JAMES MADISON UNIVERSITY

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No. **UCPJMU7142**

This contract entered into this 25th day of March 2025, by Baker Tilly Advisory Group, LP., 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:

By _____
(Signature)

Chris Kalafatis, Mike Cullen
(Printed Name)

Title: Managing Director, Principal

PURCHASING AGENCY:

By: _____
(Signature)

Doug Chester
(Printed Name)

Title: Buyer Senior

JAMES MADISON UNIVERSITY.

RFP # FDC-1220
Information Technology Security Auditing Services
Negotiation Summary for Baker Tilly Advisory Group, LP
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	$230.00	$253.00
Wireless Network Assessment	$230.00	$253.00
Firewall and Router Security Assessment	$230.00	$253.00
Server Configurations Assessment	$230.00	$253.00
Database Architecture Security Assessment	$230.00	$253.00
Network Scanning Process Assessment	$230.00	$253.00
Web Application Security Assessment	$230.00	$253.00
Active Directory Security Assessment	$230.00	$253.00
Penetration Testing	$230.00	$253.00
Telecommunications	$230.00	$253.00
**** (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. Upon completion of each Statement of Work, the Contractor shall submit a SWaM subcontractor usage report in accordance with RFP Special Term and Condition J: Small Business Subcontracting and Evidence of Compliance. Reports shall be submitted to: JMU Office of Procurement Services, Attn: SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807 or swamreporting@jmu.edu.

7. 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.

January 30, 2025

James Madison University

True transformation reaches far beyond everyday success. Explore IT audit solutions that move you forward.

Response to RFP # FDC - 1220

Baker Tilly Advisory Group, LP
8270 Greensboro Dr, Suite 400
McLean, VA 22102
bakertilly.com

January 30, 2025

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

Dear Doug:

James Madison University (JMU) seeks a trusted firm to provide a range of IT audit and advisory services in accordance with professional audit standards and frameworks. Baker Tilly is that firm. This proposal is the starting point — our vision of how we can protect and enhance your enterprise value as we achieve your immediate goal to work with experienced practitioners who can support JMU's technical resilience.

KEY SUCCESS FACTORS	BAKER TILLY
Qualified and certified IT audit, security, and risk professionals covering all technical subject areas and experienced with ISO 27002	✓
Unmatched higher education experience, including active Internal Audit work with many peer Commonwealth institutions	✓
Collaboration with SWaM businesses in the Commonwealth	✓

We're prepared to help you navigate complex landscapes, ensure regulatory compliance using industry-leading practices and build trust within the communities you serve. This means creating a robust framework for managing IT risks and safeguarding organizational assets. The approach and qualifications we've shared in our proposal show how important JMU will be as a client.

Sincerely,

Chris Kalafatis, CPA, CIA, CFE,
Managing Director
+1 (703) 923 8007 **|** Chris.Kalafatis@bakertilly.com

Mike Cullen, CISA, CISSP, CIPP/US
Principal
+1 (703) 923 8339 | mike.cullen@bakertilly.com

Contents

“ We really appreciate your support through our journey and ALL that we were able to learn with you coaching and guiding us.

Vice president | Baker Tilly client

bakertilly

1. Cover sheet

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:

Baker Tilly Advisory Group LC

8270 Greensboro Drive, Suite 400

McLean, VA 22102

By: MC *(Signature)*

Name: Mike Cullen, CISA, CISSP, CIPP/US *(Please Print)*

Date: 1/50/2025

Title: Principal - Risk Management

Web Address: www.bakertilly.com

Phone: +1 (703) 923 5339

Email: mike.cullen@bakertilly.com

Fax #: +1 (414) 777 5555

ACKNOWLEDGE RECEIPT OF ADDENDUM: #1 MC #2 MC #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. Plan and methodology

We blend technology with experience to deliver quality insights for JMU.

Our plan to address the services in scope

JMU is a one-of-a-kind institution with unique risks and opportunities. We build our service plans accordingly. Tailoring our information technology audit and advisory services service methodologies to your specific needs. Your goals, culture and the distinctive factors that impact you will play a role in shaping our approach. Along the way, our deep understanding of higher education and knowledge of JMU's unique needs will fuel our dedication to helping you achieve your goals.

Our team has the experience of conducting audits of the key areas you identified, and more.

AUDIT AREAS	BAKER TILLY EXPERIENCE
External Vulnerability Scanning	✓
Wireless Network Assessment	✓
Firewall and Router Security Assessment	✓
Server Configurations Assessment	✓
Database Architecture Security Assessment	✓
Network Scanning Process Assessment	✓
Web Application Security Assessments	✓
Active Directory Security Assessment	✓
Penetration Testing	✓
Telecommunications	✓
Cloud (SaaS, PaaS, IaaS)	✓
Internet of Things (IoT)	✓
Cybersecurity Frameworks (e.g., ISO, NIST, CIS)	✓

Below, we outline our high-level, illustrative approach to performing various assessments. Our methodology is aligned with industry standards and leading practices to ensure accuracy and consistency. Throughout the process, Baker Tilly will proactively communicate with you.

STEP 1: PLANNING

Purpose: Establish understanding of scope, approach, timing and deliverables.

Tasks

- Kick off the project
- Identify key stakeholders for the project and determine the anticipated level of effort
- Evaluate the systems to be included in scope and functions
- Develop a project plan and calendar

Deliverables

- Kick-off materials
- Preliminary documentation request list
- Control walk-through meeting agendas

STEP 2: EVALUATING

Purpose: Evaluate the current practices to determine gaps and recommendations.

Tasks

- Conduct walk-throughs and interviews with key process owners to identify capabilities, processes, and currently implemented technologies and controls
- Map current state practices to the applicable framework(s)
- Test control practices using a variety of techniques, including inquiry, review, reperformance both manually and with technical tools
- Validate initial results with stakeholders

Deliverables

- Initial observations related to control design and implementation
- An inventory of implemented security capabilities and technologies

STEP 3: REPORTING

Purpose: Develop and provide a comprehensive summary of findings and recommendations.

Tasks

- Consolidate our observations, identified areas for improvement, and recommendations into report.
- Review the report with stakeholders and make updates based on feedback provided.

Deliverables

- Report with executive summary, detailed observations/analysis, and recommendations.

Our approach to project management

Project success depends on the effective coordination of many interdependent activities. To ensure success, we manage our projects in accordance with the widely accepted principles from the Project Management Institute (PMI) and its Project Management Body of Knowledge (PMBOK). Our project management methodology also incorporates lessons learned from decades of experience in delivering services on time and on budget for our clients.

Additionally, all Baker Tilly deliverables undergo a rigorous quality review process within the firm to help ensure that both internal and client quality standards are achieved.

> *"Post- Baker Tilly, we are making great headway on security policies and procedures, and it's measurable. Our exposed surface area for cyber-attack is smaller than it's ever been. Every employee signed off on Acceptable Use, and HR verified that. Best of all, my job is less stressful …."*
>
> - *Director of Information Systems*

Maintaining open lines of communication allows us to be responsive to your needs while understanding and addressing any potential impacts to this effort. The table below illustrates some of the tools and techniques Baker Tilly has used to facilitate consistent communication and accountability throughout our engagements. Baker Tilly will work with your identified point of contact to define project management and communication requirements, tailor these tools to your organization, and to define protocols for communicating exceptional events.

TOOL/TECHNIQUE	ONGOING	ONE TIME
Project planning meeting with management/leadership		✓
Project kickoff meeting		✓
Project plan and calendar		✓
Status reports	✓	
Issues log	✓	
Information request logs	✓	
Observations validation review meeting after testing		✓
Final observations presentation / project closing		✓
Other key reporting as defined during planning	TBD	

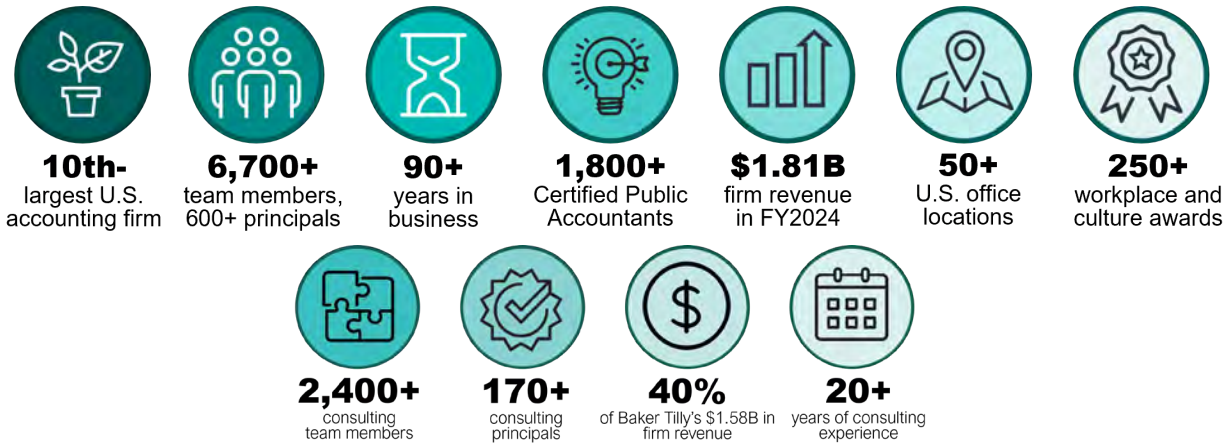
Our partners, directors, managers and staff members are available via email or telephone to JMU whenever the need arises, and **we will respond promptly** to your inquiries and concerns. JMU **can rely on us** to raise probing questions and offer ideas to spark conversation rather than imposing judgment and conclusions.

