solicitation and any resulting contract shall be governed in all respects by the laws of the Commonwealth of Virginia and any litigation with respect thereto shall be brought in the courts of the Commonwealth. The Contractor shall comply with applicable federal, state and local laws and regulations.

C. ANTI-DISCRIMINATION: By submitting their proposals, offerors certify to the Commonwealth that they will conform to the provisions of the Federal Civil Rights Act of 1964, as amended, as well as the Virginia Fair Employment Contracting Act of 1975, as amended, where applicable, the Virginians With Disabilities Act, the Americans With Disabilities Act and §10 of the Rules Governing Procurement, Chapter 2, Exhibit J, Attachment 1 (available for review at http://www.jmu.edu/procurement). If the award is made to a faith-based organization, the organization shall not discriminate against any recipient of goods, services, or disbursements made pursuant to the contract on the basis of the recipient's religion, religious belief, refusal to participate in a religious practice, or on the basis of race, age, color, gender, sexual orientation, gender identity, or national origin and shall be subject to the same rules as other organizations that contract with public bodies to account for the use of the funds provided; however, if the faith-based organization segregates public funds into separate accounts, only the accounts and programs funded with public funds shall be subject to audit by the public body. *(§6 of the Rules Governing Procurement*).

In every contract over $10,000 the provisions in 1. and 2. below apply:

1. During the performance of this contract, the contractor agrees as follows:

   a. The contractor will not discriminate against any employee or applicant for employment because of race, religion, color, sex, sexual orientation, gender identity, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment, except where there is a bona fide occupational qualification reasonably necessary to the normal operation of the contractor. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause.

   b. The contractor, in all solicitations or advertisements for employees placed by or on behalf of the contractor, will state that such contractor is an equal opportunity employer.

   c. Notices, advertisements, and solicitations placed in accordance with federal law, rule, or regulation shall be deemed sufficient for the purpose of meeting these requirements.

2. The contractor will include the provisions of 1. above in every subcontract or purchase order over $10,000, so that the provisions will be binding upon each subcontractor or vendor.

D. ETHICS IN PUBLIC CONTRACTING: By submitting their proposals, offerors certify that their proposals are made without collusion or fraud and that they have not offered or received any kickbacks or inducements from any other offeror, supplier, manufacturer or subcontractor in connection with their proposal, and that they have not conferred on any public employee having official responsibility for this procurement transaction any payment, loan, subscription, advance, deposit of money, services or anything of more than nominal value, present or promised, unless consideration of substantially equal or greater value was exchanged.

E. IMMIGRATION REFORM AND CONTROL ACT OF 1986: By entering into a written contract with the Commonwealth of Virginia, the Contractor certifies that the Contractor does not, and shall not during the performance of the contract for goods and services in the Commonwealth, knowingly employ an unauthorized alien as defined in the federal Immigration Reform and Control Act of 1986.

F. DEBARMENT STATUS: By submitting their proposals, offerors certify that they are not currently debarred by the Commonwealth of Virginia from submitting proposals on contracts for the type of goods and/or services covered by this solicitation, nor are they an agent of any person or entity that is currently so debarred.

G. ANTITRUST: By entering into a contract, the contractor conveys, sells, assigns, and transfers to the Commonwealth of Virginia all rights, title and interest in and to all causes of action it may now have or hereafter acquire under the antitrust laws of the United States and the Commonwealth of Virginia, relating to the particular goods or services purchased or acquired by the Commonwealth of Virginia under said contract.

H. MANDATORY USE OF STATE FORM AND TERMS AND CONDITIONS RFPs: Failure to submit a proposal on the official state form provided for that purpose may be a cause for rejection of the proposal. Modification of or additions to the General Terms and Conditions of the solicitation may be cause for rejection of the proposal; however, the Commonwealth reserves the right to decide, on a case by case basis, in its sole discretion, whether to reject such a proposal.

I. CLARIFICATION OF TERMS: If any prospective offeror has questions about the specifications or other solicitation documents, the prospective offeror should contact the buyer whose name appears on the face of the solicitation no later than five working days before the due date. Any revisions to the solicitation will be made only by addendum issued by the buyer.

J. PAYMENT:

1. To Prime Contractor:

    a. Invoices for items ordered, delivered and accepted shall be submitted by the contractor directly to the payment address shown on the purchase order/contract. All invoices shall show the state contract number and/or purchase order number; social security number (for individual contractors) or the federal employer identification number (for proprietorships, partnerships, and corporations).

    b. Any payment terms requiring payment in less than 30 days will be regarded as requiring payment 30 days after invoice or delivery, whichever occurs last. This shall not affect offers of discounts for payment in less than 30 days, however.

    c. All goods or services provided under this contract or purchase order, that are to be paid for with public funds, shall be billed by the contractor at the contract price, regardless of which public agency is being billed.

    d. The following shall be deemed to be the date of payment: the date of postmark in all cases where payment is made by mail, or the date of offset when offset proceedings have been instituted as authorized under the Virginia Debt Collection Act.

    e. Unreasonable Charges. Under certain emergency procurements and for most time and material purchases, final job costs cannot be accurately determined at the time orders are placed. In such cases, contractors should be put on notice that final payment in full is contingent on a determination of reasonableness with respect to all invoiced charges. Charges which appear to be unreasonable will be researched and challenged, and that portion of the invoice held in abeyance until a settlement can be reached. Upon determining that invoiced charges are not reasonable, the Commonwealth shall promptly notify the contractor, in writing, as to those charges which it considers unreasonable and the basis for the determination. A contractor may not institute legal action unless a settlement cannot be reached within thirty (30) days of notification. The provisions of this section do not relieve an agency of its prompt payment obligations with respect to those charges which are not in dispute (*Rules Governing Procurement, Chapter 2, Exhibit J, Attachment 1 § 53; available for review at http://www.jmu.edu/procurement*).

2. To Subcontractors:

    a. A contractor awarded a contract under this solicitation is hereby obligated:

(1) To pay the subcontractor(s) within seven (7) days of the contractor's receipt of payment from the Commonwealth for the proportionate share of the payment received for work performed by the subcontractor(s) under the contract; or

(2) To notify the agency and the subcontractors, in writing, of the contractor's intention to withhold payment and the reason.

b. The contractor is obligated to pay the subcontractor(s) interest at the rate of one percent per month (unless otherwise provided under the terms of the contract) on all amounts owed by the contractor that remain unpaid seven (7) days following receipt of payment from the Commonwealth, except for amounts withheld as stated in (2) above. The date of mailing of any payment by U. S. Mail is deemed to be payment to the addressee. These provisions apply to each sub-tier contractor performing under the primary contract. A contractor's obligation to pay an interest charge to a subcontractor may not be construed to be an obligation of the Commonwealth.

3. Each prime contractor who wins an award in which provision of a SWAM procurement plan is a condition to the award, shall deliver to the contracting agency or institution, on or before request for final payment, evidence and certification of compliance (subject only to insubstantial shortfalls and to shortfalls arising from subcontractor default) with the SWAM procurement plan. Final payment under the contract in question may be withheld until such certification is delivered and, if necessary, confirmed by the agency or institution, or other appropriate penalties may be assessed in lieu of withholding such payment.

4. The Commonwealth of Virginia encourages contractors and subcontractors to accept electronic and credit card payments.

K. PRECENDENCE OF TERMS: Paragraphs A through J of these General Terms and Conditions and the Commonwealth of Virginia Purchasing Manual for Institutions of Higher Education and their Vendors, shall apply in all instances. In the event there is a conflict between any of the other General Terms and Conditions and any Special Terms and Conditions in this solicitation, the Special Terms and Conditions shall apply.

L. QUALIFICATIONS OF OFFERORS: The Commonwealth may make such reasonable investigations as deemed proper and necessary to determine the ability of the offeror to perform the services/furnish the goods and the offeror shall furnish to the Commonwealth all such information and data for this purpose as may be requested. The Commonwealth reserves the right to inspect offeror's physical facilities prior to award to satisfy questions regarding the offeror's capabilities. The Commonwealth further reserves the right to reject any proposal if the evidence submitted by, or investigations of, such offeror fails to satisfy the Commonwealth that such offeror is properly qualified to carry out the obligations of the contract and to provide the services and/or furnish the goods contemplated therein.

M. TESTING AND INSPECTION: The Commonwealth reserves the right to conduct any test/inspection it may deem advisable to assure goods and services conform to the specifications.

N. ASSIGNMENT OF CONTRACT: A contract shall not be assignable by the contractor in whole or in part without the written consent of the Commonwealth.

O. CHANGES TO THE CONTRACT: Changes can be made to the contract in any of the following ways:

1. The parties may agree in writing to modify the scope of the contract. An increase or decrease in the price of the contract resulting from such modification shall be agreed to by the parties as a part of their written agreement to modify the scope of the contract.

