August 26, 2022

RSM US LLP

250 West Street
Suite 200
Columbus, Ohio 43215

T 614 224 7722

www.rsmus.com

The City of Columbus
Department of Technology
Attn: Purchasing Agent
90 West Broad Street
Columbus, OH 43215

Dear Purchasing Agent:

The following proposal, in response to RFQ 022363, reflects our understanding of your needs, summarizes our experience, and illustrates the approach we will take in providing professional services for The City of Columbus (City). Highlights include:

**Commitment to the industry and experience serving governmental entities**
Nationally, we serve more than 5,100 public sector clients, including nearly 450 government clients. We serve numerous public sector clients throughout the country, including large counties, cities, colleges and universities, school boards and other nonprofit organizations.

We have relevant experience in serving state level agencies at various levels across the country. Not only have we worked with local agencies located within Franklin County, but also have served a number of agencies in Ohio, such as Northeast Ohio Regional Sewer District.

**Providing IT and cybersecurity services since 2007, PCI assessment services since 2003 and a PCI Qualified Security Assessor (QSA) Company (QSAC) since 2007**
Additionally, we have served many government agencies and associations providing similar services across the nation, including Prince William County, City of Sacramento and counties of Alachua, Brevard and St. Lucie, to name a few. This shows that we understand the issues unique to your operations and will not require on-the-job training.

**In closing**
Our strongest statement about what differentiates RSM from the other firms comes directly from the clients we serve and the partnerships we forge with them. Our client-centric service philosophy—along with our professionalism, reliability and commitment to timeliness—has resulted in highly satisfied clients. We encourage you to contact our clients and hear it from them.

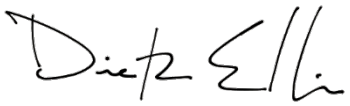
We share the City's goals of security, efficiency and transparency, and look forward to working alongside your team to implement a GRC system that provides you with peace of mind. Our team looks forward to building a long-term relationship with the City and delivering value for your organization, now and well into the future.

Once you have had the opportunity to review this response, we would be pleased to discuss your needs in greater detail or make a presentation to your team. In the meantime, please feel free to contact us with any questions.

Sincerely,

**RSM US LLP**

Andrew Weidenhamer
Principal, State and Local Government
+1 703 336 6572



Dietz Ellis
Director, Security and Privacy
+1 404 751 9049

# PROPOSAL TO PROVIDE IT AND CYBERSECURITY PRODUCTS AND SERVICES

THE CITY OF COLUMBUS

August 26, 2022

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

# TABLE OF CONTENTS

## SECTION A: UNDERSTANDING OF THE PROJECT APPROACH

The City is looking to implement a Governance, Risk and Compliance (GRC) platform that will enable the management of IT investments and associated cybersecurity risks. This platform will serve as an enabler to perform additional enhancements outlined within the RFQ.

### Services area A: Governance, risk and compliance products and services

RSM will assist the City with the full range of GRC consulting services, including requirement development, product evaluation, implementation and training of the City's selected solution. RSM has tailored our approach to meet the needs of the City by using the following methodology.

#### Planning and design process

The initial planning session will be used to better understand the City's overall cybersecurity strategy and strategic security initiatives, as well as to understand who the primary stakeholders are for the GRC implementation, including project sponsor.

This planning session will also be used to educate the City on common GRC solutions that we have seen implemented within the state and local government sector. Our understanding of the City's strategy and its strategic objectives will be used as an input during the next phases where we assist in determining gaps within your information security strategy.

Further, we will meet with you and your management team to understand the City's current security governance processes and identify opportunities for enhancements to increase communication and knowledge sharing. The goal of this phase is to further understand the relevant stakeholders and your organization's strategy and goals. This insight will facilitate tailored recommendations, that align with your business strategy and risk tolerance, to enhance your security posture. As needed, this phase will include interviews with stakeholders and the review of corporate governance processes and related documentation.

#### GRC selection process

RSM will assist the City in its review and refinement of GRC requirements and objectives, and further develop these where necessary. We will also facilitate the interview and workshops process and work to develop scoring and evaluation criteria to aid selection of a GRC solution. Once selection is complete, a presentation to City stakeholders will be made detailing the scoring results of the evaluation.

#### Build and rollout process

After the City has selected it's GRC solution, RSM will work to operationalize the deployment with the technology through a structured build and rollout process. The city has identified four functional areas which RSM will work with the organization to deploy alongside change management protocols and training initiatives:

- Security planning, assessment and compliance management
- Cybersecurity risk management
- Vendor risk management
- Governance management

Our deployment approach to implementation for each functional area is as follows:

***Step 1: Analyze***

- Review data sources and integration requirements
- Identify GRC requirements
- Conduct working session(s) to review and finalize business requirements, including process documentation and workflows
- Review GRC solution demos with business and technical stakeholders

***Step 2: Design***

- Document process workflows to guide configuration
- Document access requirements, including roles, groups, authentication requirements and permissions
- Participate in a collective demo review to provide subject matter specialist feedback and considerations

***Step 3: Build***

- Review the initial build and validate coverage of business requirements
- Conduct workshops to discuss requirement gaps (where needed) and identify resolution approach
- Socialize business process taxonomy and review specific data fields required
- Configure the selected GRC platform based on gathered requirements
- Review configured environment with stakeholders as part of iterative build process

***Step 4: Test***

- Develop test plan and User Acceptance Testing (UAT) scripts to assess requirements and help ensure that they are implemented and operational
- Review UAT identified defects and issues to confirm the specific business or technical requirement gap
- Remediate defects, as applicable, and obtain approval or retest
- Obtain City signoff and approval on UAT
- Remove test data/records

***Step 5: Deploy***

- Obtain final signoff, remove testing data and deploy the solution into a production state
- Lead trainings and deploy role-based training curriculum for users and administrators, and change management support
- Provide post-deployment support as needed

Each functional area may also contain process specific steps or considerations as noted below.

