



# PRINCE WILLIAM COUNTY

---

## Prince William County, Virginia Internal Audit – Proposed Internal Audit Plan Calendar Year Ending December 31, 2023

December 13, 2022



## TABLE OF CONTENTS

Transmittal Letter .....	1
Risk Assessment Methodology.....	2
Internal Audit Continuum and Types of Internal Audits .....	4
Proposed Internal Audit Plan – Working Draft Calendar Year 2023.....	5
Considerations for Future Proposed Internal Audit Plan .....	11
Appendix: Internal Audit Methodology .....	12

## TRANSMITTAL LETTER



December 13, 2022

The Board Audit Committee of  
Prince William County, Virginia  
1 County Complex Court  
Woodridge, Virginia 22192

**RSM US LLP**  
1861 International Drive  
Suite 400  
McLean, VA 22102  
O: 321.751.6200 F: 321.751.1385  
[www.rsmus.com](http://www.rsmus.com)

We hereby submit the proposed internal audit plan for calendar year (“CY”) ending December 31, 2023 for Prince William County, Virginia (“County” / “PWC”), as determined by updating the risk assessment for the County.

We applied a broad-based, business view of risk, linked to the annual budget, operations, and the strategic plan. We conducted interviews with members of the Board of County Supervisors (“BOCS”), the County Executive, Deputy County Executives, Director of Finance/CFO, and Department Directors to gain an understanding of their objectives and identified risks. During the interviews, we discussed and identified areas of high-risk, opportunities and vulnerabilities from their various levels of perspective.

The objective of this risk assessment is to develop a proposed internal audit plan, the purpose of which is to identify those areas determined as having a relatively high-risk profile or that otherwise require internal audit attention for various reasons. The proposed internal audit plan is *on-line real-time* and labeled as *proposed* because it is a *living document*. As factors change and situations arise, the proposed internal audit plan can and will change. As part of this risk assessment, ‘risk’ focuses on financial, strategic, performance/operational, and compliance risk, as well as the general effect of public perception related to County-wide activities and initiatives.

Our risk assessment considers ‘inherent risk’, which is the risk of a function in an environment void of controls. *Therefore, functions with inherently high-risk may be included in the identified proposed internal audit plan; although their inclusion does not mean ‘issues’ or concerns currently exist, but rather that the high-risk nature of the function is such that a higher potential exists for issues to develop.* We have provided a high-level process of each proposed audit function/area, the key potential financial, compliance, and public perception inherent risks, as well as the internal audit strategy for evaluating the effectiveness of the processes, procedures, and controls in place within the function.

We would like to thank the BOCS, the County Executive’s Office, and the various departmental personnel involved in assisting us with developing the proposed internal audit plan.

Respectfully Submitted,

*RSM US LLP*

INTERNAL AUDITORS



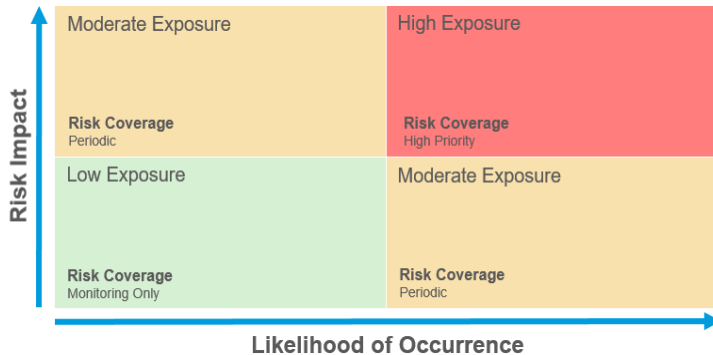
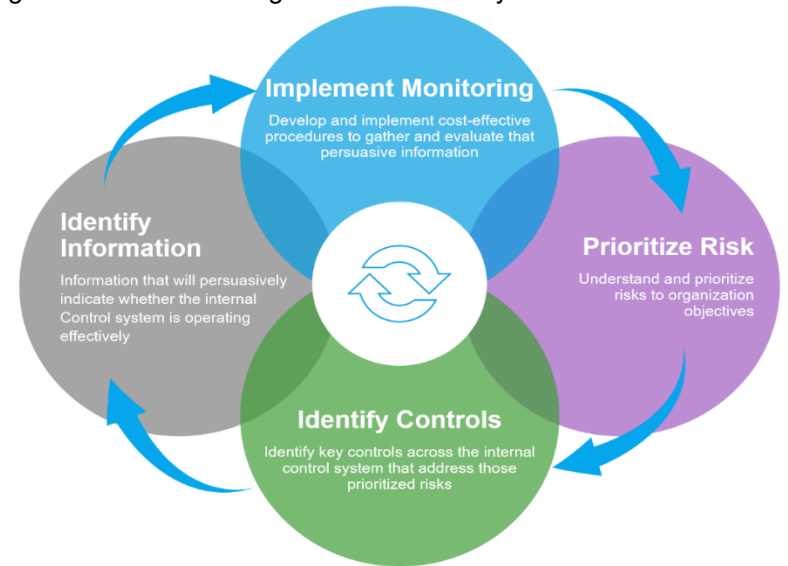
## RISK ASSESSMENT METHODOLOGY