2. The Purchasing Agency may order changes within the general scope of the contract at any time by written notice to the contractor. Changes within the scope of the contract include, but are not limited to, things such as services to be performed, the method of packing or shipment, and the place of delivery or installation. The contractor shall comply with the notice upon receipt. The contractor shall be compensated for any

additional costs incurred as the result of such order and shall give the Purchasing Agency a credit for any savings. Said compensation shall be determined by one of the following methods:

a. By mutual agreement between the parties in writing; or

b. By agreeing upon a unit price or using a unit price set forth in the contract, if the work to be done can be expressed in units, and the contractor accounts for the number of units of work performed, subject to the Purchasing Agency's right to audit the contractor's records and/or to determine the correct number of units independently; or

c. By ordering the contractor to proceed with the work and keep a record of all costs incurred and savings realized. A markup for overhead and profit may be allowed if provided by the contract. The same markup shall be used for determining a decrease in price as the result of savings realized. The contractor shall present the Purchasing Agency with all vouchers and records of expenses incurred and savings realized. The Purchasing Agency shall have the right to audit the records of the contractor as it deems necessary to determine costs or savings. Any claim for an adjustment in price under this provision must be asserted by written notice to the Purchasing Agency within thirty (30) days from the date of receipt of the written order from the Purchasing Agency. If the parties fail to agree on an amount of adjustment, the question of an increase or decrease in the contract price or time for performance shall be resolved in accordance with the procedures for resolving disputes provided by the Disputes Clause of this contract or, if there is none, in accordance with the disputes provisions of the Commonwealth of Virginia Purchasing Manual for Institutions of Higher Education and their Vendors. Neither the existence of a claim nor a dispute resolution process, litigation or any other provision of this contract shall excuse the contractor from promptly complying with the changes ordered by the Purchasing Agency or with the performance of the contract generally.

P. DEFAULT: In case of failure to deliver goods or services in accordance with the contract terms and conditions, the Commonwealth, after due oral or written notice, may procure them from other sources and hold the contractor responsible for any resulting additional purchase and administrative costs. This remedy shall be in addition to any other remedies which the Commonwealth may have.

Q. INSURANCE: By signing and submitting a proposal under this solicitation, the offeror certifies that if awarded the contract, it will have the following insurance coverage at the time the contract is awarded. For construction contracts, if any subcontractors are involved, the subcontractor will have workers' compensation insurance in accordance with§ 25 of the Rules Governing Procurement – Chapter 2, Exhibit J, Attachment 1, and 65.2-800 et. Seq. of the Code of Virginia (available for review at http://www.jmu.edu/procurement) The offeror further certifies that the contractor and any subcontractors will maintain these insurance coverage during the entire term of the contract and that all insurance coverage will be provided by insurance companies authorized to sell insurance in Virginia by the Virginia State Corporation Commission.

MINIMUM INSURANCE COVERAGES AND LIMITS REQUIRED FOR MOST CONTRACTS:

1. Workers' Compensation: Statutory requirements and benefits. Coverage is compulsory for employers of three or more employees, to include the employer. Contractors who fail to notify the Commonwealth of increases in the number of employees that change their workers' compensation requirement under the Code of Virginia during the course of the contract shall be in noncompliance with the contract.

2. Employer's Liability: $100,000

3. Commercial General Liability: $1,000,000 per occurrence and $2,000,000 in the aggregate. Commercial General Liability is to include bodily injury and property damage, personal injury and advertising injury, products and completed operations coverage. The Commonwealth of Virginia must be named as an additional insured and so endorsed on the policy.

4. Automobile Liability: $1,000,000 combined single limit. (*Required only if a motor vehicle not owned by the Commonwealth is to be used in the contract. Contractor must assure that the required coverage is maintained by the Contractor (or third party owner of such motor vehicle.*)

R. ANNOUNCEMENT OF AWARD: Upon the award or the announcement of the decision to award a contract over $100,000, as a result of this solicitation, the purchasing agency will publicly post such notice on the DGS/DPS eVA web site (www.eva.virginia.gov) for a minimum of 10 days.

S. DRUG-FREE WORKPLACE: During the performance of this contract, the contractor agrees to (i) provide a drug-free workplace for the contractor's employees; (ii) post in conspicuous places, available to employees and applicants for employment, a statement notifying employees that the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance or marijuana is prohibited in the contractor's workplace and specifying the actions that will be taken against employees for violations of such prohibition; (iii) state in all solicitations or advertisements for employees placed by or on behalf of the contractor that the contractor maintains a drug-free workplace; and (iv) include the provisions of the foregoing clauses in every subcontract or purchase order of over $10,000, so that the provisions will be binding upon each subcontractor or vendor.

For the purposes of this section, "drug-free workplace" means a site for the performance of work done in connection with a specific contract awarded to a contractor, the employees of whom are prohibited from engaging in the unlawful manufacture, sale, distribution, dispensation, possession or use of any controlled substance or marijuana during the performance of the contract.

T. NONDISCRIMINATION OF CONTRACTORS: An offeror, or contractor shall not be discriminated against in the solicitation or award of this contract because of race, religion, color, sex, sexual orientation, gender identity, national origin, age, disability, faith-based organizational status, any other basis prohibited by state law relating to discrimination in employment or because the offeror employs ex-offenders unless the state agency, department or institution has made a written determination that employing ex-offenders on the specific contract is not in its best interest. If the award of this contract is made to a faith-based organization and an individual, who applies for or receives goods, services, or disbursements provided pursuant to this contract objects to the religious character of the faith-based organization from which the individual receives or would receive the goods, services, or disbursements, the public body shall offer the individual, within a reasonable period of time after the date of his objection, access to equivalent goods, services, or disbursements from an alternative provider.

U. eVA BUSINESS TO GOVERNMENT VENDOR REGISTRATION, CONTRACTS, AND ORDERS: The eVA Internet electronic procurement solution, website portal www.eVA.virginia.gov, streamlines and automates government purchasing activities in the Commonwealth. The eVA portal is the gateway for vendors to conduct business with state agencies and public bodies. All vendors desiring to provide goods and/or services to the Commonwealth shall participate in the eVA Internet eprocurement solution by completing the free eVA Vendor Registration. All offerors must register in eVA and pay the Vendor Transaction Fees specified below; failure to register will result in the proposal being rejected. Vendor transaction fees are determined by the date the original purchase order is issued and the current fees are as follows:

Vendor transaction fees are determined by the date the original purchase order is issued and the current fees are as follows:

1. For orders issued July 1, 2014 and after, the Vendor Transaction Fee is:

    a. Department of Small Business and Supplier Diversity (SBSD) certified Small Businesses: 1% capped at $500 per order.

    b. Businesses that are not Department of Small Business and Supplier Diversity (SBSD) certified Small Businesses: 1% capped at $1,500 per order.

2. For orders issued prior to July 1, 2014 the vendor transaction fees can be found at www. eVA.virginia.gov.

3. The specified vendor transaction fee will be invoiced by the Commonwealth of Virginia Department of General Services approximately 60 days after the corresponding purchase order is issued and payable 30 days after the invoice date. Any adjustments (increases/decreases) will be handled through purchase order changes.

V. AVAILABILITY OF FUNDS: It is understood and agreed between the parties herein that the Commonwealth of Virginia shall be bound hereunder only to the extent of the funds available or which may hereafter become available for the purpose of this agreement.

W. PRICING CURRENCY: Unless stated otherwise in the solicitation, offerors shall state offered prices in U.S. dollars.

X. E-VERIFY REQUIREMENT OF ANY CONTRACTOR: Any employer with more than an average of 50 employees for the previous 12 months entering into a contract in excess of $50,000 with James Madison University to perform work or provide services pursuant to such contract shall register and participate in the E-Verify program to verify information and work authorization of its newly hired employees performing work pursuant to any awarded contract.

Y. CIVILITY IN STATE WORKPLACES: The contractor shall take all reasonable steps to ensure that no individual, while performing work on behalf of the contractor or any subcontractor in connection with this agreement (each, a "Contract Worker"), shall engage in 1) harassment (including sexual harassment), bullying, cyber-bullying, or threatening or violent conduct, or 2) discriminatory behavior on the basis of race, sex, color, national origin, religious belief, sexual orientation, gender identity or expression, age, political affiliation, veteran status, or disability.

The contractor shall provide each Contract Worker with a copy of this Section and will require Contract Workers to participate in training on civility in the State workplace. Upon request, the contractor shall provide documentation that each Contract Worker has received such training.

For purposes of this Section, "State workplace" includes any location, permanent or temporary, where a Commonwealth employee performs any work-related duty or is representing his or her agency, as well as surrounding perimeters, parking lots, outside meeting locations, and means of travel to and from these locations. Communications are deemed to occur in a State workplace if the Contract Worker reasonably should know that the phone number, email, or other method of communication is associated with a State workplace or is associated with a person who is a State employee.

The Commonwealth of Virginia may require, at its sole discretion, the removal and replacement of any Contract Worker who the Commonwealth reasonably believes to have violated this Section.

This Section creates obligations solely on the part of the contractor. Employees or other third parties may benefit incidentally from this Section and from training materials or other communications distributed on this topic , but the Parties to this agreement intend this Section to be enforceable solely by the Commonwealth and not by employees or other third parties.

VIII. SPECIAL TERMS AND CONDITIONS

A. AUDIT: The Contractor hereby agrees to retain all books, records, systems, and other documents relative to this contract for five (5) years after final payment, or until audited by the Commonwealth of Virginia, whichever is sooner. The Commonwealth of Virginia, its authorized agents, and/or State auditors shall have full access to and the right to examine any of said materials during said period.

B. CANCELLATION OF CONTRACT: James Madison University reserves the right to cancel and terminate any resulting contract, in part or in whole, without penalty, upon 60 days written notice to the contractor. In the event the initial contract period is for more than 12 months, the resulting contract may be terminated by either party, without penalty, after the initial 12 months of the contract period upon 60 days written notice to the other party. Any contract cancellation notice shall not relieve the contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation.

C. IDENTIFICATION OF PROPOSAL ENVELOPE: The signed proposal should be returned in a separate envelope or package, sealed and identified as follows:

From: _____
Name of Offeror Due Date Time

_____
Street or Box No. RFP #

_____
City, State, Zip Code RFP Title

Name of Purchasing Officer: _____

The envelope should be addressed as directed on the title page of the solicitation.