**Security planning, assessment and compliance management**

During this portion of the project, we will assist with:

- Cataloging and categorize IT-dependent business processes and applications, then mapping these relationships to business processes
- Facilitate the development of a cybersecurity control environment, then linking controls to baselines

- Developing workflow to enable plans of action and milestones to be captured alongside tracking, reporting and remediation of deficiencies and mitigation efforts
- Developing real-time reporting and dashboarding for compliance assessment, planning, and remediation activities

**Cybersecurity risk management**
During this portion of the project, we will assist with:

- Tailoring the risk assessment methodology, scoring, and risk processes to be consistent across the environment
- Developing a consistent risk assessment process and maintain risks within a single risk register
- Allowing risks to be correlated to controls, applications, and business processes and align scoring to the City's chosen risk frameworks
- Developing real-time reporting and dashboarding for risk reporting, oversight, and remediation activities

**Vendor management**
During this portion of the project, we will assist with:

- Alignment of vendor scoring and assessment methodologies across agencies, departments and divisions utilizing the platform
- Onboarding of vendor data, including linkage of vendor to vendor contracts and to City staff responsible for vendor management
- Developing workflow to enable findings, mitigation plans and exceptions to be tracked and actioned
- Developing real-time reporting and dashboarding for management of vendor risk, assessment status, and remediation activities

**Guidance management**
During this portion of the project, we will assist with:

- Loading and storing of guidance documents and associated linkages to GRC elements
- Automation of the review and approval lifecycle for governance documents
- Developing workflow to enable plans of action and milestones to be captured alongside tracking, reporting and remediation of deficiencies and mitigation efforts

## Services area B: IT security governance assessment services

RSM will perform cyber maturity assessments against in-scope city agencies as laid out within the RFQ. The main objective will be to evaluate the agencies' overall security posture and identify areas of higher risk. This information will be made easily digestible through the use of a business intelligence platform which will allow the City to evaluate the data in a number of different ways, including, but not limited to, the following:

- Agency maturity scores
- Domain specific maturity scores across agencies
- Specific control deficiencies across agencies

RSM's cybersecurity maturity assessment methodology is designed to evaluate the maturity of an organization's security program through review of its current set of controls and uses a prioritized maturity approach designed to identify areas of weak or missing controls that could result in a security or compliance risk. This assessment is a critical benchmarking tool in the development of a comprehensive security program and for determining readiness for future assessments and audits. The process involves interviewing key individuals within the organization and observing functions while on-site.

We use the NIST Cybersecurity Framework (CSF), which consists of standards, guidelines and standard industry practices to manage cybersecurity-related risks, threats and vulnerabilities present in the environment. This framework provides a prioritized and flexible approach to promote the protection of the organization's systems, infrastructure and operations. As such, the assessment will measure the City's environment based on the ability to identify, protect, detect, respond to and recover from a cyber event, which are the key functions of the NIST CSF. The goals of this assessment are as follows:

- Provide an independent verification and help ensure that the current security program meets the City's requirements.
- Provide a method for measuring the current state of the organization's information security program and whether that state has changed from previous assessments.
- Adopt standard industry practices by conforming to legal and industry regulations.
- Help build maturity through both tactical and strategic plans that identify immediate countermeasures and impact points.

We will conduct a design-level assessment of the current implementation of the technology, architecture and processes used for enterprise security execution and management against the NIST CSF cybersecurity requirements. We will review select documentation/configurations and interview stakeholders, process owners and functional staff. Tasks will include the following:

- Interview IT personnel to understand the current controls or governance framework(s) in place to align with industry practices or regulatory requirements.
- Review and compare strategic security goals and security operations.
- Conduct interviews with key personnel across departments and groups, including IT security and IT operations staff.
- Review high-level inventories of systems, applications, networks and configuration standards.

### Planning and stakeholder analysis

We will meet with you and your management team to understand the current security governance processes and identify opportunities for enhancements to increase communication and knowledge sharing.

### Current-state assessment

During this phase, we will conduct a design-level assessment of the current technology, architecture and processes used for enterprise security execution and management against the NIST CSF. Our team will review existing documentation and interview stakeholders, process owners and functional staff.

Common tasks to be completed during the NIST CSF-based current-state analysis include the following:

- Interviewing relevant personnel to understand the current control or governance framework(s) in place to align with industry practices or regulatory requirements
- Reviewing and comparing strategic security goals and security operations
- Conducting interviews with key personnel across departments and groups (security, IT operations, human resources, legal/compliance, etc.) to understand current security-related processes in place
- Reviewing supporting policies, procedures and other operational design documents
- Reviewing system configurations to help ensure alignment with overall objectives
- Interviewing management to understand the perceived and desired maturity levels

### Maturity analysis

RSM will create a current-state baseline by assessing the completeness of the overall program and the details of the processes and technology components against the selected control framework, NIST CSF. This phase will be focused on assessing the maturity levels and design of specific controls.

Control maturity is a qualitative method of determining the effectiveness of implemented controls at mitigating identified risks. Control maturity is assessed not only on meeting technical specifications, but also maintaining and enforcing technical controls through policies, procedures and governance. Our approach gauges both the pervasiveness of the technologies and processes implemented, as well as the governance of the controls and overall data protection program, and indicates whether a mature, repeatable process is in place to support security controls.