The combination of our experience and best practices has consistently enabled our teams to deliver projects for clients on schedule. Your engagement team will work remotely, in collaboration with your personnel, as needed and or requested by JMU.

3. Expertise, qualifications and experience

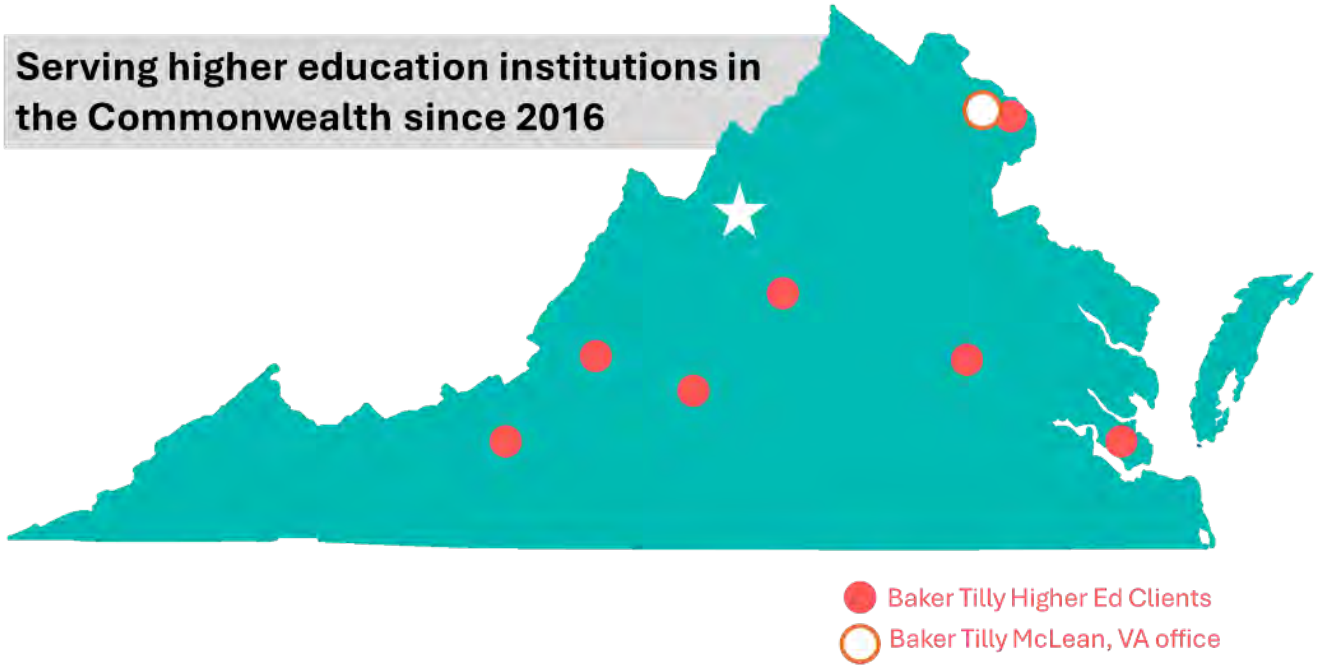
Our decades of serving higher ed is how we'll achieve success for JMU.

About Baker Tilly



Serving Virginia higher education

Our extensive service to higher education in Virgina, combined with our national network of over 50 offices, positions us to provide exceptional service and support to JMU.



Dedicated project team

Meet the team we've assembled to achieve your goals. Backed by our specialized resources, these individuals are collaborative and multidisciplinary. You'll find their bios below and complete resumes in **Appendix A**.

THE TEAM TO ACHIEVE JMU'S GOALS	
	**Mike Cullen, CISA, CISSP, CIPP/US — Principal** ***Engagement role: Overall client engagement leader*** Mike offers over 20 years of experience helping institutions tackle cybersecurity, data and information technology risks. With a dedicated focus and extensive experience in higher education, he has supported research institutions, not-for-profit organizations and a wide range of colleges, universities and state higher education systems in developing robust, secure and agile technology effectively to achieve institutional goals.
	**Chris Kalafatis, CPA, CIA, CFE — Managing Director** ***Engagement role: Public sector leader*** Chris has 25+ years of audit and consulting experience and leads Baker Tilly's public sector industry within the Risk Advisory practice. Chris and his team's primary service offerings include internal audit, IT audit, and other process improvement or IT consulting projects. Chris has served 30+ Virginia state agencies or public universities
	**Brian Nichols, CISSP, CIPP/US — Principal** ***Engagement role: Cybersecurity strategy leader*** Brian has over 15 years of experience developing cybersecurity strategies and evolving cybersecurity programs for clients across public sector, retail, consumer, airline, and railroad industries. He leads teams in conducting cybersecurity capability assessments using various industry frameworks such as NIST CSF, ISO 27001/2, CIS CSC, etc.
	**Peter Tsengas, CISA, CISM — Senior Manager** ***Engagement role: Public sector specialist*** Peter has 25+ years of IT audit and IT risk and compliance consulting experience with three top 10 firms, and industry experience in the public sector and Fortune 500. He is dedicated to helping public sector clients identify, prioritize and remediate technology and cybersecurity-related risks. Peter and has served 40+ Virginia state agencies or public universities
	**Joseph Schwendler, CISA, CRISC, CPA, CISM —Senior Manager** ***Engagement role: IT audit/cybersecurity senior manager*** Joe is an IT audit specialist who uses technical knowledge and critical thinking to introduce new approaches to control design and optimization that deliver better results for key stakeholders, uncover growth opportunities for our business and expand the capacity of diverse teams to deliver on deadlines and more overall value.

Mitchell Gorham, CISSP, CDPSE, CCSK— Senior Manager

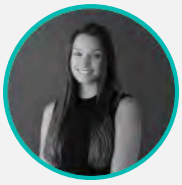
Engagement role: IT audit/cybersecurity senior manager

Mitchell focuses on risk mitigation, bringing over a decade of experience in cybersecurity. His expertise includes leading risk assessments, technology due diligence, penetration testing and vulnerability scanning. Renowned for his ability to combine technical expertise with business acumen, Mitchell effectively bridges IT and operations to achieve sustainable outcomes for his clients.

Morgan Mincey, CPA, CMMC - RP — Manager

Engagement role: IT audit/cybersecurity manager

Morgan brings experience in providing risk advisory and internal control solutions. Her clients have included higher education institutions and research institutions. She oversees audit activities and tasks to ensure timely and accurate results.



Amanda Guessford, CPA, Manager

Engagement role: IT audit/cybersecurity manager

Amanda has significant experience providing risk advisory and internal control solutions for clients that have included state systems, research institutions and both public and private colleges and universities. She conducts risk reviews, control assessments, testing activities and gap analyses to identify deficiencies in technology-related internal controls, and provides leading practices and recommendations to drive remediation.

Andrew Kennedy, CISA— Manager

Engagement role: IT audit/cybersecurity manager

Andrew will oversee audit activities and tasks to assist the team in delivering timely, valuable outcomes. He specializes in compliance-based and risk-driven assessments with a strong focus on cybersecurity and data privacy, collaborating with clients, delivering high-quality results and valuable insights, and providing long-term strategies that benefit the organization holistically as well as operationally.

Ivan Imbuido, CISSP— Senior Consultant

Engagement role: Penetration testing and vulnerability scanning

Ivan has more than 10 years of experience in digital forensics, security compliance and penetration testing. Additionally, Ivan has more than eight years of experience in system and network administration. He has also led cross-functional teams in defining, developing and delivering managed threat detection and response services.

Staff and subject matter experts

Engagement role:

Baker Tilly staffs a deep bench of practitioners with extensive, direct experience in each of the audit areas in scope. As needed, we will identify and assign appropriate resources to support specific engagement objectives.

Our dedicated and deep focus on higher education

A team of more than 70 Baker Tilly specialists devote most or all their time working with institutions like JMU. Enrollment levels of our clients range from fewer than **100 students to more than 215,000 students, with annual budgets ranging from less than $2 million to more than $18 billion.**

50+ years of higher education experience

We have spent more than 50 years of specializing in this industry and serving higher education institutions.