The Offeror takes the risk that if the envelope is not marked as described above, it may be inadvertently opened and the information compromised, which may cause the proposal to be disqualified. Proposals may be hand-delivered to the designated location in the office issuing the solicitation. No other correspondence or other proposals should be placed in the envelope.

D. LATE PROPOSALS: To be considered for selection, proposals must be received by the issuing office by the designated date and hour. The official time used in the receipt of proposals is that time on the automatic time stamp machine in the issuing office. Proposals received in the issuing office after the date and hour designated are automatically nonresponsive and will not be considered. The University is not responsible for delays in the delivery of mail by the U.S. Postal Service, private couriers, or the intra university mail system. It is the sole responsibility of the Offeror to ensure that its proposal reaches the issuing office by the designated date and hour.

E. UNDERSTANDING OF REQUIREMENTS: It is the responsibility of each offeror to inquire about and clarify any requirements of this solicitation that is not understood. The University will not be bound by oral explanations as to the meaning of specifications or language contained in this solicitation. Therefore, all inquiries deemed to be substantive in nature must be in writing and submitted to the responsible buyer in the Procurement Services Office. Offerors must ensure that written inquiries reach the buyer at least five (5) days prior to the time set for receipt of offerors proposals. A copy of all queries and the respective response will be provided in the form of an addendum to all offerors who have indicated an interest in responding to this solicitation. Your signature on your Offer certifies that you fully understand all facets of this solicitation. These questions may be sent via email directly to the Procurement Officer listed on the signature page of this solicitation or by Fax to 540/568-7935.

F. RENEWAL OF CONTRACT: This contract may be renewed by the Commonwealth for a period of four (4) successive one-year periods under the terms and conditions of the original contract except as stated in 1. and 2. below. Price increases may be negotiated only at the time of renewal. Written notice of the Commonwealth's intention to renew shall be given approximately 90 days prior to the expiration date of each contract period.

1. If the Commonwealth elects to exercise the option to renew the contract for an additional one-year period, the contract price(s) for the additional one year shall not exceed the contract price(s) of the original contract increased/decreased by no more than the percentage increase/decrease of the other services category of the CPI-W section of the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.

2. If during any subsequent renewal periods, the Commonwealth elects to exercise the option to renew the contract, the contract price(s) for the subsequent renewal period shall not exceed the contract price(s) of the previous renewal period increased/decreased by more than the percentage increase/decrease of the other services category of the CPI-W section of the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.

G. SUBMISSION OF INVOICES: All invoices shall be submitted within sixty days of contract term expiration for the initial contract period as well as for each subsequent contract renewal period. Any invoices submitted after the sixty-day period will not be processed for payment.

H. OPERATING VEHICLES ON JAMES MADISON UNIVERSITY CAMPUS: Operating vehicles on sidewalks, plazas, and areas heavily used by pedestrians is prohibited. In the unlikely event a driver should find it necessary to drive on James Madison University sidewalks, plazas, and areas heavily used by pedestrians, the driver must yield to pedestrians. For a complete list of parking regulations, please go to www.jmu.edu/parking; or to acquire a service representative parking permit, contact Parking Services at 540.568.3300. The safety of our students, faculty and staff is of paramount importance to us. Accordingly, violators may be charged.

I. COOPERATIVE PURCHASING / USE OF AGREEMENT BY THIRD PARTIES: It is the intent of this solicitation and resulting contract(s) to allow for cooperative procurement. Accordingly, any public body, (to include government/state agencies, political subdivisions, etc.), cooperative purchasing organizations, public or private health or educational institutions or any University related foundation and affiliated corporations may access any resulting contract if authorized by the Contractor.

Participation in this cooperative procurement is strictly voluntary. If authorized by the Contractor(s), the resultant contract(s) will be extended to the entities indicated above to purchase goods and services in accordance with contract terms. As a separate contractual relationship, the participating entity will place its own orders directly with the Contractor(s) and shall fully and independently administer its use of the contract(s) to include contractual disputes, invoicing and payments without direct administration from the University. No modification of this contract or execution of a separate agreement is required to participate; however, the participating entity and the Contractor may modify the terms and conditions of this contract to accommodate specific governing laws, regulations, policies, and business goals required by the participating entity. Any such modification will apply solely between the participating entity and the Contractor.

The Contractor will notify the University in writing of any such entities accessing this contract. The Contractor will provide semi-annual usage reports for all entities accessing the contract. The University shall not be held liable for any costs or damages incurred by any other participating entity as a result of any authorization by the Contractor to extend the contract. It is understood and agreed that the University is not responsible for the acts or omissions of any entity and will not be considered in default of the contract no matter the circumstances.

Use of this contract(s) does not preclude any participating entity from using other contracts or competitive processes as needed.

J. SMALL BUSINESS SUBCONTRACTING AND EVIDENCE OF COMPLIANCE:

1. It is the goal of the Commonwealth that 42% of its purchases are made from small businesses. This includes discretionary spending in prime contracts and subcontracts. All potential offerors are required to submit a Small Business Subcontracting Plan. Unless the offeror is registered as a Department of Small Business and Supplier Diversity (SBSD)-certified small business and where it is practicable for any portion of the awarded contract to be subcontracted to other suppliers, the contractor is encouraged to offer such subcontracting opportunities to SBSD-certified small businesses. This shall not exclude SBSD-certified women-owned and minority-owned businesses when they have received SBSD small business certification. No offeror or subcontractor shall be considered a Small Business, a Women-Owned Business or a Minority-Owned Business unless certified as such by the Department of Small Business and Supplier Diversity (SBSD) by the due date for receipt of proposals. If small business subcontractors are used, the prime contractor agrees to report the use of small business subcontractors by providing the purchasing office at a minimum the following information: name of small business with the SBSD certification number or FEIN, phone number, total dollar amount subcontracted, category type (small, women-owned, or minority-owned), and type of product/service provided. **This information shall be submitted to: JMU Office of Procurement Services, Attn: SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807 or swamreporting@jmu.edu .**

2. Each prime contractor who wins an award in which provision of a small business subcontracting plan is a condition of the award, shall deliver to the contracting agency or institution with every request for payment, evidence of compliance (subject only to insubstantial shortfalls and to shortfalls arising from subcontractor default) with the small business subcontracting plan. **This information shall be submitted to: JMU Office of Procurement Services, SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807 or swamreporting@jmu.edu** . When such business has been subcontracted to these firms and upon completion of the contract, the contractor agrees to furnish the purchasing office at a minimum the following information: name of firm with the Department of Small Business and Supplier Diversity (SBSD) certification number or FEIN number, phone number, total dollar amount subcontracted, category type (small, women-owned, or minority-owned), and type of product or service provided. Payment(s) may be withheld until compliance with the plan is received and confirmed by the agency or institution. The agency or institution reserves the right to pursue other appropriate remedies to include, but not be limited to, termination for default.

3. Each prime contractor who wins an award valued over $200,000 shall deliver to the contracting agency or institution with every request for payment, information on use of subcontractors that are not Department of Small Business and Supplier Diversity (SBSD)-certified small businesses. When such business has been subcontracted to these firms and upon completion of the contract, the contractor agrees to furnish the purchasing office at a minimum the following information: name of firm, phone number, FEIN number, total dollar amount subcontracted, and type of product or service provided. **This information shall be submitted to: JMU Office of Procurement Services, Attn: SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807 or swamreporting@jmu.edu** .

K. AUTHORIZATION TO CONDUCT BUSINESS IN THE COMMONWEALTH: A contractor organized as a stock or nonstock corporation, limited liability company, business trust, or limited partnership or registered as a registered limited liability partnership shall be authorized to transact business in the Commonwealth as a domestic or foreign business entity if so required by Title 13.1 or Title 50 of the Code of Virginia or as otherwise required by law. Any business entity described above that enters into a contract with a public body shall not allow its existence to lapse or its certificate of authority or registration to transact business in the Commonwealth, if so required under Title 13.1 or Title 50, to be revoked or cancelled at any time during the term of the contract. A public body may void any contract with a business entity if the business entity fails to remain in compliance with the provisions of this section.

L. PUBLIC POSTING OF COOPERATIVE CONTRACTS: James Madison University maintains a web-based contracts database with a public gateway access. Any resulting cooperative contract/s to this solicitation will be posted to the publicly accessible website. Contents identified as proprietary information will not be made public.

M. CRIMINAL BACKGROUND CHECKS OF PERSONNEL ASSIGNED BY CONTRACTOR TO PERFORM WORK ON JMU PROPERTY: The Contractor shall obtain criminal background checks on all of their contracted employees who will be assigned to perform services on James Madison University property. The results of the background checks will be directed solely to the Contractor. The Contractor bears responsibility for confirming to the University contract administrator that the background checks have been completed prior to work being performed by their employees or subcontractors. The Contractor shall only assign to work on the University campus those individuals whom it deems qualified and permissible based on the results of completed background checks. Notwithstanding any other provision herein, and to ensure the safety of students, faculty, staff and facilities, James Madison University reserves the right to approve or disapprove any contract employee that will work on JMU property. Disapproval by the University will solely apply to JMU property and should have no bearing on the Contractor's employment of an individual outside of James Madison University.

N. INDEMNIFICATION: Contractor agrees to indemnify, defend and hold harmless the Commonwealth of Virginia, its officers, agents, and employees from any claims, damages and actions of any kind or nature, whether at law or in equity, arising from or caused by the use of any materials, goods, or equipment of any kind or nature furnished by the contractor/any services of any kind or nature furnished by the contractor, provided that such liability is not attributable to the sole negligence of the using agency or to failure of the using agency to use the materials, goods, or equipment in the manner already and permanently described by the contractor on the materials, goods or equipment delivered.