Each control is rated on a five-point scale based on how well the organization maintains the controls from both a governance and tactical perspective. The rating helps identify whether maturity improvements are rooted in technology, policy or procedural deficiencies. We recognize and aim to provide reasonable recommendations for program maturity, recognizing that rarely do organizations need to seek a top maturity level. Rather, we recommend using a risk-based approach to target maturity levels so the security posture is business reasonable.

After completing the interviews and reviewing the documentation provided by City, we will perform the following activities to develop a detailed matrix of maturity levels:

- Review the current state of processes and capabilities against the NIST CSF to develop maturity ratings for each of the relevant NIST CSF categories.
- Compare with the current security levels to provide targeted recommendations to improve the maturity of the security program.
- Document each identified item in a matrix, including the recommended improvement, to align with the specific objective, as well as the level of risk posed to the organization.

## Services area C: Information system inventory and security planning services

### Inventory and security planning

RSM will assist with the creation of system security plans and associated attributes. These plans will be housed within the GRC environment and will be based on the NIST 800-18 Guide for Developing Security Plans for Federal Information Systems.

RSM will work with the City in defining the following system security plans attributes:

- Security roles
- Security categorization
- Legal or regulatory requirements
- Business purpose
- Component inventory
- Interconnections

Additionally, RSM will assist the City with identification of assets by performing some of the below steps:

- Reviewing existing documentation, including at least network diagrams, subnet schemas, and other architecture data
- Install traffic capture technology for automated asset discovery, including some metadata (e.g., operating system and manufacturer)
- Compare results of asset discovery to subnet allocations to identify where manual scanning is required
- Perform additional manual scanning where necessary

## Services area D: Information system security assessment services

RSM will perform penetration testing and system assessments against whichever compliance requirements (e.g., PCI, IRS 1075, etc.) are identified within the system security plans developed in the previous phase. Where there is a system that is not subject to compliance requirements, the NIST 800-53 R5 moderate security baselines will be used.

### NIST SP 800-53 R5 moderate baseline assessment

RSM's NIST SP 800-53 R5 moderate baseline cybersecurity maturity assessment methodology is designed to evaluate the maturity of an organization's security program through review of its current set of controls. The process involves interviewing key individuals within the organization and observing functions. We use the NIST SP 800-53 R5 baseline, which consists of standards and guidelines to manage cybersecurity-related risks, threats and vulnerabilities present in the environment. This framework provides a prioritized and flexible approach to promote the protection of the organization's systems, infrastructure and operations. As such, the assessment will measure the City's environment based on the ability to identify, protect, detect, respond to and recover from a cyber event, which are the key functions of NIST SP 800-53 R5 moderate baseline. The goals of this assessment are as follows:

- To provide an independent review of the current security program of the City's in-scope applications and supporting systems
- To provide a method for measuring the current state of the organization's information security program and whether that state has changed from previous assessments

- To adopt common practices by conforming to regulatory requirements
- To help build maturity through both tactical and strategic plans that identify immediate countermeasures and impact points
- Identify any systems covered by IRS publication 1075 and perform review and analysis as applicable

We will conduct a design-level assessment of the current implementation of the technology, architecture and processes used for enterprise security execution and management against the NIST SP 800-53 R5 cybersecurity requirements. We will review select documentation and configurations and interview stakeholders, process owners and functional staff. Tasks will include:

- Interviewing IT personnel to understand the current controls or governance framework(s) in place to align with industry practices or regulatory requirements
- Reviewing and comparing strategic security goals and security operations
- Conducting interviews with key personnel across departments and groups, including IT security and IT operations staff
- Reviewing high-level inventories of systems, applications, networks and configuration standards

**Discovery and boundary review**

During this phase, we will work with the City to confirm the appropriateness of the boundary of the in-scope environment subject to NIST SP 800-53 R5 moderate requirements, including the in-scope applications/data and supporting hardware. Clearly defined system boundaries are important to protect against unexpected expansion of system scope.

During this step, we will assess the use of segmentation, security zones, network access controls and authentication measures that make up the system boundary subject to NIST SP 800-53 R5 requirements. We will review key data flows, facilities, connections and technologies within this environment.

## External penetration testing

The objective of external penetration testing is to assess current security controls in an effort to determine the actionable impact from an attacker attempting to bypass perimeter security controls and accessing the internal network or sensitive data. The focus of penetration testing is not to prove that the network is free of all vulnerabilities, but rather to validate your organization’s security posture and configuration standards through assessing the resiliency of the external network against a determined attacker. This level of testing relies heavily on the techniques and toolsets favored by real-world threat actors in order to closely simulate an attack scenario, and leverages both manual and automated testing methods.

The product of external penetration testing is a report that documents the organization’s existing security posture, identifies specific weaknesses and vulnerabilities, provides purpose-built exploit code and examples that tell a compelling story of risk from any given vulnerability and makes recommendations for remediation. Systems that are commonly in-scope for such an engagement include, but are not limited to, the following:

- Application servers
- Network devices (load balancers, firewalls, etc.)

- Cloud infrastructure
- Mail servers

Any critical finding discovered during the penetration testing will be immediately reported informally to your organization's technical staff and point of contact.

RSM closely aligns to the Penetration Testing Execution Standard (PTES) and follows the below approach:

- **Footprinting.** The footprinting process is used to determine the amount of information available through public sources concerning your organization. Our footprinting process can include, but is not limited to, the following:
  - Mapping of domain names
  - Domain Name Service (DNS) zone transfers attempts
  - American Registry of Internet Number searches
  - DNS lookups
  - Traceroutes to public systems
- **Service and port identification.** The service and port identification process is performed to identify services and ports, as well as the associated versions running on systems identified through the footprinting process. Our service and port identification process can include, but is not limited to, the following:
  - Network port scanning
  - Shodan searches
- **Vulnerability identification and exploitation.** From the information obtained in the service and port identification process, RSM uses available resources, both online and through well-known hacking tools, to identify applicable vulnerabilities and potential public exploits. In the event that a public exploit exists, we will attempt to execute it with the objective of obtaining access to the affected system or application.