As previously noted, the objective of this risk assessment is to provide the County with a proposed internal audit plan that has coverage of those areas evaluated as having a relatively high-risk profile or that otherwise require internal audit attention for various reasons.

Our approach is based on the widely accepted Committee of Sponsoring Organizations (“COSO”) guidance on monitoring Internal Control Systems as shown below:

Preparing the proposed internal audit plan from the risk assessment will facilitate that resources are focused on areas, which are currently of most immediate concern to the County. Our risk assessment considers ‘inherent risk’, which is the risk of a function in an environment void of controls. Therefore, functions with inherently high-risk may be included in the proposed internal audit plan; although their inclusion does not mean ‘issues’ or concerns currently exist, but rather that the high-risk nature of the function is such that a higher potential exists for issues to develop. This proposed internal audit plan is *on-line real-time* and will be consistently presented in *draft* form because it is a *living document*. As factors change and situations arise, this proposed internal audit plan can and will change.

The chart below illustrates the exposure environment for positioning the County’s risks and evaluating the desired response based upon the likelihood of occurrence and priority of risk concerns. The proposed internal audit plan generally focuses on areas or functions that are high exposure and high priority (the upper right quadrant). We also consider other areas that are not included in this quadrant to insert a level of unpredictability into the proposed internal audit plan and risk assessment process in order facilitate County-wide awareness that all business units, functions, and processes may be subject to an internal audit at any time.



### Inherent Risk

- Risk of an occurrence before the effect of any existing controls.
- If you were building this process, what would you be concerned about?
- What can we not prevent?

### Residual Risk

- Risk remaining after the application of controls.
- Potentially reduced impact or likelihood.

Our risk assessment was conducted utilizing a broad-based business view of risk. We conducted interviews with members of the BOCS to gain an understanding of their perspective of risk, focusing on their objectives in order to identify potential risks. We also conducted interviews with the County Executive, Deputy County Executives, Director of Finance/CFO, and other personnel within the County to identify risks, vulnerabilities, and potential opportunities. Meeting with various levels within the County gave us insight and understanding of potential risk from their various levels of perspective. In addition, we reviewed the adopted budget for fiscal year 2023, the fiscal year 2023-2028 capital improvement plan, the strategic plan, as well as media coverage and BOCS meeting agendas, minutes, and other available documentation.



## RISK ASSESSMENT METHODOLOGY (CONTINUED)

The risk assessment process drives the planned scope of the internal audit function and forms the basis of the proposed internal audit plan. Our approach primarily defines 'Risk' in a government entity as Financial and Compliance-related risk, as well as Public Perception risk. Strategic, performance and operational risks are also considered. We evaluate the level of risk present in each area / function, across a standard spectrum of industry-accepted risk categories as follows:

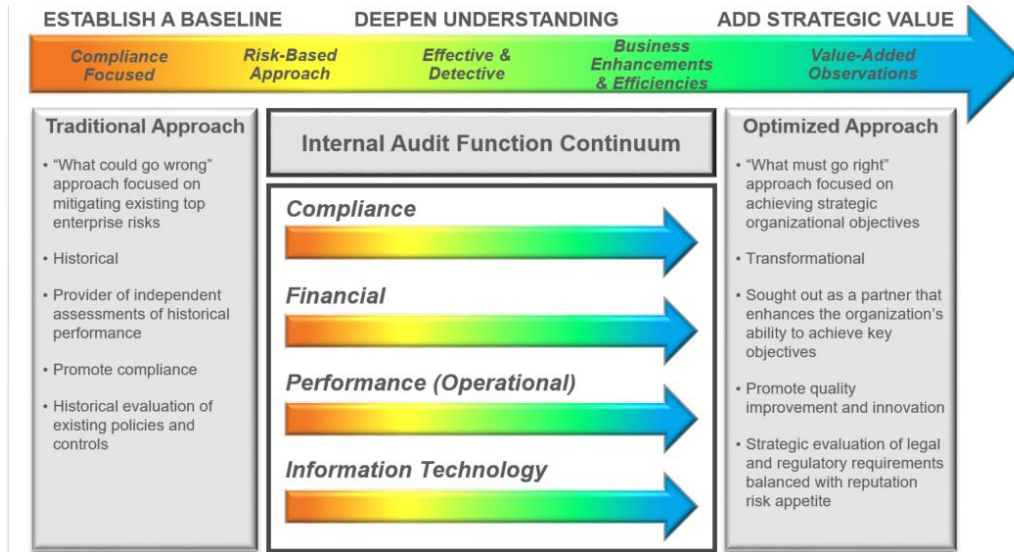
Control Environment	<ul style="list-style-type: none"> <li>• Demonstrates commitment to integrity and ethical values</li> <li>• Exercises oversight responsibilities</li> <li>• Establishes structure, authority and responsibility</li> <li>• Demonstrates commitment to competence</li> <li>• Enforces accountability</li> </ul>
Risk Assessment	<ul style="list-style-type: none"> <li>• Specifies suitable objectives</li> <li>• Identifies and analyzes risk</li> <li>• Assesses fraud risk</li> <li>• Identifies and analyzes significant change</li> </ul>
Control Activities	<ul style="list-style-type: none"> <li>• Selects and develops control activities</li> <li>• Selects and develops general controls over technology</li> <li>• Deploys through policies and procedures</li> </ul>
Information & Communication	<ul style="list-style-type: none"> <li>• Uses relevant information</li> <li>• Communicates internally</li> <li>• Communicates externally</li> </ul>
Monitoring	<ul style="list-style-type: none"> <li>• Conducts ongoing and/or separate evaluations</li> <li>• Evaluates and communicates deficiencies</li> </ul>

As shown on the following pages, a strong, high-functioning internal audit process has a balance of all types of internal audits and reviews. As such, the proposed internal audit plan includes Overall Audit Functions, Cycle Audits, Entity-Wide Audits, Individual Function Audits and Special Requests. The proposed plan may also include performance and / or consultative-type projects that assist management with strategy, ongoing initiatives, and planning. We have presented a snapshot of the proposed internal audit plan working draft separately, as well as a summary of the planned audit strategy for each audit, subject to modification during the initial planning stages of each audit and subsequent discussions with management.

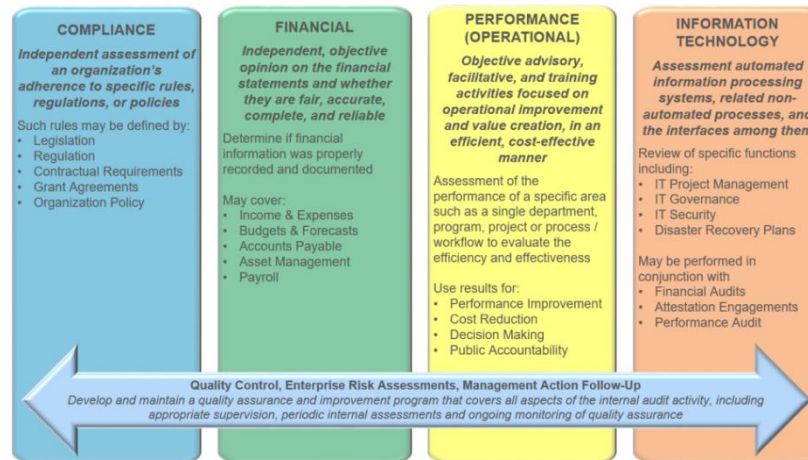


## INTERNAL AUDIT CONTINUUM AND TYPES OF INTERNAL AUDITS

As an internal audit function develops and matures, the various types of audits performed will move through a lifecycle of the control environment in order to not only strengthen and enhance processes and controls, but also to facilitate strategy, decision-making and long-term planning.