O. ADDITIONAL GOODS AND SERVICES: The University may acquire other goods or services that the supplier provides than those specifically solicited. The University reserves the right, subject to mutual agreement, for the Contractor to provide additional goods and/or services under the same pricing, terms, and conditions and to make modifications or enhancements to the existing goods and services. Such additional goods and services may include other products, components, accessories, subsystems, or related services that are newly introduced during the term of this Agreement. Such additional goods and services will be provided to the University at favored nations pricing, terms, and conditions.

P. ADVERTISING: In the event a contract is awarded for supplies, equipment, or services resulting from this proposal, no indication of such sales or services to James Madison University will be used in product literature or advertising without the express written consent of the University. The contractor shall not state in any of its advertising or product literature that James Madison University has purchased or uses any of its products or services, and the contractor shall not include James Madison University in any client list in advertising and promotional materials without the express written consent of the University.

Q. PRIME CONTRACTOR RESPONSIBILITIES: The contractor shall be responsible for completely supervising and directing the work under this contract and all subcontractors that he may utilize, using his best skill and attention. Subcontractors who perform work under this contract shall be responsible to the prime contractor. The contractor agrees that he is as fully responsible for the acts and omissions of his subcontractors and of persons employed by them as he is for the acts and omissions of his own employees.

R. SUBCONTRACTS: No portion of the work shall be subcontracted without prior written consent of the purchasing agency. In the event that the contractor desires to subcontract some part of the work specified herein, the contractor shall furnish the purchasing agency the names, qualifications and experience of their proposed subcontractors. The contractor shall, however, remain fully liable and responsible for the work to be done by its subcontractor(s) and shall assure compliance with all requirements of the contract.

S. CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION: The contractor assures that information and data obtained as to personal facts and circumstances related to faculty, staff, students, and affiliates will be collected and held confidential, during and following the term of this agreement, and will not be divulged without the individual's and the agency's written consent and only in accordance with federal law or the Code of Virginia. This shall include FTI, which is a term of art and consists of federal tax returns and return information (and information derived from it) that is in contractor/agency possession or control which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI is categorized as sensitive but unclassified information and may contain personally identifiable information (PII). Contractors who utilize, access, or store personally identifiable information as part of the performance of a contract are required to safeguard this information and immediately notify the agency of any breach or suspected breach in the security of such information. Contractors shall allow the agency to both participate in the investigation of incidents and exercise control over decisions regarding external reporting. Contractors and their employees working on this project may be required to sign a confidentiality statement.

IX. METHOD OF PAYMENT

The contractor will be paid based on invoices submitted in accordance with the solicitation and any negotiations. James Madison University recognizes the importance of expediting the payment process for our vendors and suppliers; we request that our vendors and suppliers enroll in our bank's Comprehensive Payable options: either the Virtual Payables Virtual Card or the PayMode-X electronic deposit (ACH) to your bank account so that future payments are made electronically. Contractors signed up for the Virtual Payables process will receive the benefit of being paid Net 15. Additional information is available online at:
http://www.jmu.edu/financeoffice/accounting-operations-disbursements/cash-investments/vendor-payment-methods.shtml

X. PRICING SCHEDULE

The Offeror shall provide an off-site hourly rate broken down by position type for the proposed services and a flat fee onsite hourly rate that includes all billables (e.g., travel, lodging, etc.). Pricing for all other products and services shall also be included. The resulting contract will be cooperative, and pricing shall be inclusive for the attached Zone Map, of which JMU falls within Zone 2.

Specify any associated charge card processing fees, if applicable, to be billed to the university.

XI. ATTACHMENTS

Attachment A: Offeror Data Sheet

Attachment B: Small, Women, and Minority-owned Business (SWaM) Utilization Plan

Attachment C: Standard Contract Sample

Attachment D: Zone Map

ATTACHMENT A

OFFEROR DATA SHEET

TO BE COMPLETED BY OFFEROR

1. QUALIFICATIONS OF OFFEROR: Offerors must have the capability and capacity in all respects to fully satisfy the contractual requirements.

2. YEARS IN BUSINESS: Indicate the length of time you have been in business providing these types of goods and services.

   Years_____ Months_____

3. REFERENCES: Indicate below a listing of at least five (5) organizations, either commercial or governmental/educational, that your agency is servicing. Include the name and address of the person the purchasing agency has your permission to contact.

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #

4. List full names and addresses of Offeror and any branch offices which may be responsible for administering the contract.

5. RELATIONSHIP WITH THE COMMONWEALTH OF VIRGINIA: Is any member of the firm an employee of the Commonwealth of Virginia who has a personal interest in this contract pursuant to the CODE OF VIRGINIA, SECTION 2.2-3100 – 3131?
   [ ] YES [ ] NO
   IF YES, EXPLAIN:_____

ATTACHMENT B

Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Offeror Name: _____ Preparer Name: _____

Date: _____

Is your firm a **Small Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No_____

If yes, certification number: _____ Certification date:_____

Is your firm a **Woman-owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No_____

If yes, certification number: _____ Certification date:_____

Is your firm a **Minority-Owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes____ No_____

If yes, certification number: _____ Certification date:_____

Is your firm a **Micro Business** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No_____

If yes, certification number: _____ Certification date: _____

Instructions: *Populate the table below to show your firm's plans for utilization of small, women-owned and minority-owned business enterprises in the performance of the contract. Describe plans to utilize SWAMs businesses as part of joint ventures, partnerships, subcontractors, suppliers, etc.*

Small Business: "Small business " means a business, independently owned or operated by one or more persons who are citizens of the United States or non-citizens who are in full compliance with United States immigration law, which, together with affiliates, has 250 or fewer employees, or average annual gross receipts of $10 million or less averaged over the previous three years.

Woman-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more women who are U.S. citizens or legal resident aliens, or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more women, and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified women-owned businesses are also a small business enterprise.**

Minority-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more minorities or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more minorities and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified minority-owned businesses are also a small business enterprise.**

Micro Business is a certified Small Business under the SWaM Program and has no more than twenty-five (25) employees **AND** no more than $3 million in average annual revenue over the three-year period prior to their certification.

All small, women, and minority owned businesses must be certified by the Commonwealth of Virginia Department of Small Business and Supplier Diversity (SBSD) to be counted in the SWAM program. Certification applications are available through SBSD at 800-223-0671 in Virginia, 804-786-6585 outside Virginia, or online at http://www.sbsd.virginia.gov/ (Customer Service).

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B (CNT'D)

Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Procurement Name and Number: _____ Date Form Completed:_____

Listing of Sub-Contractors, to include, Small, Woman Owned and Minority Owned Businesses
for this Proposal and Subsequent Contract

Offeror / Proposer:

_____	_____	_____
Firm	Address	Contact Person/No.

Sub-Contractor's Name and Address	Contact Person & Phone Number	SBSD Certification Number	Services or Materials Provided	Total Subcontractor Contract Amount (to include change orders)	Total Dollars Paid Subcontractor to date (to be submitted with request for payment from JMU)

(Form shall be submitted with proposal and if awarded, a SWaM Sub-contractor Reporting Form shall be submitted to swamreporting@jmu.edu)

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT C

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No._____

This contract entered into this_____day of_____20____,by _____ hereinafter called the "Contractor" and Commonwealth of Virginia, James Madison University called the "Purchasing Agency".

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

SCOPE OF CONTRACT: The Contractor shall provide the services to the Purchasing Agency as set forth in the Contract Documents.

PERIOD OF PERFORMANCE: From_____ through_____

The contract documents shall consist of:

(1) This signed form;

(2) The following portions of the Request for Proposals dated _____:
- (a) The Statement of Needs,
- (b) The General Terms and Conditions,
- (c) The Special Terms and Conditions together with any negotiated modifications of those Special Conditions;
- (d) List each addendum that may be issued

(3) The Contractor's Proposal dated _____and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
- (a) Negotiations summary dated _____.

IN WITNESS WHEREOF, the parties have caused this Contract to be duly executed intending to be bound thereby.

CONTRACTOR:	PURCHASING AGENCY:
By:_____	By:_____
(Signature)	(Signature)
_____	_____
(Printed Name)	(Printed Name)
Title:_____	Title:_____

ATTACHMENT D

Zone Map

Virginia Association of State College & University Purchasing Professionals (VASCUPP)

List of member institutions by zones

Zone 1 George Mason University (Fairfax)	**Zone 2** James Madison University (Harrisonburg)	**Zone 3** University of Virginia (Charlottesville)
Zone 4 University of Mary Washington (Fredericksburg)	**Zone 5** Christopher Newport University (Newport News) College of William and Mary (Williamsburg) Norfolk State University (Norfolk) Old Dominion University (Norfolk)	**Zone 6** Virginia Commonwealth University (Richmond) Virginia State University (Petersburg)
Zone 7 Longwood University (Farmville)	**Zone 8** Virginia Military Institute (Lexington) Virginia Tech (Blacksburg) Radford University (Radford)	**Zone 9** University of Virginia - Wise (Wise)

JAMES MADISON UNIVERSITY

January 10, 2025

ADDENDUM NO.: One

TO ALL OFFERORS

REFERENCE:	Request for Proposal No:	RFP# FDC-1220
	Dated:	December 17, 2024
	Commodity:	Information Technology Security Auditing Services
	RFP Closing On:	~~January 21, 2025 at 2:00 p.m.~~
		January 30, 2025 @ 2:00 p.m.

Please note the clarifications and/or changes made on this proposal program:

Due to the number of questions received for this RFP, James Madison University has extended the closing date to **January 30, 2025, at 2:00 p.m**.