The following illustrates some of the different vulnerabilities/attack types that we could cover during our external penetration testing. This list is not intended to be exhaustive, and the actual testing performed depends on the specifics of your organization.

- Layer 7 attacks
  - SQL injection
  - Exploitation of file upload vulnerabilities
  - Authentication bypass techniques
  - Directory traversal
- Brute-force attacks
  - Reverse and forward brute forcing attacks against company and default usernames
- Network-/operating system-layer attacks
  - Exploitation of operating system and software-related vulnerabilities and misconfigurations
- Cloud vulnerabilities
  - Permissive S3 buckets
  - Misconfigured APIs
- Data protection
  - Transport
  - Storage

During this testing, denial-of-service vulnerabilities may be identified, but exploitation will not be attempted in order to not affect your business. Also, it is possible that there may be some high-risk vulnerabilities that we mutually agree to not exploit due to the potential risk to system stability.

- **Limited vulnerability scanning.** Basic vulnerability scanning involves using various commercial and open-source tools to identify vulnerabilities on your organization's systems and devices. Our limited vulnerability scanning includes, but is not limited to, the following:
  - Ping scans of public IP address blocks and internal systems
  - Port scans of public systems
  - Basic vulnerability testing using commercial and open-source tools to determine how much information can be harvested from your public computing assets
  - Manual false-positive identification when possible
  - Mapping of technical risk to business function
- **Post-exploitation.** In the event that RSM is successful at exploiting a vulnerability using a publicly available or custom exploit, we will continue our penetration efforts through our post-exploitation process. This process has a specific focus on obtaining access to sensitive systems and data. Post-exploitation includes, but is not limited to, the following:
  - Internal network enumeration
  - Lateral movement across the corporate network
  - Gaining access to sensitive applications and data (e.g., file servers, database servers, corporate laptops)
  - Installing persistence (when applicable and when allowed)

All data will be sent to an external server hosted and managed by RSM.

### Internal Penetration Testing

The objective of internal penetration testing is to assess your current security controls in an effort to determine the actionable impact from an attacker gaining access to the internal network. The focus of penetration testing is not to prove that the network is free of all vulnerabilities; rather, the focus is to validate your organization's security posture and configuration standards through assessing the resiliency of the internal network against a determined attacker who has compromised your perimeter. This level of testing relies heavily on the techniques and toolsets favored by real-world threat actors in order to closely simulate an attack scenario, and leverages both manual and automated testing methods. The product of internal penetration testing is a report that documents the organization's existing security posture, identifies specific weaknesses and vulnerabilities, provides purpose-built exploit code and examples that tell a compelling story of risk from any given vulnerability, and makes recommendations for remediation.

Similar to the above external penetration testing, RSM aligns to the PTES for completing internal penetration testing, and as a result, uses a similar methodology to the above testing. However, during this phase, we operate from behind your firewall and test your internal network assets. Examples of some common devices tested include, but are not limited to, the following:

- Network infrastructure, such as routers, switches and wireless access points
- Security infrastructure, such as firewalls and intrusion detection/prevention systems
- Servers (domain controllers, application servers, etc.)
- User workstations
- Internal applications

The following illustrates some of the different vulnerabilities/attack types that we could cover during our internal penetration testing. This list is not intended to be exhaustive, and the actual testing performed depends on the specifics of your organization.

- Layer 2 attacks
  - VLAN hopping
  - Address Resolution Protocol cache poisoning
  - Insufficient segmentation and access controls
  - Exploitation of weaknesses within the switched architecture related to trunking, Spanning Tree Protocol or failover protocols
- Layer 3 attacks
  - IP address redirection
  - Session hijacking
  - Session replay
  - Password capture
- Network-/operating system-layer attacks
  - Network pass-the-hash
  - Exploitation of Dynamic Host Configuration Protocol weaknesses
  - Microsoft and UNIX weaknesses
  - Compromise of network control equipment
  - Exploitation of operational traffic flows (man-in-the-middle attacks)
- Logical attacks
  - Abuse of functionality
  - Privileged account compromise
  - Dormant account take over
  - Active Directory misconfiguration abuse
- Data protection
  - Transport
  - Storage

## Services area E: IT assessment services

Utilizing the outputs of Services area C, RSM will perform assessment utilizing the GRC environment to review system use, technical condition, staff resources and associated business processes, and classify systems utilizing the Gartner Xas-a-service (XaaS) framework.

RSM will work to develop reports within the GRC platform that identify opportunities for greater return on value in systems planning and deployment.

## Services area F: Cybersecurity incident response services

RSM handles approximately 250+ cyber incident responses per year. The types of incidents we typically encounter fall into a range of categories, including:

- Malware
- Ransomware
- Theft of intellectual property/trade secrets
- Business email compromise (Microsoft Office 365, Gmail, Microsoft Exchange)
- Active incident project management
- Security awareness training
- Post-incident remediation and recovery
- PC/mobile device analysis
- Incident response plan (IRP) development and review
- Post-incident shadow audit/review and assessment
- Financial fraud/internal or government inquiries
- Cyber threat intelligence
- Wire transfer/W-2/tax fraud
- Lost or stolen devices
- Web application compromise
- Endpoint detection and response proactive network monitoring
- Incident response tabletop exercises
- Employee misconduct/IT separation due diligence
- Expert witness services

RSM is available to assist the City with incident response services.