The various types of audits that are proposed should include a hybrid mix of audit types, as shown below.





## CALENDAR YEAR ENDED DECEMBER 31, 2023 INTERNAL AUDIT PLAN – WORKING DRAFT

As the County's Internal Auditors, we have developed an internal audit methodology aligned with Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and AICPA consulting standards. These include systematic audits selected through the risk assessment, ad hoc audits as new facts emerge, or requests by the BOCS or County Executive.

### Overall Audit Functions

#### **Risk Assessment and Audit Plan Development**

As required by the RSM Internal Audit Methodology, the internal auditor uses risk assessment techniques in developing the internal audit plan and determining priorities for allocating internal audit resources. The Risk Assessment is used to examine auditable units and select areas for review to include in the internal audit plan that have the greatest risk exposure.

#### **Update Risk Assessment and Audit Plan Development**

Risk is not stagnant. It is constantly evolving. As factors change and situations arise, this plan can and will change. As required by the RSM Internal Audit Methodology, the risk assessment and proposed audit plan is required to be updated annually.

#### **Fraud, Waste, and Abuse Hotline Monitoring**

RSM is responsible for monitoring the County's Fraud, Waste, and Abuse hotline. We intake all notifications received, and triage as deemed necessary. Activity is reported to the Board Audit Committee of Prince William County at each meeting.

#### **Follow-up Procedures**

As required by the RSM Internal Audit Methodology, internal auditors should establish a follow-up process to ensure that management actions have been effectively implemented or that Management has accepted the risk of not taking action. Included within each report provided, for each audit completed, a Management Response section will be added for Management to respond and include an action plan for remediation (if needed), as well as a targeted date of completion. Follow-up procedures will be performed after the completion date noted by Management. Follow-up typically occurs after ample time has passed with the new control / procedure in place (generally six months) to verify and report the implementation status of the recommendations and Management's action related to the previously reported findings. Annually, we perform procedures for those issues where the target dates have been reached to verify and report the implementation status of recommendations to the previously reported findings. Follow-up reports will be presented to the Audit Committee periodically through-out the calendar year.



#### **Quality Control**

The RSM Internal Audit Methodology requires the internal auditors to maintain a quality assurance and improvement program that covers all aspects of the internal audit activity, including appropriate supervision, periodic internal assessments, and ongoing monitoring of quality assurance. RSM's Quality Control processes specific to public sector clients include, when applicable, concurring partner review (independent of the engagement) and, when necessary, consultation with the County's Attorney prior to reports being issued into the public record.



## PROPOSED INTERNAL AUDIT PLAN – WORKING DRAFT (CONTINUED)

The objective of this assessment is to identify those areas judged as having a relatively high-risk profile or that otherwise require internal audit attention for various reasons. Through the risk assessment, we have identified and propose the following functions to be reviewed during CY 2023. In addition, we have identified proposed audit areas for possible inclusion in future internal audit plans. The below proposed subject areas are in no particular order.

### ***General Controls for Information Technology***

The County leverages a variety of technology platforms and applications to support County operations. Widespread use of technology carries with it several inherent risks that, if realized, could have dire consequences on the County's ability to execute its day-to-day operations. In recent years, the County has implemented multiple systems and increased reliance on third-party service providers including Microsoft Azure, Amazon, Oracle, and AWS. These new systems and partnerships provide various improvements but also introduce new IT risks.

Inherent risks may include: Unauthorized or inappropriate access to County system resources and data; Inappropriate or unintended changes to critical systems and applications; Inadequate backups and availability of critical data and systems; and Theft of technology assets.