We advise clients in all categories from Ivy Plus schools to faith-based liberal arts colleges to community and technical colleges. We immerse ourselves in the challenges faced by our clients and provide targeted training and continuing education to our staff. This sector specialization ensures you will work with an engagement team possessing the necessary knowledge and skills. With nearly **400 clients in total across the higher education sector,** the Baker Tilly team understands the unique financial, operational and compliance challenges JMU faces and is familiar with risks across the whole spectrum of higher education operations.

A representative sample of higher education clients who engaged our risk and/or internal audit services appears below

OUR HIGHER EDUCATION CLIENTS

- Auburn University
- Ball State University
- Boston College
- Brandeis University
- Brown University
- California Institute of Technology
- Carnegie Mellon University
- Catholic University of America
- Columbia University
- Cornell University
- Dartmouth College
- Duke University
- Emory University
- Fordham University
- George Mason University
- George Washington University
- Georgetown University
- Harvard University
- Johns Hopkins University
- Lehigh University
- Louisiana State University
- Loyola University Chicago
- Marquette University
- Massachusetts Institute of Technology
- Minnesota State Colleges and Universities
- New Jersey Institute of Technology
- New York University
- Northeastern University
- Northwestern University
- Oklahoma State University
- Oregon State University
- Pennsylvania's State System of Higher Education
- Pennsylvania State University
- Pepperdine University
- Portland State University
- Princeton University
- Rice University
- St. John's University
- Stanford University
- Teachers College of Columbia University
- Temple University
- Texas Tech University
- Tufts University
- Tulane University
- University of California System
- University of Delaware
- University of Florida
- University of Kansas
- University of Massachusetts
- University of Michigan
- University of Minnesota
- University of Oregon
- University of Pennsylvania
- University of Pittsburgh
- University of Richmond
- University of Southern California
- University of Texas System
- University of Toledo
- University of Vermont
- University of Virginia
- University of Washington
- University of Wisconsin System
- Virginia Polytechnic Institute and State University
- Yale University

The following table illustrates audit areas Baker Tilly has assessed for higher education institutions over the last five years.

FUNCTIONS	SPECIALITY AREAS	COMPLIANCE	IT FUNCTIONS	SYSTEMS
• AP & AR • Conflicts of interest • Financial aid • Hotline • Human resources • Payroll • Procurement and procurement cards • Shared services • Travel and expense • Vendor management	• Admissions • Accreditation • Advancement • Athletics • Construction and facilities • Enterprise Risk Management • Fraud risk • International operations • Records management • Sponsored research • Student wellness	• ADA • Clery Act • CMMC • FAR • FERPA • GLBA • HIPAA • NCAA • NSPM-33 • OMB Uniform Guidance • OSHA • PCI DSS • Title IX	• Asset management • Change management • Cybersecurity program • Data classification • Identify & access management • Incident response • IT governance • IT/cloud vendor management • Internet of Things (IoT) • Network security • System implementations • Vulnerability & patch management	• Amazon Web Services • Banner • Blackboard • Canvas • Cayuse • Colleague • Google Workspace & cloud • Microsoft 365 & Azure • Oracle ERP & cloud • Peoplesoft ERP & Campus Solutions • Slate • Workday

Complimentary resources and thought leadership

Ongoing communication throughout the year is the hallmark of our client service approach. This allows us to discuss issues affecting JMU as they arise and keep you informed on an array of sector topics. Your engagement team will be in contact throughout the year and establish periodic meetings as an opportunity to discuss any challenges at no additional charge to you.

Our active higher education sector involvement and specialization translates into knowledge we will proactively share with JMU. We will regularly invest time in our relationship to inform you about emerging sector issues and new accounting standards.

Complimentary educational opportunities include:

- **Regular webinars** on topics such as accounting standards updates, Uniform Guidance, tax compliance, fraud, understanding financial reports, grant-related topics and cost reduction and revenue maximization. These webinars are free to our clients and qualify for continuing professional education (CPE). Prior webinars are archived on our website and can be viewed at any time.
- **Board educational training** to meet the need for continuous board educational training to assist board members in complying with their fiduciary responsibilities. We will offer a two-hour annual training session, as desired, based on a variety of possible topics to be selected by JMU.
- **Audit committee presentation** during the annual meeting with the audit committee. Baker Tilly will deliver a comprehensive PowerPoint presentation, which will include pertinent information such as financial ratios, benchmarking data and sector trends and updates, among other information.
- **Annual board of directors' presentation** where, upon request, Baker Tilly will provide JMU's board with materials that include pertinent information such as financial ratios, benchmarking data, sector trends and updates.
- **Higher Education Advisor, our quarterly newsletter** with guidance on sector, regulatory and resource optimization issues by our professionals who also contribute articles to other sector publications.
- **Higher Ed Advisor, our podcast series** dedicated to providing insightful guidance and leading practices for college, university and research institution leaders and board members.
- **Tax Strategist, our bi-monthly tax publication** offering in-depth technical information and our own best practice insight on tax issues.
- **Periodic alerts** on laws, regulations or decisions with an immediate or near-future impact on higher education institutions.

Higher education sector involvement to keep JMU informed

One of the greatest value-adds we can offer JMU is insights gained from more than 50 years of substantial involvement in the higher education sector. Active engagement in our clients' sector is important to keep both our team and our clients up to date on the issues and trends facing higher education institutions.

Contributing to events and initiatives by key sector organizations

We regularly present at conferences, including the Association of Governing Boards of Universities and Colleges (AGB), the Association of Independent Colleges and Universities of Pennsylvania (AICUP), National Council of University Research Administrators (NCURA), National Association of College and University Business Officers (NACUBO) and Society for Corporate Compliance and Ethics (SCCE).

INVOLVEMENT IN HIGHER EDUCATION SECTOR ASSOCIATIONS

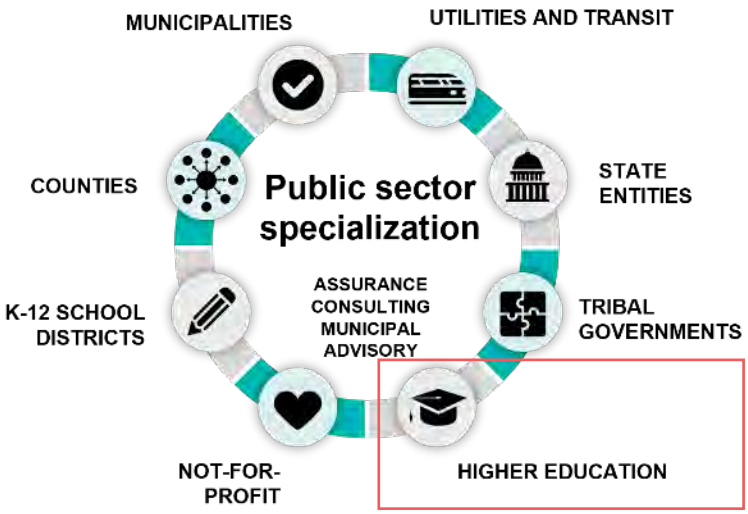
JMU can rely on Baker Tilly to keep you apprised of sector trends and developments affecting your institution. Our professionals work with leading sector associations and author thought leadership on important operational, fiscal and regulatory issues impacting the higher education sector.

ACUA Association of College & University Auditors
SCCE Society of Corporate Compliance and Ethics
NACUBO
AUECO Association of University Export Control Officers
NCURA Supporting Research...together™
EDUCAUSE
AGB Association of Governing Boards of Universities and Colleges

Our work in the public sector

Baker Tilly has served state and local governments since our establishment more than 90 years ago. We are one of the few advisory, tax and assurance firms with a practice dedicated entirely to serving governmental clients.

Unlike many other firms, Baker Tilly is organized by industry, not service line. What does this mean for JMU? It means you will be served by a carefully selected team that blends our government-focused professionals with experienced specialists in the activities of your agency. JMU will work with a knowledgeable team that understands your specific challenges and provides innovative solutions to help you overcome them.



State and local government is a complex, unique environment shaped by fiscal, regulatory and operational considerations not found in other industries. Recognizing this complexity and eager to serve as a true valued advisor to the public sector, Baker Tilly formalized its dedicated public sector specialization more than 50 years ago. **Today, more than 350 Baker Tilly professionals — including**

nearly 30 principals — focus directly on serving governments and provide hundreds of thousands of client service hours annually to agencies like JMU.