**Cybersecurity response consulting services**
RSM understands the primary objective is to provide on-call cybersecurity response consulting support to allow the City to engage RSM for assistance in the event a cyber event occurs. Should a cyber event occur, The City will have the ability to contact RSM's security operations center support team through a dedicated toll-free number. An on-call analyst will be available 24/7 during the service period and will acknowledge the event. Once the declared incident is reviewed by the on-call analysist based on the service levels, a member of the RSM incident response team will contact the City to discuss the event and start the process of determining if an incident occurred.

**Declared incident consulting support**
A "declared incident" is when the City requests RSM to provide consulting services in relation to any malicious act or suspicious event that compromises, or was an attempt to compromise, the City's infrastructure, or disrupts, or was an attempt to disrupt, the security of the City's operations.

For each time that the City declares an incident, RSM will acknowledge the incident, provide initial contact and initiate response consulting activities, but not necessarily provide a complete resolution. For the duration of the consulting services, the City will have access to the RSM security operations center support team to initiate acknowledgement. If an incident is declared, the City may determine to engage RSM to perform incident response and forensic services via a new Statement of Work.

**Incident response forensic support**
We will conduct a review of available network, system and application log files for evidence of unauthorized access, acquisition or use of network, egress of electronically stored information or other types of malicious activity, computer systems and/or electronically stored information. Analyze relevant information for evidence of unauthorized access to the network, computer systems and/or electronically stored information, IOCs or malicious sources and activities. Analysis tasks may include the following:

- Perform log file reviews from systems, applications, networking equipment, etc.
- Perform a review of email header/metadata information.
- Perform an automated/manual review for email attachments to determine if email attachments possess malicious capabilities.
- Review activity for unauthorized access to computer systems, networks, databases, attached network storage or applications and unauthorized access to or acquisition of electronically stored information.
- Perform an automated and/or manual review for evidence of malicious files and determine capabilities of any suspect software that is located.
- Attempt to identify the attack vectors utilized to compromise the impacted systems and/or applications.
- Attempt to identify potentially compromised information and determine whether or not it was exfiltrated.

**Incident response remediation assistance**
We will provide remote and/or incident response and IT infrastructure support to assist with containment, recovery and remediation efforts.

During this evaluation, we will provide resources as needed to continue with the recovery requirements. Our team will perform triage, recovery and remediation tasks that may include the following:

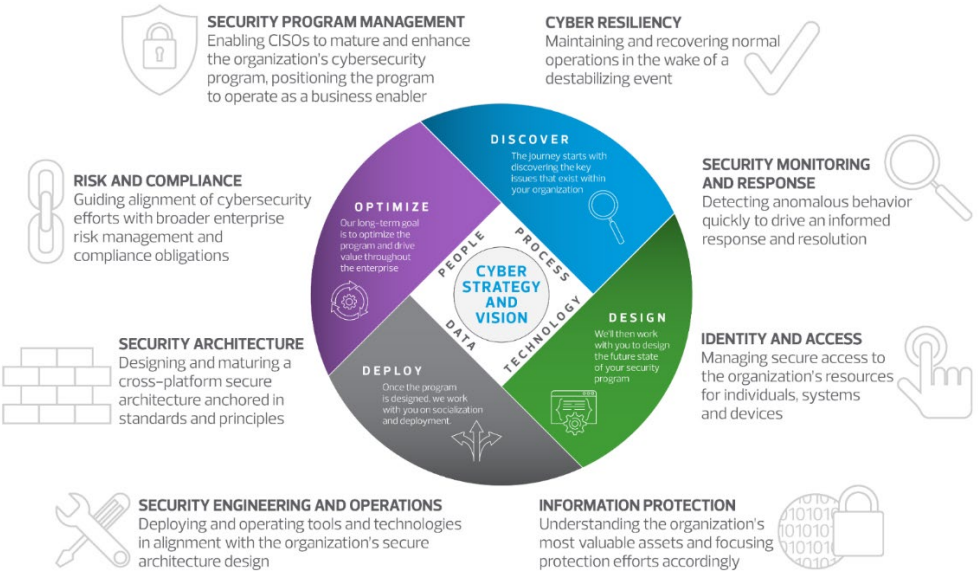
- Provide IT infrastructure support to address critical business or security needs identified while exercising the tasks outlined below.
- Run decryption utility against impacted data files.
- Restore, rebuild or reinstall damaged, impacted or infected servers, workstation and/or networking systems.
- Assist with the reinstallation of third-party software and application on impacted systems.
- Assist with the migration of Active Directory and group policy.
- Restore and/or migrate user-created and/or application data from impacted systems.
- Assist with data and system integrity checks and monitoring.

## Services area G: As-needed supplemental advanced cybersecurity services

**Value-added activities and ideas**

Having significant experience with other state and local governments in similar situations, we can bring additional skills and ideas other than the requested projects A–F. These value-added activities and ideas include bringing our diverse set of professionals to help assist with and complete projects identified as outside of the scope of this RFQ.

- **Management of operational and technical controls.** RSM has dedicated risk consulting practices that focus in control design and assessment. These teams are often supplemented with subject matter experts to help ensure adequately of control design, testing methodology, and results. These hybrid teams can operate within a co-source model with the City or alternatively, operate independently as the City's third line of defense.
- **RSM's eight dimensions for cyber programs.** RSM's Security and Privacy Risk Consulting practice is aligned to and has dedicated teams for each of the eight dimensions outlined below. We serve a full spectrum of clients within state and local government to delivery robust security services spanning all security domains.