A second addendum will be posted next week with responses to vendor questions.

Signify receipt of this addendum by initialing *"Addendum #1"* on the signature page of your proposal.

Sincerely,
Doug Chester
Buyer Senior
Phone: 540-568-4272

January 16, 2025

ADDENDUM NO.: Two

TO ALL OFFERORS

REFERENCE:	Request for Proposal No:	RFP# FDC-1220
	Dated:	December 17, 2024
	Commodity:	IT Security Auditing Services
	RFP Closing On:	January 30, 2025 @ 2:00 p.m.

Please note the clarifications and/or changes made on this proposal program:

AMS refers to JMU's Office of Audit Management Services

The following questions are answered below:

1. Are the audits listed in a. through j. all intended to be completed in the one-year contract?

   Answer: The audits listed are a population of potential audits. Typically, 3-5 are selected each year.

2. Has the University contracted with outside service providers to conduct IT Security Audits in the past? If so:
   a. When were the most recent IT Security Audits conducted and what was the scope?
   b. Who was the service provider?

   Answer: Yes. We typically have 3-5 done annually by our contracted vendors.

3. Would the University be willing to share the results of prior IT Security Audits with the awarded vendors?

   Answer: Results are FOIA exempt. They could potentially contain sensitive security information and will not be shared.

4. Does the University have a preference for awarding this project to service providers who have conducted work within the Commonwealth of Virginia?

   Answer: The vendor must be registered to work within the Commonwealth of Virginia and with eVA (https://eva.virginia.gov).

5. Does the University's AMS intend to provide resources and staff to support the IT Security Audits, or is the vendor to provide all the resources?

   Answer: The IT Auditor in AMS manages the audits, assists consultants during the audit, arranges the entrance conference for each audit, and ensures consultants have what they need to complete the audit (credentials, etc.).

6. Will the requested IT Security Audits be required to be conducted to meet Institute of Internal Auditors (IIA) standards?

   Answer: Not required

7. Will the requested IT Security Audits be considered performance audits under Yellow Book?

Answer: No

8. What is the requested start and completion date of the one-year contract?

   Answer: The contract will start after the successful completion of the RPF process. The contract will last for one year and have four optional one-year renewals.

9. Does the University use an audit tracking or compliance software that the audit results will be imported into? If so, what?

   Answer: Documents related to each audit are stored in AMS automated workpaper system.

10. Does the University have an allocated budget for this engagement that can be shared with proposers?

    Answer: AMS has a fixed budget for IT Security Auditing projects.

11. The RFP states, "The selected contractor(s) shall supply professionally certified staff, at hourly rates, qualified to perform IT Security Audits at the direction of the Director of Internal Audit." This seems to indicate that all work will be performed in a staff aug capacity to where JMU leadership will supervise all of the winning bidder's team instead of the bidder's Partner/ Principal/Director's leadership. Can you confirm if this is accurate or if some audits will be co-sourced entirely to the bidder such that the bidder's leadership team is responsible for staff supervision and review of the final deliverables.

    Answer: The contractor chosen to conduct an audit will manage their own staff. AMS will provide assistance to ensure that they have what they need to complete the audit. See #5 answer

12. Does JMU have any estimate for what percentage of the audits or work hours will need to be performed onsite vs just done remotely?

    Answer: Onsite or remotely depends on the audit. Most are done remotely.

13. Does JMU have a planned annual budget for these services or some idea of how many audits will need to be staffed with the winning bidder?

    Answer: AMS has a fixed budget for IT Security Auditing projects. AMS meets with IT annually to discuss the year's upcoming IT audits. Cost is one of the factors that determine the number of audits.

14. Can you clarify if SWAM participation is required or optional, and how will the 10 pts for SWAM usage be scored?

    Answer: SWaM participation is not required. However, JMU strives to work with SWaM vendors whenever practicable. A SWaM vendor would get 10 points if they are a certified SWaM vendor (registered with the Virginia Department of Small Business and Supplier Development (VSBSD)). A non-SWaM vendor utilizing SWaM sub-contractor (registered with VSBSD) would receive some portion of the 10 points available.

15. Can you clarify whether the projects require a mix of on-site and off-site work, or are they predominantly one or the other?

    Answer: Audits are typically either on-site or remote and determined during planning.

16. How will the scope of work for each project be defined? Will templates or prior examples be provided?

    Answer: The scope of audits are typically defined during an entrance conference meeting.

17. What are JMU's highest-priority areas for IT security auditing? Are there any recent audit findings that should be addressed in these engagements?

    Answer: AMS conducts a risk assessment annually. In the past, audits have been on a three-year cycle. Systems that support critical functions are considered a higher priority to assess.

18. Will JMU require resumes or bios for assigned staff during each project proposal?

    Answer: Bios for staff are required for the initial review and selection process. We will select 3-5 organizations to have on contract.

19. Are subcontractors allowed, and if so, are there any restrictions or additional requirements?

    Answer: Yes, they are allowed. Organizations may need to provide bios for any subcontractors used prior to any audit.

20. Can you elaborate on the specific deliverables required for each type of audit (e.g., penetration testing, vulnerability scans, etc.)?

    Answer: A final draft report covering the audit scope, approach and any findings should be provided at the end of an engagement. Any supporting documentations should be provided as well. Scan results, etc.

21. Are sample reports or templates available for review?

    Answer: No. Report format is up to the consultant performing the audit as long as it covers the scope, methodology and findings/recommendations.

22. What specific systems, applications, or networks are in scope for the penetration testing? Are there any excluded systems, applications, or segments of the network?

    Answer: All of our systems are potential candidates for audits. What will be included in an audit will be determined during an entrance conference.

23. What are the primary objectives of the penetration testing (e.g., vulnerability identification, exploit validation, compliance verification)? Is the focus on internal, external, or hybrid penetration testing?

    Answer: Pen tests will be conducted from both internal and external perspectives. The objectives are determined during an entrance conference.

24. Does JMU have a preferred penetration testing methodology (e.g., OWASP Testing Guide, PTES, or NIST SP 800-115)?

    Answer: We do not have a preferred methodology as long as the methodology used is well known.

25. Are automated scanning tools allowed, or is manual testing preferred?

    Answer: Yes, automated scanning tools are allowed. Organizations are responsible for the appropriate use of any tool used during an audit.

26. How often does JMU require penetration testing to be performed (e.g., annually, quarterly)?

    Answer: Annually for GLBA requirement. Network is every other year. Systems that support critical functions once every three years (hosted systems).

27. Will ad-hoc testing be required for major system changes or incidents?

    Answer: In the past, IT has used our contract to have a consultant assess a system after an upgrade.

28. Can JMU provide a network diagram, including segmentation and firewall configurations, to help define testing boundaries?

    Answer: Yes, if necessary, these will be provided prior to an audit.

29. Are there any cloud-based services or hybrid infrastructure elements that need to be tested?

    Answer: We do not conduct testing on cloud systems. We rely on third-party reports.

30. Will test accounts with specific privileges (e.g., admin, standard user) be provided for application testing?

    Answer: Yes, the appropriate accounts will be provided to consultants to complete an audit.

31. Is testing expected to include credentialed scans or only external unauthenticated testing?

    Answer: This will depend on the scope of the audit, which will be determined during an entrance conference.

32. Are wireless networks within scope? If so, how many wireless networks exist, and are separate SSIDs used for guest and internal networks?

    Answer: A wireless network audit is a potential engagement. Actual numbers and SSIDs will be discussed during planning.

33. Are there compliance frameworks or regulatory requirements guiding the penetration testing (e.g., NIST 800-53, ISO 27001, FERPA, HIPAA)?

    Answer: This would be discussed in planning for each project. It could depend on the type of data being processed/stored in the target area.

34. Are there specific reporting formats or templates required to align with these standards?

    Answer: No. Report format is up to the consultant performing the audit as long as it covers the scope, methodology and findings/recommendations.

35. Are there restrictions on the tools, scripts, or software that can be used during testing?

    Answer: No, all automated scanning tools, scripts and software are allowed. Organizations are responsible for the appropriate use of any tool used during an audit.

36. Is social engineering (e.g., phishing or pretexting) included in the scope?

    Answer: Social engineering typically is not included in an audit.

37. Will JMU provide a “blue team” to coordinate defensive responses during testing?

Answer: The Information Security Officer is included in all phases of the audit and will handle defensive responses initially and will delegate to the necessary staff to address.

38. Does JMU expect formal red-team engagements or assume passive observation?

    Answer: Engagements are typically more red team.

39. What specific details are required in the final penetration testing report? (e.g., executive summary, findings by severity, recommendations, risk matrix)

    Answer: A final draft report covering the audit scope, approach and any findings should be provided at the end of an engagement. Any supporting documentations should be provided as well. Scan results, etc.

40. Should reports include mitigation strategies or just identified vulnerabilities?

    Answer: Recommendations on how to remediate the findings are typically included.

41. Does JMU have a preferred risk rating framework for findings (e.g., CVSS scores, custom classifications)?

    Answer: Consultants are free to use any framework.

42. Are proof-of-concept exploits required to demonstrate identified vulnerabilities?

    Answer: They should be included as supporting evidence for identified issues.

43. Is there a process for safe exploitation to minimize downtime or disruptions?

    Answer: Testing times are identified during the entrance conference. Typically, times that would have a low impact are chosen for engagements. Consultants should use caution when testing.

44. Will follow-up testing be required after remediation efforts?

    Answer: Some audits may require follow-up testing.