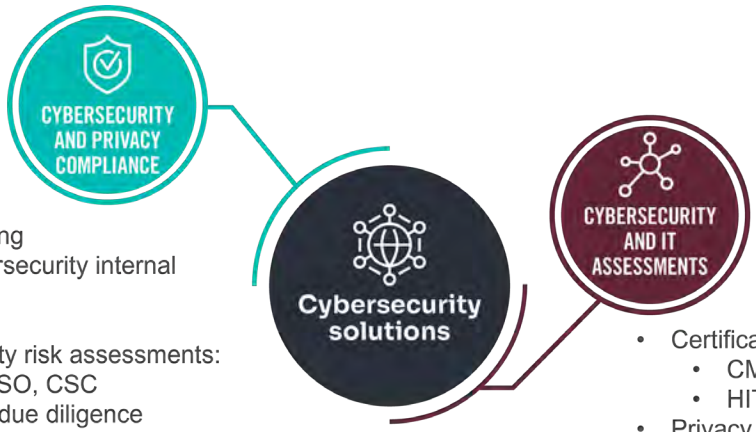
Nationwide, our public sector practice serves nearly **4,000 state and local governmental entities**, including public universities, school districts, counties, municipalities, utilities, transit organizations, airports and special authorities. Several of these client groups are now served by dedicated specialists in distinct sub-practices.

JMU will benefit from our industry specialization in several specific ways:

- **Dedication to the public sector:** Your engagement team members live and breathe government and work exclusively with the public sector year-round. This translates into insights only experience can bring, as well as an understanding of the best ways to communicate and collaborate with public-sector entities.
- **Specialized training and continuing education:** JMU can be assured of an engagement team with the necessary skills and timely knowledge to effectively perform your engagement.
- **Industry involvement:** Members of our public sector practice are leaders in key industry organizations, including the AICPA and its Governmental Audit Quality Center (GAQC) as well as the International City/County Management Association (ICMA). Because of our work with these groups, we know about dynamic trends and consequential developments in state and local government — and are equipped with leading practices to help JMU best respond to them.
- **Knowledge sharing with JMU:** At Baker Tilly, serving governments goes beyond delivering services – we also supply our clients with crucial thought leadership in the form of webinars, workshops, articles and our regular newsletter, CommuniTIES.
- **Year-round consultation:** Throughout our relationship, we will be available for routine calls and technical questions, connecting you with recommendations and ideas to address the inevitable operational issues that arise. We can also alert you to new opportunities for us to collaborate and create value for JMU.

Experienced cybersecurity and IT audit/risk credentials

To avert threats and mitigate risks in the constantly changing cybersecurity landscape, JMU must manage known vulnerabilities and proactively identify new ones. JMU's leaders need an accurate and objective view of your organization's ability to protect information assets from theft, compromise and destruction. Engaging Baker Tilly can help you achieve these outcomes with a range of service offerings, including:



- SOC reporting
- IT and cybersecurity internal audits
- IT SOX
- Cybersecurity risk assessments: NIST CSF, ISO, CSC
- Technology due diligence
- Penetration testing and vulnerability assessment

- Certifications
  - CMMC
  - HITRUST
- Privacy compliance assessments
  - GDPR
  - CCPA
- Security compliance assessments
  - CMMC
  - HIPAA
  - NYSDFS
  - NIST 800-171
  - NIST 800-53

Professional credentials

These team members have done the work, earning a breadth of professional certifications that demonstrate their commitment to deep knowledge of the issues and trends that affect each client's business, including:

PROFESSIONAL CERTIFICATIONS	
• Certification in Risk Management Assurance (CRMA) • Certified Regulatory Compliance Manager (CRCM) • Certified Financial Services Auditor (CFSA) • Certified Information Systems Auditor (CISA) • Certified Information Systems Security Professional (CISSP) • Project Management Professional (PMP)	• Certified Public Accountant (CPA) • Certified Fraud Examiner (CFE) • Certified Internal Auditor (CIA) • Certified Compliance Professional (CCP) • Certified Information Security Manager (CISM) • Certified Information Privacy Professional (CIPP) • Certified Information Privacy Professional/United States (CIPP/US)

WHAT DO WE BRING TO THE TABLE?	
	**A cohesive team with cybersecurity and IT audit expertise:** JMU will have a team of highly specialized resources to assess and test your information security infrastructure, risks and controls. Baker Tilly's **more than 100** qualified cybersecurity and IT risk professionals have combined technical training with hands-on experience in completing cybersecurity, IT audit and consulting engagements for clients in diverse industries. Demonstrating their expertise, team members also hold a variety of certifications, as detailed above.
	**Complementary industry and technical experience:** In helping organizations like JMU identify vulnerabilities and inefficiencies and mitigate IT-related risks, we draw from a deep understanding of the transportation and extensive experience in working with similar companies to more effectively manage cybersecurity risks and reduce the likelihood and impact of an exposure.
	**An understanding of security risks in the context of your organization**: Effective cybersecurity management requires a holistic perspective on potential threats and associated risks across the entire company — beyond just the IT department. As experienced consultants and auditors, we understand how to address security risk within the context of business risk. We start by working with your personnel to gain a complete picture of their unique operations, cybersecurity control environment and applicable regulatory requirements. Then we provide practical guidance based on lessons learned and **leading cybersecurity frameworks** such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ISO 27000/27001 and many more.
	**Practical and cost-effective strategies to mitigate risk:** Our services focus on proactively identifying risk mitigation strategies that are pragmatic, actionable and cost-effective. We understand the importance of "right-sizing" our approach and recommendations to meet your unique staffing and budgetary constraints. Our integrated cybersecurity management approach helps clients safeguard information assets by reinforcing protection while ensuring critical business operations are not disrupted.

I really was zeroing in on someone that knew what they were doing. You need someone that speaks that lingo. And there are very few firms that have that experience.

– Chief audit and compliance officer, higher education institution

Demonstrating our ability via similar projects

By highlighting our expertise through comparable projects, Baker Tilly assures JMU that we will utilize this knowledge to understand your distinct culture and needs, delivering customized and adaptable IT audit and consulting services.

IT VULNERABILITY MANAGEMENT	
Our client's need	A large, private research university needed help to review the vulnerability management processes managed by IT.
Baker Tilly solution	Serving as the university's internal audit function, Baker Tilly reviewed vulnerability management processes and validated the approach to resolve vulnerabilities and mitigate the risk to university systems and data. We interviewed stakeholders and walked through processes to understand responsibilities for vulnerability identification, prioritization and resolution; the process for detection, validation and prioritization of vulnerabilities, how risks were assessed and how IT monitored vulnerability resolution. We reviewed the results of recent vulnerability scans to validate that vulnerabilities were resolved following the established practices. We analyzed metrics for measuring vulnerability management practices (e.g., percent of total systems monitored or scanned, mean time to remediate a vulnerability, etc.) and then recommended enhancements to better measure the successes of vulnerability management. Finally, we analyzed the intersection of vulnerability management and other key IT process areas, including asset management, change management and patch management.
Results achieved	The university and IT received the results of our analysis, including recommendations to improve controls around the vulnerability management process. Our work helped the university better understand the risks of potential exposure or loss of university data and the impact on system availability and ultimately supported improvements in the vulnerability remediation and monitoring processes.

NIST FRAMEWORK MATURITY ASSESSMENT	
Our client's need	A company wanted an assessment of its current information security processes, controls and infrastructure, specifically regarding its compliance with key regulations, standards and frameworks, including NIST.
Baker Tilly solution	Baker Tilly sought to gain an understanding of the company's current security posture. This entailed an in-depth document review, including 32 published policies, standards and procedures, as well as more than 40 interviews with key personnel.
Results achieved	Findings from the research phase were used to develop a roadmap, which included a defined set of projects to treat risk areas and improve security posture at the company. Baker Tilly's recommendations included a deeper integration of data protection into operations, improvements to the communication of cybersecurity risks and the creation of an incident response strategy. Recommendations were broken into a series of key tasks and a suggested timetable for executing these recommendations — based on the company's resources — were also offered.

Serving you with purpose and relying on your feedback

Our level of service to JMU impacts your success and the success of your students and staff, so you'll never get less than our best. You'll see our longstanding reputation for excellence has not developed by chance. It is an approach we've honed over nine decades — an approach that relies heavily on feedback from JMU.

Don't just take our word for it; explore our industry-leading client satisfaction scores.

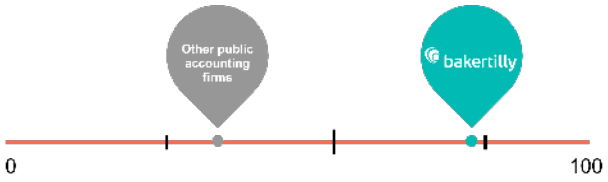
When done right, exceptional service earns exceptional recognition. The proof of our client service quality lies in our metrics.

Net Promoter Score (NPS) is a metric used to gauge customer loyalty by asking how likely customers are to recommend a company to others. An NPS of over 50 is considered "excellent."

Your feedback is not a nice to have — it's necessary

With your feedback, we can make "our good better and our better best."