## SECTION B: COMPETENCE TO PERFORM THE REQUIRED SERVICES

### RSM overview

RSM's purpose is to deliver the power of being understood to our clients, colleagues and communities through world-class audit, tax and consulting services focused on middle market businesses. The clients we serve are the engine of global commerce and economic growth, and we are focused on developing leading professionals and services to meet their evolving needs in today's changing business environment.

Founded in 1926, today RSM US is the fifth largest accounting, tax and consulting firm in the U.S., as ranked in Accounting Today's 2022 Top 100 Report. RSM US and RSM Canada go to market together and together have 14,700 professionals in 82 cities and six locations in Canada. We are the U.S. member of RSM International, a global network of independent firms with 51,000 people across 120 countries.

We serve clients across several industries and segments, including state, local and federal governments, business and professional services, industrials, consumer products, real estate, life sciences, nonprofit and education, health care, gaming, private clubs and technology, media and telecommunications.

Consulting services, including risk consulting services, accounts for 37% of our revenue. We have been providing cybersecurity services for more than 15 years.

We provide training, mandate personnel involvement and track participation. To maximize the depth of industry knowledge, our personnel select an industry focus, enabling them to share industry and regulatory insights with clients.

### Program manager and anticipated project team

The following professionals have the qualifications and experience to handle cybersecurity task orders resulting from our proposed MSA, and are committed to exceeding the expectations of those agencies.

**Andrew Weidenhamer, CISSP, CISA, QSA**
**State and Local Government Security and Privacy Risk Leader**
**Email: andrew.weidenhamer@rsmus.com** **Education: Ohio University**

**Role**: Relationship lead
I will be responsible for your complete satisfaction with the services we provide. I will serve as your escalation point for any concerns on the delivery of our services.

**Qualifications**

- More than 20 years of consulting expertise within the state and local government sector
- Has led large statewide projects, including NIST CSF assessments, strategic roadmap development and IAM strategy design (workforce and citizen), among other projects
- Has provided thought leadership in all areas of security through presentations at industry recognized conferences such as Defcon, ISACA, IIA and OWASP

**Jennifer Mt Castle, PMP**
**State and Local Government Project Management Office Leader**
**Email: jennifer.mtcastle@rsmus.com** **Education: Towson University**

**Role**: Program manager
I will manage and coordinate the overall program of seven planned projects. I will serve as your primary contact on day-to-day matters, keep you informed about our progress, provide status updates at the cadence you desire, and promptly address your questions and concerns.

**Qualifications**

- Over 15 years project managing large public sector projects, including but not limited to, the below:
  - Security maturity assessments
  - Grant management
  - CARES Act Fund Management
  - ARPA Stimulus Fund Management

**Dietz Ellis, CISSP, GICSP**
**Director, National Enterprise Governance, Risk, and Compliance Leader**
**Email: dietz.ellis@rsmus.com** **Education: University of Georgia**

**Role**: Engagement consulting leader
I will be responsible for overseeing all aspects of the City engagement and will work closely with Andrew, keeping him updated and helping ensure your expectations are being met.

**Qualifications**

- Over 10 years overseeing multiyear GRC transformations for complex risk programs
- Has helped to automate and enabled monitoring of the client's risk management function, including enterprise, IT, and operational risk management
- Experience with the development and implementation of multi-year roadmaps and associated execution of program components
- Oversaw all Office of the CISO (oCISO) services across 25+ clients to provide staff augmentation through fulfilling CISO roles

**Ryan Millerick, CISSP, CIPT**
**Manager, Security and Privacy Risk Consulting**
**Email: ryan.millerick@rsmus.com** **Education: California State University**

**Role**: Engagement manager
I will oversee projects AE and will help ensure successful deployment of the Governance Risk and Compliance project that will enable the City to transform its cybersecurity function.

**Qualifications**

- More than 15 years working on large scale enterprise governance risk and compliance programs
- Provides solutions, such as GRC selection, implementation, and deployment for large enterprise clients

**Ken Smith, OSCP, OSWP, ASIS**
**Director, National Security Testing Leader**
**Email: ken.smith@rsmus.com** **Education: University of Dayton**

**Role**: Cybersecurity technical subject matter expert
I will serve as your primary contact on day-to-day matters for the technical cyber testing workstream, to continuously keep you informed about our progress, perform quality assurance reviews of deliverables, and promptly address your questions and concerns.

**Qualifications**

- Leads a team of over 50 technical security engineers who may be called upon, as needed
- Has led large penetration testing projects for government clients, including the states of Maryland and Florida
- Frequent speaker at industry cybersecurity conferences

**Bobby Mcgahee-Shangvi, SANS GCFE**
**Manager, Data Forensics and Incident Response**
**Email: bobby.mcgahee@rsmus.com** **Education: Florida Atlantic University**

**Role**: Digital forensics and incident response subject matter expert
I will provide subject matter expertise and serve as your primary contact on day-to-day matters for the incident response workstream.

**Qualifications**

- 12+ years consulting across industry sectors, including state and local government
- Has led hundreds of incident response tabletop exercises
- Developed incident response programs and playbooks

**Representative Senior Associate(s) and Associate(s), Security and Privacy Risk**
**Education: BA/BS Degree**

**Role**: Staff Consultant(s)
Our staff consultants will be part of the delivery team executing on the various workstreams provided to the City.

**Qualifications**

- 1–5 years of information security consulting experience with particular focus on performing information security risk assessments
- Has helped to execute a number of PCI-related projects, including report on compliance assessments

## Financial strength and stability

For the most recent fiscal year ended April 30, 2022, RSM reported revenue of $3.3 billion, an increase of 15% in comparison to the prior year. The average of our last three fiscal years of revenue is $2.96 billion.

As of May 1, 2022, RSM US LLP was assigned a low risk viability rating by Dun & Bradstreet (D&B). An independent D&B comprehensive credit report for RSM US LLP (DUNS # 07-348-2424) can be ordered via the D&B website.