45. Should the proposal account for retesting as part of the deliverable or provide optional pricing for retesting?

    Answer: Yes, if it is determined during the entrance conference that follow-up testing will be part of the engagement. Otherwise, follow-up testing will be a separate engagement.

46. Is there a dedicated staging or test environment, or will testing occur in the production environment?

    Answer: This will be determined during an entrance conference. Some core systems do have a test environment.

47. What safeguards need to be followed when testing in production?

    Answer: Testing times are identified during the entrance conference. Typically, times that would have a low impact are chosen for engagements. Consultants should use caution when testing. Safeguards are typically discussed during planning.

48. Are there restricted testing windows to avoid disruptions to university operations?

Answer: Testing times are identified during the entrance conference. Typically, times that would have a low impact are chosen for engagements. Consultants should use caution when testing. Safeguards are typically discussed during planning.

49. What are JMU's preferred schedules for conducting tests (e.g., weekends, nights)?

    Answer: Testing times are identified during the entrance conference. Typically, times that would have a low impact are chosen for engagements. Consultants should use caution when testing. Safeguards are typically discussed during planning.

50. What is the process for notifying stakeholders and getting approvals prior to testing?

    Answer: Stakeholders are identified during planning. Most of the time consultants do not need a separate approval prior to testing. They are required to send an email to stakeholders notifying them that they are starting and another email at the end of testing. Consultant's IP address should be shared as well.

51. Are there specific points of contact required during the testing period?

    Answer: Stakeholders are identified during planning. Most of the time consultants do not need a separate approval prior to testing. They are required to send an email to stakeholders notifying them that they are starting and another email at the end of testing. Consultant's IP address should be shared as well.

52. Are there data privacy or legal restrictions that must be observed during testing (e.g.,FERPA, HIPAA)?

    Answer: The university must comply with many regulations, including, but not limited to, HIPAA, FERPA, and GLBA. Consultants are required to proceed cautiously with testing to ensure the security of university systems and data.

53. Will there be specific contract terms to limit liability for findings related to downtime or data exposure?

    Answer: AMS is not sure how a finding could create liability.

54. Are NDAs required for testers, and if so, will templates be provided?

    Answer: Yes, NDA's may be required. A template will be provided.

55. What is JMU's process for responding to vulnerabilities or breaches identified during testing?

    Answer: In most cases, university staff will contact the vendor of the system to determine a resolution.

56. Will testers be involved in drafting incident response plans or conducting tabletop exercises?

    Answer: This has not been done in the past.

57. Does JMU expect named resources (e.g., resumes, certifications) to be identified in the proposal?

    Answer: It would be helpful to identify all potential staff and their experience. This will help us to select the most qualified consultants to have on contract.

58. Is there a minimum certification level required (e.g., OSCP, CEH, GPEN)?

Answer: Consultants who have staff that possess more certifications will be looked at more favorably.

59. Should pricing account for fixed-price engagements, or does JMU prefer time and materials pricing for penetration testing?

    Answer: Consultants should provide an hourly rate for on-site (inclusive of travel) and an hourly rate for remote/off-site work.

60. Are there restrictions on billing categories, such as separate charges for travel and software licenses?

    Answer: Allowable expenses will be discussed during planning.

61. Does JMU require post-engagement workshops or training sessions for internal IT staff?

    Answer: If there are findings, all that is needed are recommendations and appropriate resolutions.

62. Should documentation include step-by-step remediation guidance for IT teams?

    Answer: Any information that will help resolve a finding should be included in a recommendation.

63. Is ongoing vulnerability scanning or maintenance required as part of the contract?

    Answer: The engagements will be a point-in-time assessment of systems.

64. Should pricing for managed services or recurring assessments be included?

    Answer: The engagements will be a point-in-time assessment of systems.

65. Will JMU provide access to any tools, software, or scanning platforms?

    Answer: This has not been done in the past. Consultants have been required to use their own tools.

66. Are there restrictions on third-party tools we can use?

    Answer: The university expects that consultants will use reputable tools during engagements. Any questions about tools can be discussed during planning.

67. How frequently are status reports or updates required?

    Answer: Not all engagements are the same and this will be discussed during planning.

68. Are there any formal review or sign-off processes for deliverables?

    Answer: AMS has an internal review and sign-off process for deliverables received during the engagement.

69. Does JMU prefer fixed-price or time-and-material pricing structures for specific projects?

Answer: Consultants should provide an hourly rate for on-site (including travel) and an hourly rate for remote/off-site work.

70. Should travel costs be itemized separately or included in flat rates?

    Answer: Included in flat rates.

71. What invoicing formats and documentation are required for payment processing?

    Answer: There is no requirement for a specific format. An invoice with the costs associated with completing the engagement should be submitted for payment.

72. Are there specific payment terms for milestone-based deliverables?

    Answer: Payment for engagements is handled when the final report is provided to AMS. There are no exceptions to this.

73. What are the requirements for on-site visits, including badging and access controls?

    Answer: This will be discussed during planning. Typically, consultants are provided with credentials for testing. They will be escorted through sensitive areas if required.

74. Are there specific blackout dates or periods where testing cannot occur due to academic schedules?

    Answer: Yes. Typically, testing will be conducted during times to minimize any impacts.

75. Would the University consider accepting certifications other than those listed in the definition of "Certified Professional" on p. 2 (for example, ITIL Foundation v3, Certified Associate Chief Information Security Officer (C | CISO)? Also, could you please clarify whether all team members must fit the definition of Certified Professional, or if it's sufficient that each engagement be led by consultants with the required certifications?

    Answer: Yes, alternate certifications could be acceptable. Not all team members would need certifications, as long as they are under supervision of a certified consultant.

76. Are there any GLBA or PCIS audit needs that should be included?

    Answer: GLBA required audit is a potential engagement.

77. Is there a preference for NIST 800 or ISO 27001 compliance frameworks?

    Answer: Currently, JMU IT is using ISO.

78. Does this count as a VASCUPP award or is this just for JMU?

    Answer: This contract will be made available to the VASCUPP schools for their use, should they choose to do so. This will be a cooperative contract that can be utilized by any public body, (to include government/state agencies, political subdivisions, etc.), cooperative purchasing organizations, public or private health or educational institutions or any University related foundation and affiliated corporations

79. When is the next anticipated need for audit work to start at JMU?

    Answer: The goal is to have the selected consultants on contract before the end of the current fiscal year. Most likely, the need will not be until next fiscal year (7/1/2025-6/30/2026).

80. The RFP states "Definition of Term – Certified Professional is defined as holding current Certified Information Systems Auditor (CISA), Certified Information Systems Security professional (CISSP), Certified Information Systems Manager (CISM), Microsoft Certified Professional (MCP), Cisco Certified Network Associate (CCNA), Information Systems Security Management Professional (ISSMP)." This Reads as if all of the listed certifications are required for each consultant. Is that correct or is it just that a consultant must have one of the listed certifications for their appropriate area to be deemed a certified professional?

    Answer: At least one of the certifications.

81. Can you explain the last two columns of the table in Attachment B, specifically:
    "Total Subcontractor Contract Amount"
    "Total Dollars Paid Subcontractor to date"

    Answer:

    Total Subcontractor Contract Amount – Dollar amount allocated to SWaM subcontractor in the direct performance of the contract/task.

    Total Dollars Paid Subcontractor to date – The total dollar amount paid by the contract to the subcontractor.

82. Do the columns refer to work previously performed where the Offeror has used the sub-contractor to perform work? Does either value represent an estimate of what work might be performed by a given contractor?

    Answer: No. They should represent an estimate of the what work might be specific to the contract.

83. Under section 5 Part B #6, the ask is to identify sales in the past 12 months to VASCUPP members. Many of these institutions have moved to the VHEPC contract. Can VHEPC data be used in the response?

    Answer: Yes

84. Could you kindly provide information regarding the current budget allocated for these services or details about the prices paid under previous contracts for similar services?

    Answer: Our current budget has been sufficient to do GLBA testing and two to five other projects each year. Each project is carefully planned and scoped with input from JMU's IT and the consultant.

85. Will the University be permitting penetration testing to be performed by existing or previous IT or Managed Service Providers? Or will the University be requiring third-party independence to reduce the risks of conflicts of interest or the optics of "grading one's work"?

    Answer: We are looking to have contracts with some consultants who will perform pen tests.

86. Is the University currently using any service providers that are assisting the University in performing the requested services? If so, who are these providers?

Answer: The current providers can be found here.

87. Is there an incumbent providing similar services to the University? If yes, is the incumbent performing to the satisfaction of the University, and the Chief Information Security Officer?

    Answer: See the answer to question 86 above.

88. Is the incumbent eligible to bid on this contract?

    Answer: Yes.

89. Can the University provide any information on the budget required to support these services? (E.g., budget details)

    Answer: AMS has a fixed budget for these services and cost will be a factor. No more details about the budget will be provided.

90. Does the University have onsite audit preference or vendor can perform remotely?

    Answer: Potential engagements include on-site. There is no preference.

91. Can the University provide a brief high-level description and accounting of their computing infrastructure? (e.g., hard-wired versus wireless, Windows and or Linux and or Mac, number of domains, number networks, number of IP addresses, etc.)

    Answer: If necessary, infrastructure will be discussed during planning for each engagement.

92. How many of the external IP addresses are live or currently in use?

    Answer: Will be discussed during planning for each engagement if necessary.

93. For wireless access points, how many SSIDs and how many locations are in scope?

    Answer: Will be discussed during planning for each engagement if necessary.

94. Are all campus/network locations accessible from the central location of the network?

    Answer: Will be discussed during planning for each engagement if necessary.

95. Is there a EDR solution is in place? If so, what vendor is it? Is it centrally managed?

    Answer: The university refrains from answering this question.