In the accounting industry, the average benchmark is 41 according to a 2023 report by ClearlyRated. Baker Tilly consistently receives an NPS of greater than 65 and the Risk Advisory practice that will perform work scored 89. While that's unexpected in the advisory, tax and assurance world, it's what you can expect from us — an experience that goes beyond what other firms deliver.



Client Satisfaction Score (CSAT) is another well-known metric. We consistently score well above the industry average of 82 (published by Retently - retently.com/blog/customer-satisfaction-score-csat/).

"

They took the time to understand the business and processes of our organization from an overall perspective first.

– Chief financial officer

4. 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 93 Months _____

50+ years serving higher education
25+ years providing risk advisory services

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 #
University of Arkansas System	2019 - Present	2404 N. University Ave Little Rock, AK 72207	Laura Cheak, Chief Audit Exec +1 (501) 686 2908
University of Oregon	2015 - 2023	720 E. 13th Ave. Eugene, OR 97401	Katie Bumgardner, IS Auditor +1 (907) 450 8093
University of Tennessee	2023 - Present	Knoxville, TN 37996	Anthony Thompson, Asst. Audit Director +1 (865) 974 6613
VA Dept of Corrections	2024 - Present	6900 Atmore Dr. Richmond, VA 23225	Kyle Wakefield, Deputy IA Dir. +1(804) 887 8147
NYC Bd of Education Retirement System	2019 - 2024	65 Court St,16th Flr Brooklyn, NY 11201	Iyeekeze Ada Ezefili, Dir. IA +1 (929) 305 3861

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

JMU will have access to resources in more than 50 U.S. Baker Tilly office locations across 20 states and 13 international office locations. A list of offices can be found here: https://www.bakertilly.com/contact/offices

Local office: 8270 Greensboro Drive, Suite 400, McLean, Virginia 22102

Headquarters: 205 N. Michigan Ave, Suite 2800, Chicago, Illinois 60601

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 [X] NO

IF YES, EXPLAIN: _____

5. Small business contracting plan

ATTACHMENT B

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

Offeror Name: Baker Tilly Advisory Group, LP **Preparer Name:** Chris Kalafatis, CPA, CIA, CFE

Date: 1/30/2025

Is your firm a **Small 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 **Woman-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 **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____ No X

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: Information Technology Security Auditing Services RFP#FDC-1220 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:

Baker Tilly Advisory Group, LP (Firm) | 8270 Greensboro Drive, Suite 400, McLean, VA 22102 (Address) | Chris Kalafatis, CPA, CIA, CFE - +1 (804) 307 2610 (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)
Ignitec, Inc. 22365 Broderick Dr, Suite 340 Sterling, VA 20166	Howard Huang, CEO +1 (703) 215 8277	814855	IT auditing	20%	TBD

(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

6. Experience with VASCUPP members

The total amount fees invoiced to members of VASCUPP by Baker Tilly since January 2024 are as follows:

VASCUPP Member	Fees invoiced
George Mason University	$204,399.90
James Madison University	$12,000.00
University of Mary Washington Foundation	$54,722.50
Virginia Military Institute	$148,481.20
College of William & Mary	$25,591.71
UVA Health System (University of Virginia Health)	$40,000

7. Proposed cost

We propose value for fees. That means sharing industry insights, gaining efficiencies and directing our best resources to JMU.

Providing our standard hourly rates

Any fees will be based on our standard rates shown below. Before we send a final invoice, we confirm that you've received the value you deserve.

Existing Commonwealth Contract Internal Audit Rates

STAFF LEVEL	OFF-SITE HOURLY RATE	ON-SITE HOURLY RATE
Principal / Managing Director	$479.04	$526.95
Director / Senior Manager	$405.90	$446.49
Manager	$336.30	$369.93
Senior	$258.61	$284.47
Staff	$191.69	$210.85

Potential Discounted Internal Audit Rates (based on type and volume of work)

STAFF LEVEL	OFF-SITE HOURLY RATE	ON-SITE HOURLY RATE
Principal / Managing Director	$400.00	$440.00
Director / Senior Manager	$350.00	$385.00
Manager	$260.00	$286.00
Senior	$200.00	$220.00
Staff	$160.00	$176.00

No unnecessary charges

You won't see add-on charges for routine calls, emails or quick consultations. They're included in our fees because we're here to earn your trust. If your need is out of scope, we'll never perform additional work unless you give us the go-ahead. Our final billing will always be based on the value we deliver to you.

Key assumptions

We base our fee estimate on your needs. If any of the assumptions below change, we'll share any new requirements, budgetary considerations and options.

- Adequate support, preparedness, cooperation and feedback from management
- No major changes in scope or organizational structure, including mergers or expansions

Appendix A: Resumes

PRINCIPAL

Mike Cullen, CISA, CISSP, CIPP/US

Mike is a principal and the higher education cybersecurity and IT risk leader with the firm.

Baker Tilly Advisory Group, LP

8270 Greensboro Drive
Suite 400
McLean, VA 22102
United States

T: +1 (703) 923 8339
mike.cullen@bakertilly.com

bakertilly.com

Education

Bachelor of Science in business information technology
Virginia Polytechnic Institute and State University

Mike Cullen, a principal in Baker Tilly's risk advisory practice, helps clients tackle cybersecurity, data and information technology risks. He works with clients in multiple industries with a dedicated focus and extensive experience with higher education, research institutions, not-for-profit organizations and government contractors.

Since 2001, he has been executing various cybersecurity, privacy and IT assessments, myriad of IT internal audits, risk reviews for large transformation projects and numerous IT compliance projects.

Currently, Mike leads multifaceted practice teams with industry specialization all with the goal of helping clients protect data and systems and enhance cybersecurity and IT risk management practices.

Specific experience

- Interfaces with various client personnel from analysts to chief officers (e.g., information, business, financial, executive) as well as boards and trustees to advise and report on cybersecurity and IT areas in the appropriate context and without technical jargon
- Delivers reports tailoring those cybersecurity and IT concepts into actionable observations and practical recommendations
- Develops IT strategies including related guidance, practices and roadmaps for organizations focused on aligning IT operations with IT strategies that support an organization's overall mission, strategic plans and goals
- Empowers clients to address the opportunities and challenges posed by various cybersecurity and IT frameworks, laws, regulations and standards such as: FERPA, HIPAA, HITECH Act, PCI DSS, GLBA, NIST CSF, NIST SP 800, CMMC, ISO 27000, CIS Critical Controls, FAR/DFARS and GDPR
- Advises on various, large-transformation projects including myriads of system implementations by providing project management, risk management, resource management, issue management and strategy guidance before, during and after implementation/go-to-live
- Provides IT contract and vendor process consulting in the areas of enhancements to risk assessment, project deliverable, compliance and best practices in order to reduce client risk when working with vendors

Industry involvement

- Information Systems Audit and Control Association (ISACA)
- International Association of Privacy Professionals (IAPP)
- International Information Systems Security Certification Consortium (ISC2)
- Institute of Internal Auditors (IIA)

Thought leadership

- “Compliance Potpourri, IT, Privacy and Data Security,” “Getting Practical about Privacy,” “Cybersecurity threats in higher education,” “Protecting your institution with effective cybersecurity governance,” “Auditing your institution’s cybersecurity incident/breach response plan,” “Conducting a system implementation risk review at higher education institutions,” “Cyber risk emerging trends and regulatory update,” and, “Using IT Audit to Your Advantage,” Association of College and University Auditors (ACUA), presenter
- “Cyber Risk for Foundations,” “The Board’s Role in Cybersecurity,” and “Cybersecurity Issues That Keep You Up at Night,” Association of Governing Boards (AGB), presenter
- “The Cybersecurity Headache,” Association of Healthcare Internal Auditors (AHIA), author
- “IT Risk Assessment: Learn from Our Work, Leverage at Your Campus,” “Digital Transformation in a Time of Uncertainty,” and “CMMC Latest Developments and How to Prepare,” EDUCAUSE, presenter
- “A Framework for Auditing Mobile Devices,” Institute of Internal Auditors (IIA) GRC and All-Star conferences, presenter
- “More Malware, Less Ransomware in Higher Ed,” Inside Higher Ed, contributor
- “Cybersecurity Issues in Research,” “CMMC Should Scare You – Latest Developments and How to Prepare,” and “Research Data Discussion Group,” National Council of University Research Administrators (NCURA), presenter
- “CMMC and Cybersecurity – Addressing Now and Planning for the Future” and “CMMC and Cybersecurity for Research Data,” Society of Research Administrators International (SRAI), presenter
- “CMMC Should Scare You,” Society of Corporate Compliance and Ethics (SCCE), presenter
- “PCI Compliance Crackdown,” UniversityBusiness.com, contributor

MANAGING DIRECTOR

Chris Kalafatis, CPA, CIA, CFE

Chris is managing director of the firm's risk advisory public sector practice.