## Relevant certifications

### Industry-specific certifications

- Certificate in Executive Protection (ASIS EP)
- Certified Ethical Hacker (CEH)
- Certified in the Governance of Enterprise IT (CGEIT)
- Certified Information Privacy Professional (CIPP)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Information System Security Professional (CISSP)
- Certified Information Technology Professional (CITP)
- Certified Public Accountant (CPA)
- Certified in Risk and Information Systems Control (CRISC)
- Certified TG-3 Auditor (CTGA)
- Common Security Framework Certified (HITRUST CSF)
- Provisional Auditors 27001:2005 (ISO/IEC 27001)
- Offensive Security Certified Professional (OSCP)
- Offensive Security Wireless Professional (OSWP)
- Social Engineering Pentest Professional (SEPP)
- Reverse Engineering Malware (GREM)
- GIAC Security Expert (GSE)
- GIAC Security Essentials (GSEC)

### PCI certifications

- Approved Scanning Vendor (ASV)
- PCI Payment Application (PA)
- Qualified Security Assessor (QSA)

### Global information assurance certifications

- Penetration Tester (GPEN)
- Certified Incident Handler (GCIH)
- Web Application Penetration Tester (GWAPT)
- Certified Intrusion Analyst (GCIA)
- Certified Forensic Analyst (GCFA)

### Privacy

- Certified Information Privacy Manager (CIPM)
- Certified Information Privacy Professional specializing in Government (CIPP/G)
- Certified Information Privacy Professional (CIPP)
- Certified Data Privacy Solutions Engineer (CDPSE)

### Ancillary

- Project Management Professional (PMP)
- Global Industrial Cyber Security Professional (GICSP)

## SECTION C: ABILITY TO PERFORM THE REQUIRED SERVICES

### Program manager availability

RSM will provide a fulltime 40-hour per week program manager to support this engagement, as applicable. As engagements wind down, and in consultation with the City, RSM will reduce the time as applicable.

### Anticipated project team

Dependent on requested level, our project team resources average between 20–40 hours per week. RSM offices are closed during the following 11 holidays: New Year's Eve, New Year's Day, Martin Luther King Jr. Day, Memorial Day, Fourth of July, Labor Day, Thanksgiving Day, Friday after Thanksgiving Day, Christmas Eve and Christmas Day. Given a month of lead-time and confirmation of engagement start date, RSM will provide full availability for each required resource.

### Total personnel of contractor

RSM employs more than 14,700 professionals, dedicated focus in the state and local government sector. The City will benefit from the proposed team's experience and knowledge providing services to numerous state and local government entities.

Below shows the number of professionals, by level, available to pull from to serve the City.

| Professional level | Employee count |
|---|---|
| Managers and administrators | 26 |
| Cybersecurity risk analysts | 46 |
| Cybersecurity project managers | 20 |
| Cybersecurity architects | 10 |
| PCI QSA Qualified Security Assessors (QSAs) | 21 |

**Specialists and subject matter experts**

Our team approach emphasizes assigning professionals with the right level of experience for each aspect of the engagement. Assistance will be sought, as needed, from persons possessing specialized knowledge and expertise relative to the situation. Whether resolution—of any matter—is needed or dialogue with one of our subject matter experts is desired by the City, engagement leader, Andrew Weidenhamer, will coordinate this for you.

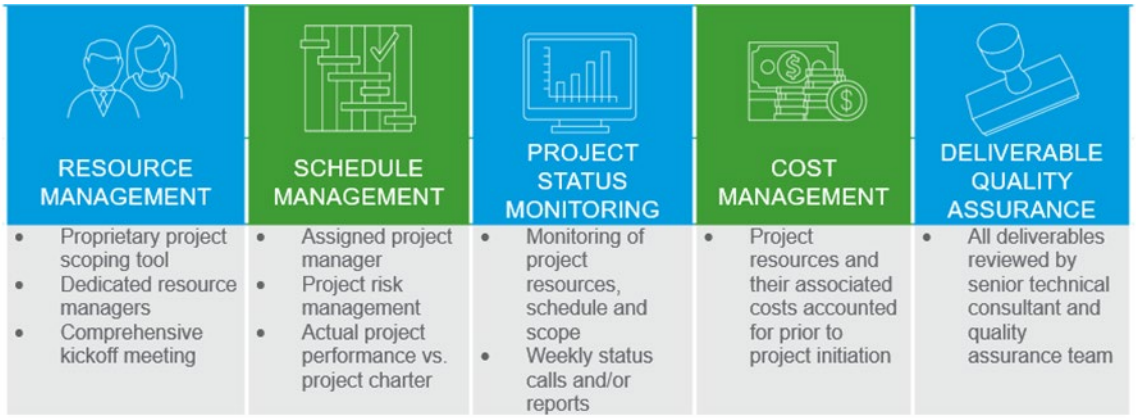
### Project management

For a project to be successful, all of the stakeholders involved must clearly understand why the project is being undertaken, what work product is expected from the project, who is responsible for doing what, how project communications will be handled, when the deliverables must be completed, and which rules govern the entire process.

An essential factor in providing this structure for a project is the methodology used to establish guidelines and control project activities throughout the project's life cycle. By using a proven methodology, the project team can significantly improve communications, planning and

performance from the initial proposal stage through completion of project deliverables to project closure.

Planning and guiding a project using a well-designed, fully featured methodology that is deployed by trained project managers and technical resources greatly enhance the probability that project requirements will be completed on time and as budgeted. Our project management approach is described below.