#### **Internal Audit Strategy:**

The purpose of the internal audit will be to assess whether the system of internal controls is adequate to address key areas of information technology risk, including logical and physical access, systems development life cycle, change management, and backup and recovery of data, and automated job scheduling and processing. Audit procedures may include inspection of policies and procedures, testing the design and operating effectiveness of internal controls covering the aforementioned risks, and provision of recommendations to enhance the efficiency or effectiveness of IT general controls.

### ***Physical Security***

All organizations face some degree of physical threat, whether from crime, natural disasters, technological incidents, or human error. Physical security is the protection of people, property, and physical assets from actions and events that could cause damage or loss. A physical security assessment is the most foundational and effective review of an organization's security program.

The County utilizes a myriad of facilities for ongoing operations and citizen services. Managing access to, and the security of, County buildings is critical to protecting employees, citizens, and assets. Management of County security is currently partially decentralized with different responsibilities distributed among multiple departments, including Facilities and Fleet Management, DoIT, and Finance. There is no singular position or department responsible for the creation, maintenance, or implementation of the overall physical and virtual security policy.

Inherent risks may include: Unauthorized or inappropriate access to facilities; Safety incidents; Theft or destruction of property and assets; Theft or destruction of records or personal/personnel information and Various other threat actors.

#### **Internal Audit Strategy:**

The purpose of the internal audit will be to perform a holistic review of the overall physical security of the County's buildings, facilities, and locations. We will evaluate the physical security controls in place at locations that are in scope. For example, our staff evaluates access control systems, security guards, closed-circuit television (CCTV) cameras, access badges, locks, security lighting, fences and more. The physical security assessment is a noninvasive walk-through assessment that is guided by the client's security personnel while on-site. Our approach follows industry-accepted testing methodologies and are largely adapted from ASIS International guidelines and standards.





## PROPOSED INTERNAL AUDIT PLAN – WORKING DRAFT (CONTINUED)

### ***Cyber Security and Privacy – Penetration Testing***

Cybersecurity is a priority within the public sector. We have periodically performed network scanning and deeper targeted penetration testing since 2015. Threats are constantly changing and evolving, thus inherently high-risk. Organizations like the County are under constant attack from external attackers. The prospect of finding that an attacker has penetrated the organization's defenses and is able to steal data from the organization's network keeps most leaders up at night. As threats to data and systems have evolved, so have the requirements for safeguarding user and County information. The processes and people that support the security of technology are the key components in protecting these valuable business assets. Given the work-from-home environment due to the COVID-19 pandemic, it is imperative to constantly measure the security of technology assets to understand the ability to defend against threats.

Inherent risks may include: Undetected threats and attacks to County systems; Loss or manipulation of critical data; Systems and applications are not configured appropriately to support proper maintenance and monitoring (closed-loop feedback); County data not being stored securely; and Time and resources may be inefficiently spent manually analyzing threats to County systems.

#### **Internal Audit Strategy:**

The objective of *internal* penetration testing is to assess current security controls to determine the actionable impact of an attacker gaining access to the internal network. The objective of *external* penetration testing is to assess current security controls to determine the actionable impact of 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; rather, the focus is to validate the organization's security posture and configuration standards by assessing the resiliency of the internal network against a determined attacker. This level of testing relies heavily on 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.

### ***Contract Compliance Reviews***

Contract compliance encompasses all contractual agreements including, but not limited to, vendor and contractor agreements. Although certain aspects of the Purchasing Function are centralized within the Purchasing Division within the Department of Finance, many of the high-risk areas like contract administration and monitoring are decentralized to the individual departments/agencies.

Inherent risks may include: Compromised transparency and accountability; Inappropriate spending due to non-compliance with the contract; Damaged public perception of the County and vendors; Conflicts of interest; Unidentified non-compliance with contract provisions; and Inadequate documentation and audit trail of projects and vendor history.

#### **Internal Audit Strategy:**

The purpose of the internal audit will be to assess whether the system of internal controls is adequate and appropriate, at the department/agency level, for promoting and encouraging the achievement of management's objectives for effective contract monitoring and administration. The focus of this contract compliance audit will be on contracts owned by departments determined to be in scope and will be expanded to include additional aspects such as fee optimization. The selection of departments/agencies and contracts to be tested during this audit will be based upon existing circumstances and conditions at the time and the results of applicable previous audits. As such, the selection will occur closer to the time of the audit.