Baker Tilly Advisory Group, LP

8270 Greensboro Drive
Suite 400
Mclean, VA 22102

United States

T: +1 (703) 923 8007
chris.kalafatis@bakertilly.com

bakertilly.com

Education

Bachelor of Science in accounting
Virginia Commonwealth University

Chris is a self-motivated leader with more than 25 years of audit and consulting experience and is the public sector industry leader within Baker Tilly's risk advisory practice. He consistently delivers on commitments and achieves individual and team goals and offers strong management abilities, setting high expectations for himself and the teams he leads.

Specific experience

- Directly led projects with more than 50 public sector entities and more than 10 Fortune 1000 companies, including 30+ Commonwealth of Virginia state agencies or public universities
- Directed financial, operational, IT, SOX and compliance audits
- Supervised and/or performed more than 200 fraud investigations
- Presented audit reports and investigations to audit committees and executive management
- Served as chief audit executive for multiple internal audit outsource relationships
- Identified internal control issues and operational deficiencies that impacted service delivery to citizens, caused financial losses to state and local governments, and non-compliance with laws and regulations
- Uncovered collusion between city employees and a vendor that led to the arrest of nine individuals. This investigation revealed a culture of overtime abuse that was prevalent for approximately 20 years
- Partnered with a vendor to develop an app to allow citizens to report fraud on their smartphone. This city became the second local government in the U.S. to develop a fraud reporting app for citizens
- Previously served as director of internal audit at a Fortune 500 international company and reported to the CFO and audit committee. Also worked for the higher education specialty team for the VA Auditor of Public Accounts

Industry involvement

- Institute of Internal Auditors (IIA)
- Association of Local Government Auditors (ALGA)
- Association of Government Accountants (AGA)
- Association of Certified Fraud Examiners (ACFE)

Licenses and Certifications

- Certified Public Accountant (CPA)
- Certified Internal Auditor (CIA)
- Certified Fraud Examiner (CFE)

Thought Leadership

- Delivered more than 25 CPE presentations or webinars to audit and accounting organizations such as the IIA, AGA, ALGA, ISACA, and ACFE. Example topics included fraud, internal controls and supply chain management
- Authored multiple thought leadership articles on topics such as fraud and inventory management

Awards and Recognition

- Recipient of the AGA's 2024 Private Sector Financial Excellence Award given to an individual across the nation that exemplifies and promotes excellence in state or local government financial management, outstanding leadership, high ethical standards and innovative management techniques

PRINCIPAL

Brian Nichols, CISSP, CIPP/US

Brian is a principal in Baker Tilly's risk advisory practice.

Baker Tilly Advisory Group, LP

17 Cowboys Way
Suite 800
Frisco, TX 75034
United States

T: +1 (972) 748 0496
brian.nichols@bakertilly.com

bakertilly.com

Education

Master's in accounting and information Systems
Bachelor's in accounting and information Systems
Virginia Tech

Brian has more than 10 years of experience in developing cybersecurity strategies and enhancing cybersecurity programs for clients across retail, consumer, airline, railroad, healthcare and financial services industries. He is a proven leader in helping clients align their cybersecurity programs to their business objectives and effectively manage their cybersecurity risk. Brian leads teams in conducting cybersecurity capability assessments using various industry frameworks (e.g., NIST CSF, ISO 27001/2, CIS CSC, etc.). He has helped many organizations establish their cybersecurity program through developing strategies, policies and procedures, risk management methodologies, governance, controls libraries and metrics and reporting.

Specific experience

- Develops cybersecurity strategy and service catalogs aligned to business objectives and risk tolerance levels
- Builds cybersecurity risk management programs to assess and respond to emerging cybersecurity threats
- Assesses cybersecurity capabilities against industry frameworks and develops recommendations and roadmaps to enhance capabilities and manage risk
- Enhances data protection capabilities through risk-driven data classification and control requirements
- Develops effective and implementable security policies and standards based on industry best practices
- Performs incident response and remediation activities for PCI data breaches
- Performs ISO 27001 ISMS readiness assessments, including that for a global financial services client
- Develops cybersecurity thought leadership for mobile device security and unified security control frameworks
- Designs, implements and operates a Data Loss Prevention (DLP) solution, including one for a retail and pharmaceutical client
- Assesses security awareness capabilities and develops recommendations for enhancements and computer-based trainings

Continuing professional education

- Certified Information Systems Security Professional (CISSP)
- Certified Information Privacy Professional/United States (CIPP/US)
- Certified ISO Lead Implementer
- AWS Cloud Practitioner

SENIOR MANAGER

Peter Tsengas, CISA, CISM

Peter is a senior manager with Baker Tilly's risk advisory public sector practice.

Baker Tilly Advisory Group, LP

8270 Greensboro Drive
Suite 400
Mclean, VA 22102
United States

T: +1 (703) 827 9350
peter.tsengas@bakertilly.com

bakertilly.com

Education

Bachelor of Science in accounting and information systems
Virginia Polytechnic Institute & State University

Peter has more than 25 years of IT audit and IT risk and compliance consulting experience with three top 10 firms, and industry experience in the public sector and Fortune 500. He stays current on new industry technologies, risks and regulatory compliance requirements. Peter is experienced in leading managers and other team members and serving as a client relationship manager.

Specific experience

- Led and supervised IT risk and compliance projects with 40+ public sector entities in the Commonwealth of Virginia (COV), including IT security audits for sensitive systems and independent COV RAMP (formerly ECOS) assessments for third-party cloud hosted sensitive systems, to assess compliance with the Virginia Information Technologies Agency (VITA) IT Security Standard SEC530 (formerly SEC501/SEC525) and other industry best practice standards such as NIST (Publication 800-53 and NIST Cybersecurity Framework)
- Led and supervised multiple annual IT audits for Internal Audit outsourced public sector clients
- Led and supervised annual Agency Risk Management and Internal Controls Standards (ARMICS) IT general controls testing efforts for 10+ COV clients
- Led and supervised a business resiliency project for a COV client that included 50+ project stakeholders, and focused on delivering a revised business impact assessment (BIA), business continuity plan (BCP), and disaster recovery (DR) plan for the client
- Led and supervised multiple Independent Verification & Validation (IV&V) engagements for COV clients to assess compliance with VITA's project management standard (CPM 112) requirements
- Led and supervised a general controls IT risk and compliance engagement that resulted in improvements to the organization's IT security governance framework
- Previously served as an IT Auditor for several Commonwealth of Virginia state agencies, including the Auditor of Public Accounts (APA), Department of Corrections (DOC), and Department of Transportation (DOT), where he led and supervised multiple IT security audits, IT general controls audits, and IT systems development audits

Industry involvement

- Information System Audit and Control Association (ISACA)
- Institute of Internal Auditors (IIA)
- Association of Government Accountants (AGA)

SENIOR MANAGER

Peter Tsengas, CISA, CISM

Page 2

Thought leadership

- Delivered numerous IT risk and compliance focused presentations at CPE events across multiple states for organizations such as ISACA, IIA and the AGA
- Authored an IT whitepaper focused on the best practices for IT systems development

Continuing professional education

- Certified Information Systems Auditor (CISA)
- Certified Information Systems Manager (CISM)

SENIOR MANAGER

Joseph Schwendler, CISA, CRISC, CPA, CISM

Joseph is a senior manager with Baker Tilly's risk advisory practice.

Baker Tilly Advisory Group, LP

205 N Michigan Ave
28th Floor
Chicago, IL 60601
United States

T: +1 (414) 510 9978
joe.schwendler@bakertilly.com

bakertilly.com

Education

Bachelor of Business Administration
Marquette University

Joe is an IT audit specialist who utilizes technical knowledge and critical thinking to introduce new approaches to control design and optimization that deliver better results for key stakeholders, uncover growth opportunities for our business and expand the capacity of diverse teams to deliver on deadlines and more overall value.

Specific experience

- Oversees the development of system security plans based on client's current processes and controls
- Developed new and enhanced test plans and procedures over IT controls within PeopleSoft working with the center of excellence team to share with other engagement teams
- Worked closely with several key stakeholders on internal audits engagements to provide innovative best practice recommendations to approaching IT, operational and third party (SOC 1/2/3) assessments
- Positioned Governance, Risk, and Compliance (GRC) tools to optimize client monitoring and utilization
- Worked in engagement teams to ensure the client adhered to National Institute of Standards and Technology (NIST) or general data protection regulation (GDPR) standards by evaluating IT procedures, policies and controls ranging from the IT security control environment within the application and network layers

Industry involvement

- Information Systems Audit and Control Association (ISACA) chapter, Chicago
- American Institute of Certified Public Accountants (AICPA), Illinois

Community involvement

- Chicago Cares financial literacy

Continuing professional education

- Certified Information System Manager, ISACA
- Certified Information Technology Professional, AICPA
- Certified in Risk and Information Systems Control, ISACA
- Certified Public Accountant, Illinois, AICPA
- Certified Information System Auditor, ISACA

ADVISORY SENIOR MANAGER

Mitchell Gorham, CISSP, CDPSE, CCSK

Michell is an advisory senior manager with Baker Tilly's risk advisory practice.