96. Is there a cybersecurity department? Is there an ISO or CISO on staff?

    Answer: The university has an ISO. University IT manages cybersecurity.

97. When was the last time an overarching IT security risk assessment was performed?

    Answer: JMU conducts various risk assessments to meet the needs of the University.

98. Does the University have documentation of the designated system owners and data owners?

    Answer: Yes

99. Is there a conclusive/documented inventory of all assets in scope that can be provided to selected Vendor?

Answer: Will be discussed during planning for each engagement.

100. Does the University currently utilize any internal network vulnerability assessment tools? If so, what is the scan frequency?

Answer: Yes. The university refrains from answering this question.

101. Does the University use baseline images for systems?

Answer: Yes

102. Is formalized change management in place?

Answer: Yes

103. How many voice VLANS and IP phones are in-scope?

Answer: Will be discussed during planning if necessary.

104. How many wireless locations are in-scope?

Answer: Will be discussed during planning if necessary.

105. Does the University want any cloud environments tested? If so, which vendor?

Answer: We do not conduct testing on cloud systems. We rely on third-party reports.

106. Does the University have any remote access services in use (on-demand VPN, GoTo my PC, LogMeIn, etc.) in-scope?

Answer: Will be discussed during planning if necessary.

107. Does the University have any in-bound modems (or remote access) in use?

Answer: Will be discussed during planning if necessary.

108. Is there any allowability to redline terms and conditions to negotiate later?

Answer: Will be discussed during planning if necessary.

109. The RFP is titled “Information Technology Security Auditing Services”, will all projects awarded be strictly security focused? For instance, the statement of needs mentions wireless network assessment/server configuration which can include many considerations aside from security.

Answer: Engagements will be focused on security to assess the controls protecting university systems and data.

110. How is the security team currently staffed/structured and how would you describe your current approach to security?

Answer: Information about the Information Technology Department can be found at https://www.jmu.edu/computing/about/index.shtml

111. Is there a routine and scheduled IT and Security audit services?

Answer: AMS works with IT annually to create the annual audit plan.

112. How often does JMU conduct IT and Security Audit assessments?

Answer: Up to five consultant engagements may be conducted during a fiscal year.

113. Who manages the IT and Security Audit service schedules for JMU?

Answer: Most are managed by the IT Audit Specialist in AMS.

114. Is each academic division responsible for managing its own IT asset?

Answer: Some academic units manage their own systems.

115. Is each academic division responsible for conducting routine and scheduled IT and Security Audit?

Answer: They are included in audits managed by AMS

116. Who is Audit and Management Services (AMS)? Is this an external entity, like a contractor hired by JMU to perform routine IT And Security Audit services? Or, is AMS a division within JMU?

Answer: AMS is JMU's internal audit department.

117. Who is responsible for managing JMU's IT Assets?

Answer: Central IT manages most IT assets.

118. Does JMU keep an inventory list of its IT Assets?

Answer: Yes

119. Who tracks JMU's IT Assets?

Answer: Central IT manages most IT assets.

120. Does each academic division track its own IT Assets?

Answer: Yes

121. Who performs routine and scheduled maintenance?

Answer: Central IT for most systems

122. Is this RFP to replace the existing/current staff of contractors performing under formal Statement of Work agreement?

Answer: The current contracts expire in April of 2025.

123. Is this RFP to provide supplemental support to JMU Personnel performing IT Audit functions listed in Section IV, Paragraph C (a-j)?

Answer: Yes, we outsource highly technical audits, such as pen tests and vulnerability assessments. JMU's IT Auditor oversees the outsourced projects.

124. Is this RFP to also provide supplemental support to current Staff of Contractors that are performing IT Audit functions under formal Statement of Work agreement?

Answer: This RFP is to support JMU's AMS department.

125. How many Staff of Contractors currently provide IT Audit Services to JMU-AMS under formal Statement of Work agreement?

Answer: We have four vendors on contract.

126. How many of these IT Audit functions are being performed by JMU Personnel?

Answer: The listed examples are performed by consultants.

127. How many of these IT Audit functions are being performed by the Staff of Contractors that are performing under formal Statement of Work agreement?

Answer: The listed examples are performed by consultants.

128. How many web applications are being assessed?

Answer: This will be determined during planning.

129. What framework and platform are being used for the web application(s)?

Answer: This will be discussed during planning.

130. How many static pages are being assessed? (approximate)

Answer: This will be discussed during planning.

131. How many dynamic pages are being assessed? (approximate)

Answer: This will be discussed during planning.

132. Will the source code be made readily available?

Answer: No

133. Do you want role-based testing performed against this application?

Answer: This will be discussed during planning.

134. Do you want credentialed scans/assessments of the web applications performed?

Answer: This will be discussed during planning.

135. How many total IP addresses are being tested?

Answer: This will be discussed during planning.

136. How many internal IP addresses, if applicable?

Answer: This will be discussed during planning.

137. How many external IP addresses, if applicable?

Answer: This will be discussed during planning.

138. Are there any security devices in place that may impact the results of a penetration test such as a firewall, intrusion detection/prevention system, web application firewall, or load balancer?

Answer: This will be discussed during planning.

139. Would the University prefer SWaM agencies?

Answer: JMU strives to work with SWaM vendor whenever practicable.

140. Is subcontracting mandatory for SWaM-certified agencies?

Answer: No

141. Would the university award 10 points as per the evaluation criteria to a Prime -SWaM certified agency if the Prime vendor does not subcontract for this opportunity?

Answer: Yes, as long as they are SWaM certified with the VSBSD.

142. How many individual projects or separate Statement of Works were issued under this award in the previous five-year contract period?

Answer: We typically have 3-5 engagements per fiscal year.

143. Can you please provide the total dollar value of work awarded under this award during the previous five-year contract period?

Answer: This information is not readily available.

144. Who is the individual the proposal will be addressed to?

Answer: Instructions are on page 17 of the RFP.

145. The RFP states that a certified professional is defined as someone holding a current CISA, CISSP, CISM, MCP, CCNA, or ISSMP certification. Would JMU consider adding the CompTIA Advanced Security Practitioner (CASP+) to the list? This certification requires 10 years' of hands-on IT experience and at least 5 years of hands-on IT security experience. The certification demonstrates advanced competency in areas such as risk management, enterprise security, and governance.

Answer: This list is not comprehensive. All reputable certifications should be mentioned.

146. Who is responsible for determining the on-site versus off-site requirements?

Answer: This will be discussed during planning.

147. What is the anticipated level of on-site engagement, if any? And how many locations will require an on-site visit?

Answer: This will be discussed during planning.

148. Are there specific workshare requirements under the Small Business Subcontracting Plan?

Answer: There are no requirements to utilize SWaM vendors. However, JMU strives to work with SWaM vendors whenever practicable.

149. Is strict adherence to ISO 27002 security framework requirements mandatory, or are alternative frameworks, such as NIST, acceptable?

Answer: ISO 27002 is preferred. However, any reputable framework could be used.

150. Is it required to provide resumes for all proposed personnel at the time of submission?

Answer: It will help us adequately assess potential consultants if they provide information for all potential staff.

151. Can you confirm the number of wireless networks to be assessed and their respective locations?

Answer: This will be discussed during planning.

152. Could you provide the total number of web applications that require testing?

Answer: This will be discussed during planning.

153. Are there any specific requirements or needs for cloud security assessments in this engagement?

Answer: No. We do not conduct testing on cloud systems.

154. Is the request for a point in time scan of the Universities attack surface or an ongoing service to monitor for external vulnerabilities in real-time?

Answer: The engagements will be a point-in-time assessment of systems.

155. Is there an expectation that active or passive wireless survey would be conducted? If so the locations and floor plans of locations to be surveyed would be needed for an accurate SOW.

Answer: This will be discussed during planning.

156. What are the vendors, models, operating system versions and quantities of firewall and routers in the environment?

Answer: This will be discussed during planning.

157. What server operating system version and number of servers in the environment? Are these servers physical or virtual?

Answer: This will be discussed during planning.

158. What hypervisors are being used in the environment?

Answer: This will be discussed during planning.

159. What IaaS and SaaS platforms are being used in the environment?

Answer: This will be discussed during planning.

160. How many databases are in the environment?

Answer: This will be discussed during planning.

161. What platforms are these databases hosted on?

Answer: This will be discussed during planning.

162. What applications use these databases?

Answer: This will be discussed during planning.

163. Is the intent of this assessment to review the network vulnerability management process?

Answer: This will be discussed during planning.

164. How many web applications are in scope?

Answer: This will be discussed during planning.

165. Where are these web applications hosted?

Answer: This will be discussed during planning.

166. What platforms do these applications run on?

Answer: This will be discussed during planning.

167. What version of Windows are the domain controller running?

Answer: This will be discussed during planning.

168. Is there integration with Entra ID or other identity providers?

Answer: This will be discussed during planning.

169. If the state has already arrived at best market value rates for these services and an contract is in place to reference, why is an RFP being issued?)

Answer: JMU's current contracts for these services will expire in April 2025, and this RFP is being issued to replace them.

170. Is the support requested in the proposal hands-on, or purely advisor in performing an audit of functions conducted by JMU?

Answer: Our goal is to have multiple contractors on contract to provide audit services to assess technical controls. The engagements could be considered hands-on.

171. In order to perform work in this RFP, are contractors required to possess all or some of the certifications listed in Paragraph C? May some of these certifications be alternated pending we have more technical certifications that meet the same requirement?

Answer: It is not required for the staff to possess all the certifications.