We will coordinate, communicate and review with City management the engagement schedule, work plans and reports. A kickoff meeting will be conducted to clarify the scope of the engagement to detail the procedures for the performance of the engagement and introduce the RSM engagement team to the environment and staff.

We recognize that City management expects ongoing, straightforward communications—and a high level of involvement by team leadership in all phases of your engagement. Our team will perform weekly and monthly status reporting to the City, so you stay informed throughout the engagement.

In addition to communicating with you frequently throughout the process, we will employ a thorough, centralized project plan to facilitate regular status updates, limit disruptions and control costs. Our customized approach to reporting allows us to provide this centralized project management function across all the key facets of your organization, branching to each of the compliance requirements needed. A no-surprises engagement is our goal.

## Staff turnover

While turnover rates fluctuate from year to year, RSM's employee attrition rates are generally consistent with the industry average. Should the need for team member adjustments arise, your RSM program manager will work closely with you to help ensure that the transition is secure and seamless.

## Use of sub-contractors

We do not currently plan to utilize any subcontractors to perform work associated with this RFQ. If the need arises for local/regional/national project support or other specialized skills or certifications, we will discuss such requirements with you.

## SECTION D: PAST PERFORMANCE

### Relevant work history

| Representative state and local government clients | | |
|---|---|---|
| • State of Maryland<br>• Franklin County<br>• Northeast Ohio Regional Sewer District<br>• Prince William County | • Alachua County<br>• Brevard County<br>• St. Lucie County<br>• City of Sacramento | • Florida Department of Management Services<br>• Maryland State Retirement and Pension System<br>• Amtrak<br>• State Board of Administration of Florida |

### References

We encourage you to contact our references to learn more about us, our team and our process. Contact information for each of our listed references can be provided upon request.

| Name of company/organization | Contact | Work performed |
|---|---|---|
| **State of Maryland Department of Information Technology** | Chip Stewart<br>Chief Information Security Officer | • NIST CSF assessments<br>• Penetration testing<br>• Strategic roadmap development<br>• Agency ISO support |
| **BankUnited** | Kavitha Singh<br>Vice President and Head of Operational Risk | • GRC business requirement identification<br>• GRC product evaluation and scoring |
| **Franklin County, Ohio Job and Family Services** | Juan Torres<br>Chief Information Officer | • Provided RSM HHS Case Management Accelerator to create a case management system |
| **City of Sacramento** | Ignacio Estevez<br>City Manager | • PCI assessment services |

## SECTION E: RATE SHEET

All rates listed below are RSM employee rates. We do not anticipate the use of subcontractors for this engagement.

| Classification title | Typical responsibilities | Minimum education and certifications | Average years of experience | Hourly rate for 1–40 hours* | Hourly rate for 160+ hours* |
|---|---|---|---|---|---|
| Cybersecurity Project Manager | Oversee engagement quality and deliverables | BA/BS degree, PMP | 5+ years | $321 | $315 |
| Senior Cybersecurity Engineers | Perform configurations and review manager and analyst work | BA/BS degree, CISSP | 10+ years | $321 | $315 |
| Senior Cybersecurity Managers | Oversee project direction and review mid-level and analyst work | BA/BS degree, CISSP | 10+ years | $321 | $315 |
| Senior Cybersecurity Analysts | Oversee technical execution and review mid-level and analyst work | BA/BS degree, CISSP, Security+ | 10+ years | $258 | $253 |
| Mid-Level Cybersecurity Analysts | Perform technical execution and review mid-level work | BA/BS degree, Security+ | 4+ years | $206 | $202 |
| Junior Cybersecurity Analysts | Perform technical execution | BA/BS degree | 1 year | $125 | $120 |
| Exploitation Analyst | Perform technical execution and exploitation of systems | BA/BS degree, GPEN, CEH, CompTIA PenTest+ | 3+ years | $258 | $253 |

| Classification title | Typical responsibilities | Minimum education and certifications | Average years of experience | Hourly rate for 1–40 hours* | Hourly rate for 160+ hours* |
|---|---|---|---|---|---|
| Payment Card Industry (PCI)–Data Security Standard (DSS) Qualified Security Assessor (QSA)<br><br>PCI QSA | Perform PCI DSS assessment work | BA/BS degree, PCI QSA | 5+ years | $258 | $253 |

*The primary RSM resources identified for this engagement are located throughout 82 cities, including Columbus, Ohio. Some of our professionals may reside outside of the Columbus, Ohio area. For onsite rates of non-local resources, add 10% to the rates listed above.

## Additional disclaimer

We have reviewed the City of Columbus ("City") Request for Statement of Qualifications ("RFQ") for IT and Cybersecurity Products and Services. If the City selects us based upon our response to the RFP, we would seek to negotiate in good faith general terms and conditions ("Terms and Conditions") expected to be incorporated into a negotiated contract ("Agreement") entered into between RSM and the City. The Terms and Conditions would include terms customary and commensurate with the contemplated nature and complexity of the services requested, including by way of illustration, but not limited to, limitations of liability, exclusion of consequential damages, warranty of services provisions, network security authorization provisions, change order management, etc. We prefer to use our standard contract terms as the basis for such negotiation, since our standard contract is tailored to fit RSM's services and the deliverables we provide. Given our extensive experience in contracting with entities similar to the City, we are confident that we can reach an agreement with you on these issues. Notwithstanding anything to the contrary contained in the RFP or this response thereto, our obligation to perform any services shall follow the execution by both parties of a mutually agreed upon definitive agreement. As part of the selection process, RSM will follow the process to complete and obtain a City of Columbus Contract Compliance Certificate Numbers (CCCN).

**www.rsmus.com**

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party.

For more information, visit rsmus.com/who-we-are for more information regarding RSM US LLP and RSM International.