Baker Tilly Advisory Group, LP

17 Cowboys Way
Suite 800
Frisco, TX 75034
United States

T: +1 (214) 420 3262
mitchell.gorham@bakertilly.com

bakertilly.com

Education

MBA in artificial intelligence and data science in business, Texas Tech University

Bachelor of Science in information systems, Park University

Mitchell Gorham specializes in risk mitigation, bringing over a decade of experience in cybersecurity and enterprise risk management to Baker Tilly. His expertise spans leading risk assessments, technology due diligence, internal audits, penetration testing and vulnerability scanning. Known for his ability to blend technical acumen with business insight, Mitchell effectively bridges IT and operations to drive organizational growth and achieve sustainable outcomes for his clients.

Specific experience

- Applied expertise in cybersecurity frameworks such as NIST CSF, ISO 27001/2, and PCI DSS to ensure compliance and enhance security posture
- Conducted rigorous evaluations of IT modernization initiatives, meticulously identifying and addressing risk, governance, and technical control gaps to fortify organizational resilience
- Provided expert guidance to clients on FedRAMP cloud migrations, meticulously ensuring adherence to regulatory standards and safeguarding against potential compliance risks
- Led the research, solution identification, funding approval, and execution for a tool that enabled the organization's first independent audit program, creating systematic alignment with NIST 800-53 and achieving RMF auditing requirements
- Developed and wrote security procedures, including SSP, SCTM, and CMP documents, creating a sustainable process to ensure compliance while standardizing processes

Industry involvement

- Information Systems Audit and Controls Association
- International Information System Security Certification Consortium, Inc. (ISC2)

MANAGER

Morgan Mincy, CPA, CMMC - RP

Morgan is a manager with Baker Tilly's risk advisory practice.

Baker Tilly Advisory Group, LP

8270 Greensboro Drive
Suite 400
McLean, VA 22102
United States

T: +1 (703) 923 8537
morgan.mincy@bakertilly.com

bakertilly.com

Education

Bachelor of Science in commerce, concentrations in information technology and accounting
University of Virginia

Morgan brings experience in providing risk advisory and internal control solutions. Her clients have included higher education institutions and research institutions.

Specific experience

- Assisted with a cybersecurity audit and gap assessment to analyze compliance with applicable regulations and frameworks (e.g., NIST), testing the client's internal controls surrounding cybersecurity for operating effectiveness and identifying opportunities for improvement in clients' policies, procedures and processes
- Assisted a university in conducting an IT risk assessment with a focus on the evaluation of risks associated with critical application systems and infrastructure components supporting key business processes
- Evaluates IT internal controls over financial reporting applications to ensure adequate design and operating effectiveness of system controls for a variety of clients
- Provided assistance in identifying, documenting and testing internal controls in relation to SOX compliance from a financial perspective
- Assists universities in performing operational assessments of their institution's compliance with the terms and conditions of grants

Industry involvement

- Institution of Internal Auditors (IIA), Northern Virginia Chapter
- Information Systems Audit and Control Association (ISACA), D.C. Chapter

Thought leadership

- "Third-Party Risk Management," IIA, Virginia Chapter, November 2022
- "Learn to Audit Cyber Compliance with NIST SP 800-171 for GLBA, NSPM-33, CMMC, etc.," Auditors of College and Universities Association (ACUA), mid-year conference, March 2023

Continuing professional education

- Certified Public Accountant (CPA), Virginia
- Cybersecurity Maturity Model Certification Registered Practitioner (CMMC – RP)

MANAGER

Amanda Guessford, CPA, CISA

Amanda is a manager with Baker Tilly's risk advisory practice.

Baker Tilly Advisory Group, LP

8270 Greensboro Drive
Suite 400
McLean, VA 22102
United States

T: +1 (703) 827 3921
amanda.guessford@bakertilly.com

bakertilly.com

Education

Bachelor of Science in accounting and information systems
Bachelor of Science in business administration
Virginia Polytechnic Institute and State University

Amanda has experience in providing information technology (IT) and cybersecurity risk advisory, internal audit and internal control solutions.

Specific experience

- Serves as lead project manager to develop and maintain relationships with clients and process owners, allowing for open communication and collaboration
- Performs and manages various IT and cyber-related internal audits (e.g., change management audits, device management audits, secure network engineering audits, internet of things audits) for higher education institutions and state systems
- Performs and manages IT regulatory compliance assessments [e.g., IT Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST), office of management and budget (OMB) A-123] for organizations by conducting risk reviews, control assessments, testing activities and gap analyses to identify deficiencies with internal controls and related processes and provide recommendations for compliance
- Conducts assessments to evaluate the processes for identifying, executing, managing and responding to research data security requirements
- Conducts IT risk assessments with a focus on the evaluation of risks associated with critical application systems and infrastructure components supporting key business processes
- Evaluates information technology internal controls over financial reporting applications to ensure adequate design and operating effectiveness of system controls for a variety of clients, including, higher education institutions
- Works in a co-sourced capacity with multiple organizations to assist in achieving the organizations' internal audit objectives
- Performs consulting services to plan, develop, execute and improve internal control procedures for suitability of design and operational effectiveness

Industry involvement

- American Institute of Certified Public Accountants
- Association of College and University Auditors
- Information Systems Audit and Control Association
- Institute of Internal Auditors – North Virginia Chapter (IIA)

MANAGER

Andrew Kennedy, CISA

Andrew is a consulting manager with Baker Tilly's risk advisory practice.

Baker Tilly Advisory Group, LP

11750 Katy Freeway
Suite 1100
Houston, TX 77079
United States

T: +1 (346) 318 0209
andrew.kennedy@bakertilly.com

bakertilly.com

Education

Bachelor of Business Administration in finance
Texas A&M University

Andrew has over 6 years of experience providing cybersecurity, financial, and process-oriented risk advisory, attestation, and consulting services to clients in both the public and government sectors. He maintains an industry-agnostic stance, has a proven record across a variety of geographies and revenue ranges, and is well versed in building cross-functional teams to bridge the gap between Business and IT Risk Management. He excels at developing risk-based approaches to designing and testing systems of internal controls, collaborating with process owners to effectively prioritize remediation efforts, and reporting key metrics, next steps, and current state observations to Management.

He is a Certified Information Security Systems Auditor with a background in Finance and assessing systems of internal controls across organizations of varying sizes.

Specific experience

- IT Due Diligence and Information Security Risk Assessments (NIST CSF, ISO 27001, etc.)
- Developing systems of internal controls, including the establishment of relevant policies, procedures, and standards.
- Internal Audit across Information Technology, financial, and business process areas
- ERP best practices, with a focus on Segregation of Duties
- SOC1 and SOC2 readiness and attestation
- Financial and IT SOX compliance
- Data privacy assessments (HIPAA, GDPR, CCPA/CPRA)
- Business Process Improvement
- Incident Response Planning
- Business Continuity and Disaster Recovery Planning
- Strategic Guidance
- Data Analysis

Certifications

- Certified Information Security Auditor (CISA), via ISACA.

SENIOR CONSULTANT

Ivan Imbuido, CISSP

Ivan is a senior consultant in Baker Tilly's risk advisory and cybersecurity practice.

Baker Tilly Advisory Group, LP

17 Cowboys Way
Suite 800
Frisco, TX 75034
United States

T: +1 (972) 748 0300
ivan.imbuido@bakertilly.com

bakertilly.com

Education

Bachelor of Science in information technology
Colorado Technical University

Ivan has more than 10 years of experience in digital forensics, security compliance and penetration testing. Additionally, Ivan has more than eight years of experience in system and network administration in the government sector. He has led cross-functional teams in defining, developing and delivering managed threat detection and response services.

Ivan currently holds several industry certifications such as CISSP, GWAPT, CEH and Security+. He has successfully completed training in AlienVault USM Anywhere, SANS 578, SANS 560, SANS 542, InfoSec Institute, and Reid Technique of Interview and Interrogation.

Specific experience

- Penetration testing to identify vulnerabilities and evaluate the security posture of client environments and conforming to the MITRE ATTACK framework, OWASP Top 10, CIS Top 20 and NIST cybersecurity framework: external, internal, wireless, web application and social engineering and phishing campaigns
- Digital forensics and incident response services to global customers involved in cyber incidents, including network investigations, analysis, monitoring and vulnerability and threat management
- Led cross-functional teams in the product development lifecycle of the AlienVault platform including creating use cases, defining technical specifications, and defining development priorities using the Scaled Agile Framework for Enterprises (SAFe) methodology

Continuing professional education

- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- Alien Vault Security Engineer (AVSE)
- GIAC Web App Penetration Tester (GWAPT)
- Certified Penetration Tester (CPT)
- Certified Computer Forensics Examiner (CCFE)
- Security+ (CompTIA)

Appendix B: Introducing Ignitec

Company Description

Ignitec, Inc. (Ignitec), founded in 2018, is a Virginia-based, Small Business Administration (SBA) minority-owned disadvantaged small business delivering dynamic and innovative solutions and staffing to complex challenges across the fields of IT, Telecommunications, Accounting, Finance, Human Resources, Engineering, Program Operations, Procurement, and Supply Chain Management.