172. (C.1.a) Pertaining to conducting External Vulnerability Scanning, are there any third-party assets or assets explicitly excluded from this scope?

Answer: This will be discussed during planning.

173. (C.1.b) Pertaining to conducting Wireless Network Assessments: A) How many networks are in scope? B) How many wi-fi access points are in scope? C) Do we have an up-to-date inventory of all wireless access points (APs) and their locations? D) What is the architecture of the wireless network (e.g., standalone, controller-based, cloud-managed)? E) Are there any mesh networks, IoT devices, or specialized APs in use? F) Are there any known issues with signal interference or channel congestion?

Answer: This will be discussed during planning.

174. (C.1.c) Pertaining to conducting Firewall and Router Security Assessments: A) Does JMU use one specific vendor (ie., Cisco, Juniper, Palo Alto) or a combination of vendors for its solution? If so, which vendors are leveraged within its Firewall and Router solution? B) Are any virtual firewalls or cloud-managed routers part of the assessment? C) Are logs enabled for both firewalls and routers? D) Do you allow telemetry to be exported to external entities (such as our SOC)? E) Are logs integrated with a SIEM (Security Information and Event Management) system for analysis?

Answer: This will be discussed during planning.

175. (C.1.d) Pertaining to conducting Server Configuration Assessments: A) Is there an updated inventory of all servers, including their roles and locations? B) Are server configurations documented and maintained in a central repository? C) Is access to remote management interfaces restricted to specific IPs or networks?

Answer: This will be discussed during planning.

176. (C.1.e) Pertaining to conducting Database Architecture Security Assessments: A) Are both production and non-production environments included in the assessment? B) Is there an updated inventory of all databases, including versions and roles? C) Are database architecture diagrams and data flow diagrams documented and up to date? D) Are logs entralized/monitored (e.g., through a SIEM system)? E) Is there a process for evaluating/applying updates without disrupting operations?

Answer: This will be discussed during planning.

177. (C.1.f) Pertaining to conducting Network Scanning Process Assessments: A) Are the tools configured for active, passive, or hybrid scanning? B) How does the organization discover and inventory all connected devices? C) Are unauthorized or rogue devices detected and flagged during scans? D) What size subnet/subnet range does JMU administer/lease? E) What is an estimate of the number of endpoints to be expected on the network? 500 – 1000, 1000 – 2,500, 2-500 – 5,000, or 5,000+? F) Do you allow telemetry to be exported to external entities (such as our SOC)?

Answer: This will be discussed during planning.

178. (C.1.h) Pertaining to conducting Active Directory Security Assessments: A) How many domains and domain controllers (DCs) are in the environment? B) Are all domain controllers running supported OS versions and fully patched? C) Are logs centralized (e.g., SIEM) and monitored for suspicious activities?

Answer: This will be discussed during planning.

179. (C.1.i) Pertaining to conducting Penetration Testing: A) Are there specific exclusions (e.g., certain servers, critical infrastructure)? B) Is the testing internal, external, or both (e.g., testing from within the network or from an external perspective)? C) Are cloud environments, third-party services, or IoT devices included? D) Is testing white-box (full access), black-box (no prior knowledge), or gray-box (partial knowledge)?

Answer: This will be discussed during planning.

180. (C.1.j) Pertaining to assessing Telecommunications: A) Which telecommunication services are included (e.g., voice, VoIP, wireless, data)? B) Are third-party managed services or service providers within scope? C) Are specific geographical locations or facilities included? D) Are third-party carriers and vendors assessed for security and compliance risks? E) Are contracts regularly reviewed for adherence to terms and emerging security needs? F) Are logs collected, centralized, and analyzed for security events?

Answer: This will be discussed during planning.

181. Please briefly describe what you mean by "Network Scanning Process Assessment" and “Telecommunications”.

Answer: Telecom would focus on the security of the VOIP implementation. The network scanning process assessment has never been included in our audit plan because we feel that we are covered by the internal and external pen tests.

182. Please describe what "other products and services" you typically see in your audits, or what you mean by this phrase.

Answer: We have not had any billing for services other than travel and lodging.

183. What is the typical lead time that you provide to your vendors for your audits?

Answer: During our meeting with IT at the beginning of the fiscal year, we identify the audits to be included for the year as well as identifying the potential consultants. AMS will reach out to those consultants to determine availability and request proposals.

184. Will the universities in each of the listed zones be utilizing services from selected vendors, or just JMU?

Answer: This RFP is being issued for JMU’s needs and will be made available to other VASCUPP schools, should they choose to utilize it. Pricing should be provided so that any VASCUPP school could potentially use it.++

185. How much did JMU spend across all task orders on the previous contract vehicle?

Answer: This information is not readily available.

186. How many task orders were issued on the previous contract vehicle?

Answer: This information is not readily available.

187. What was the work breakdown structure between the 4 incumbents on the previous contract vehicle? Can we see the number of task orders awarded to each contractor?

Answer: This information is not readily available.

188. What is the spending ceiling on the contract vehicle?

Answer: Our current budget is sufficient to support GLBA pen testing, plus 2-5 additional projects per year.

189. Are we required to provide auditing services for all 10 categories, or is it OK to support only a subset?

Answer: No. AMS will contact contractors to submit a proposal for one of the audits when it is on the schedule. It is fine to support a subset of the services.

190. Is certification required for all bidder participants? Can education, training and experience replace certifications?

Answer: Consultants who have staff that possess more certifications will be looked at more favorably.

191. What brand of firewall equipment are you using?

Answer: This will be discussed during planning.

192. What brand of router equipment are you using?

Answer: This will be discussed during planning.

193. Does your Active Directory (AD) consist of on-premise, Azure AD, or some combination?

Answer: This will be discussed during planning.

194. What types of services does Telecommunications entail?

Answer: This will be discussed during planning.

195. With regards to Telecommunications, what sort of audit or IT activity should be expected? Would this be geared as an audit of process and controls, or a technical assessment for vulnerabilities and penetration testing (i.e. war dialing).

Answer: Telecom would focus on the security of the VOIP implementation.

196. C.1.a - C.1.i- What tools and technologies are currently in place for external vulnerability scanning, network assessments, and penetration testing? Are consultants expected to use university-provided tools or supply their own?

Answer: We expect consultants to use their own tools.

197. Page 3, Paragraph #6: Does JMU provide access to system architecture diagrams, configurations, or previous audit reports to inform the current project scope?

Answer: These will be shared during the planning of an engagement.

198. Page 3, Paragraph A: Since JMU follows ISO 27002, how mature is the current implementation of these controls across IT systems? Are there specific areas of non-compliance that require attention?

Answer: The university refrains from answering this question.

199. C.1.a - C.1.i What level of access will consultants be granted during audits (e.g., administrative privileges, network access)?

Answer: Consultants will be given necessary access to system to complete testing.

200. For on-site engagements, what are the physical security requirements and protocols for accessing sensitive areas of the network or facilities?

Answer: This will be determined during planning of an engagement. Consultants, at a minimum, will be escorted to sensitive areas.

201. What level of collaboration is expected between the consultant and JMU's internal IT teams during the project?

Answer: The IT Auditor in AMS manages the audits and will assist consultants during the audit. Arranging the entrance conference for each audit and ensuring consultants have what they need to complete the audit (credentials, etc.).

202. In the event that significant risks or vulnerabilities are identified, how quickly can the IT team allocate resources to address them, and what role will the consultants play in the remediation process?

Answer: IT has the resources to address issues identified during an audit. Consultants should notify IT and AMS as soon as possible of significant risks or vulnerabilities as well as providing a recommendation to address the issue(s).

203. How does JMU's IT team currently track and manage vulnerabilities or remediation tasks? Should the consultants integrate with existing ticketing or reporting systems? No

Answer: Will be discussed during planning for each engagement.

204. Is there a preferred ratio of remote to on-site work for projects, or is this determined on a case-by-case basis?

Answer: This is determined during planning.

205. How frequently will status updates or check-in meetings be required during active audit engagements?

Answer: This is determined during planning.

206. For larger projects, is there a preferred team size, or is it acceptable for a single highly qualified professional to perform the audit?

Answer: These audits can be completed by one person.

207. What is the expected format for audit reports and findings? Does JMU have a preferred reporting template?

Answer: The consultant can utilize their own format. We would like to see the scope, audit approach (methodology), findings and recommendations.

208. Is there an established process for presenting audit findings to executive leadership or stakeholders at JMU?

Answer: Audit reports are presented to the Board of Visitors (Audit, Risk and Compliance Committee)

209. Beyond final reports, are interim reports or preliminary findings required during the audit process?

Answer: No, unless determined otherwise during planning.

210. What is the typical turnaround time for report reviews and feedback after submission?

Answer: Could take up to two weeks for AMS to review reports. Typically, one week.

211. How does JMU prioritize remediation actions following audit findings, and is the consultant involved in verifying that corrective measures are implemented?

Answer: Critical issues are directed to IT immediately after discovery. For these issues, the consultant should work with IT to help address the issue.

212. Specify the VLAN detail; how many are included in the scope?

Answer: This will be determined during planning.

213. Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)?

Answer: The university refrains from answering this question.

214. How much (%) of the infrastructure is in the cloud?

Answer: In-scope infrastructure location will be discussed during planning.

215. In the IT department/environment, how many employees work?

Answer: Information about the Information Technology Department can be found at https://www.jmu.edu/computing/about/index.shtml

216. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

Answer: JMU has multiple server rooms and utilizes some cloud solutions.

Signify receipt of this addendum by initialing *"Addendum #2"* on the signature page of your proposal.

Sincerely,

Doug Chester
Buyer Senior
Phone: 540-568-4272