Under the leadership of Howard (Howie) Huang, Ignitec's President and CEO, we have built a robust capability to deliver strategic solutions that address the evolving needs of government (federal, state, county, and city) agencies and commercial enterprises. Howie's extensive experience in management, technology, and government contracting enables Ignitec to offer comprehensive, tailored, and scalable services that integrate cutting-edge technologies and best practices to optimize business performance and streamline operations for each of our clients.

Ignitec is a leading provider of specialized workforce solutions with core competencies in technology, finance, project management, and strategic staff augmentation. Our expertise spans various domains, including software engineering, application development, data management, financial analysis, budgeting, accounting, and comprehensive project management support. This capability, combined with our commitment to operational excellence and fostering a dynamic work environment, positions Ignitec as a trusted and vital partner.

Ignitec has extensive experience in IT security audits and consulting, along with financial analysis and oversight. Our team specializes in evaluating system vulnerabilities, ensuring compliance with regulatory requirements, and implementing effective risk management strategies. We approach security audits with precision, conducting comprehensive assessments of IT systems to identify risks and recommend actionable solutions. This includes reviewing policies, procedures, and technical controls to ensure organizations meet industry standards and safeguard their digital environments.

Our consulting expertise lies in guiding clients to enhance their IT security frameworks. By implementing tailored solutions, we help organizations mitigate threats, improve incident response, and strengthen system resilience. Our team is skilled in areas such as access control, data encryption, and network security. These capabilities enable us to support organizations in achieving robust protection against evolving cybersecurity threats.

In the financial domain, we excel in providing critical insights through financial audits, compliance reviews, and budgeting support. We assist clients in aligning financial practices with federal standards such as GAAP while enhancing reporting accuracy and decision-making. Our analysts evaluate financial processes to ensure efficiency and accountability, contributing to optimized resource allocation and long-term financial stability.

Through our work, Ignitec demonstrates a commitment to precision, reliability, and tailored support. We enable clients to maintain secure systems and sound financial practices, empowering them to focus on achieving their strategic objectives with confidence.

Consultant Bios

Senior IT Audit Consultant – Jean Kouadio

Jean Kouadio, MSc, CISM, CASP+CE, MCSE, PMP, is a Senior IT Audit Consultant with over 26 years of expertise in IT security, information assurance, and cybersecurity. He has successfully led and executed complex IT security and compliance initiatives for prominent government clients, including the FDIC, CMS, FAA, DOE, HUD, and more. Jean excels at implementing NIST frameworks, managing Security Assessment and Authorization (SA&A), and delivering risk assessments and security documentation in compliance with FISMA, FedRAMP, and other regulatory standards. His deep technical acumen, combined with a proven record of aligning IT security solutions with organizational goals, positions him as a trusted leader in the field.

Holding multiple advanced certifications, including CISM, PMP, CASP+CE, and MCSE, Jean is well-versed in assessing, managing, and mitigating enterprise-level cybersecurity risks. He has consistently demonstrated his ability to lead cross-functional teams, support CIOs and CISOs, and develop comprehensive cybersecurity strategies that ensure regulatory compliance while enhancing operational efficiency.

Key Highlights

- **Extensive Federal Experience:** Supported IT security programs for agencies like FDIC, CMS, FAA, DOE, HUD, and Amtrak Police Department, focusing on SA&A, FISMA compliance, and risk management.
- **Comprehensive Cybersecurity Expertise:** Implemented and assessed security controls using NIST standards (800-53, 800-53A, 800-37) and frameworks like FedRAMP for both on-premises and cloud systems.
- **Proven Leadership in SA&A:** Successfully led over 200 SA&A processes, achieving Authorizations to Operate (ATO) for numerous General Support Systems (GSS) and applications.
- **Policy Development:** Created and maintained essential IT security policies, including Access Control, Incident Response, and Contingency Planning, tailored to meet client-specific regulatory needs.
- **Strong Technical Acumen:** Hands-on expertise with tools like Nessus, WebInspect, AppScan, and ServiceNow to manage vulnerabilities, track POA&Ms, and enhance IT security postures.
- **Recognized Certifications:** Holds certifications such as Certified Information Security Manager (CISM), Project Management Professional (PMP), and Microsoft Certified Systems Engineer (MCSE).

IT Audit Consultant – Marie Grace

Marie Grace is a Certified Information Systems Auditor (CISA) and accomplished Senior IT Audit Consultant with over seven years of experience conducting IT audits, risk assessments, and compliance reviews across government and commercial sectors. She has a proven record of supporting high-profile organizations like the U.S. Secret Service (USSS), Navy Federal Credit Union, and Cardinal Bank in implementing and assessing IT controls, evaluating compliance with regulatory frameworks, and mitigating operational risks. Marie specializes in IT General Controls (ITGCs), Information Security, and Enterprise Resource Planning (ERP) system audits, leveraging her expertise to enhance organizational security postures and ensure regulatory compliance.

Marie holds certifications such as CISA, CompTIA Security+, and Professional Scrum Master (PSMI), which complement her technical proficiency in tools like MetricStream, Teammate, ServiceNow, and AuditBoard. Her deep knowledge of frameworks like NIST, SOX, PCI, COBIT, and ITIL allows her to provide tailored recommendations to improve control environments and reduce risk. With a results-oriented approach and a commitment to safeguarding information systems, Marie consistently delivers value through strategic audits and innovative risk management solutions.

Key Highlights

- **Comprehensive IT Audit Expertise**: Skilled in conducting ITGC and IT application controls testing, SOC reporting, and compliance audits using frameworks like NIST, SOX, and PCI.
- **Diverse Client Experience**: Supported critical IT audit and compliance initiatives for organizations such as USSS, Navy Federal Credit Union, and Cardinal Bank, ensuring effective risk management and operational resilience.
- **ERP and Information Security Audits**: Executed audits for SAP, Oracle Financials, and cloud computing environments, assessing the adequacy and effectiveness of controls.
- **Regulatory Compliance Leadership**: Conducted A-123 internal control testing, risk assessments, and POA&M management to address gaps and align with regulatory mandates.
- **Technical Proficiency**: Proficient with tools such as Teammate, AuditBoard, ServiceNow, and Nessus, supporting efficient audit execution and reporting.
- **Certifications and Education**: Holds CISA, CompTIA Security+, and PSMI certifications, with a Bachelor's degree in International Business from the University of Paris-Sorbonne.

IT Audit Consultant – Nuro Osman Auro-Akondo

Nuru Osman Auro-Akondo is a dedicated Senior IT Audit Consultant with over six years of experience in IT assurance, compliance, and risk consulting. His expertise encompasses testing IT General Controls (ITGCs), Application Controls (ITACs), and ERP systems, particularly SAP. Nuru has worked on both internal (SOX) and external (SSAE 18/SOC) audits for financial services, healthcare, and other industries, ensuring compliance with frameworks such as COBIT and HIPAA. His proven ability to analyze risks, identify control gaps, and implement robust audit procedures has consistently supported clients in achieving operational excellence and regulatory compliance.

Nuru's technical proficiency with tools like SQL, UNIX, Linux, ACL, and IDEA enhances his ability to conduct thorough audits and data analysis. Having passed the Certified Information Systems Auditor (CISA) exam, he is positioned as a trusted expert in IT auditing and compliance.

Key Highlights

- **Comprehensive IT Audit Expertise**: Conducted ITGC and ITAC testing to ensure control effectiveness and compliance with SOX 404, FSA, and PCAOB standards.
- **ERP System Proficiency**: Experienced in auditing ERP systems, particularly SAP, focusing on completeness, accuracy, and control reliability.
- **SOX and SSAE 18/SOC Audits**: Led audits for SOC 1 and SOC 2 reports, including process walkthroughs, control testing, and risk assessments for financial and healthcare entities.
- **Risk and Compliance Leadership**: Performed impact and risk assessments, identified control deficiencies, and provided recommendations for performance improvement.
- **Technical Acumen**: Skilled in leveraging tools like SQL, ACL, and IDEA for audit analytics and data validation, with hands-on experience in UNIX, Linux, and Active Directory environments.
- **Certifications and Education**: Passed the Certified Information Systems Auditor (CISA) exam; pursuing an MBA in Marketing at Lincoln University.

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