## PROPOSED INTERNAL AUDIT PLAN – WORKING DRAFT (CONTINUED)

### ***Data Governance and Protection***

Data governance consists of the execution and enforcement of authority over the management of data and data-related assets. It is a continuous practice that permeates throughout the entire entity, rather than ownership being solely to Department of Information Technology (“DoIT”). Once implemented, it becomes a standard operating procedure which produces strong and reliable output, efficiency, and communication across the County. Data governance enables data to be used as a strategic asset, and assists decision-makers define goals, objectives, and focus areas. Privacy concerns are inherently high-risk wherever sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. As laws and regulations surrounding data protection are constantly changing, it is critical to keep abreast of any changes in laws/regulations and continually reassess compliance with data privacy and security regulations.

Inherent risks may include: Outdated, inadequate or undocumented policies, and procedures; Inadequate controls to detect fraud, waste and abuse; Inadequate segregation of duties; Inappropriate handling of data due to non-compliance with applicable standards; Non-compliance and inconsistencies with policies and procedures; and Failure to meet privacy concerns of stakeholders.

#### **Internal Audit Strategy:**

The purpose of the internal audit will be to assess and identify any areas of risk associated with protection of sensitive data that could cause harm to the County. We will perform additional procedures on-site as deemed necessary to appropriately assess the operations and control environment.

### ***Procurement***

The County’s Purchasing Division within the Finance Department (“Purchasing Division”), is the central division responsible for managing the acquisition process for all materials and services. The procure-to-pay process involves a number of sequential stages, ranging from need identification and vendor procurement, including RFP solicitation compliance, to financial system profiles and invoice payment. Steps in a procure-to-pay process need to be executed in a strict order to effectively mitigate associated risks and comply with County and State regulations.

Inherent Risks may include: An Inadequate system of controls to mitigate the procurement risk within an acceptable level; Inadequate process(es) in place to monitor and reevaluate the adherence of existing vendors in the system to County policies; Non-existent consideration of potential or current vendors’ SOC reporting compliance; Ineffective policies and procedures surrounding procurement processes and vendor payments; Ineffective inventory/service need monitoring Inadequate purchasing limits; Duplicate payments of vendor invoices are not monitored; Inadequate controls or segregation of duties for approving, furnishing and reconciling vendor payments; and Reconciliation of invoices is not being performed timely.

#### **Internal Audit Strategy:**

The purpose of the internal audit will be designed to assess whether the system of internal controls is adequate and appropriate, at the department (or division) level, for promoting and encouraging the achievement of management’s objectives in the categories of compliance with applicable laws, administrative rules, and other guidelines as it relates to each step within the procure to pay business process. This audit will focus on compliance with certain purchasing aspects, management and administration of vendors, procurement of goods/services, and remittance. It will include the selection of certain high-risk vendors and/or contracts.



## PROPOSED INTERNAL AUDIT PLAN – WORKING DRAFT (CONTINUED)

### ***Accounts Payable***

The Accounts Payable function's main responsibility is to process and review transactions between the County and third parties and to make sure that all outstanding invoices are approved, processed, and paid. Processing an invoice includes recording important data from the invoice and inputting it into the company's financial system. After this is accomplished, the invoices must go through the company's respective business process to be paid. Accounts payable main objective is to ensure the County pays only legitimate and accurate invoices.

Inherent risks may include: Payment made to an incorrect or unapproved vendor; Payment made for goods or services that have not been procured; Duplicate or inaccurate payment; Inadequate segregation of duties and user access controls; Outdated, inadequate or undocumented policies, and procedures; Non-compliance and inconsistencies with policies and procedures and Inefficient monitoring process for account standings, past due balances, discounts offered, etc.

#### **Internal Audit Strategy:**

The purpose of the internal audit will be to assess whether the system of internal controls is adequate and appropriate to mitigate financial and operational risks posed by the accounts payable processes. Audit procedures may include review of controls, policies and procedures, detailed testing of payment processing, assessment of accounts payable monitoring procedures, and recommendations for process improvement opportunities. We will perform additional procedures as deemed necessary to appropriately assess the operations and control environment.

### ***Tax Administration – Segregation of Duties***

The County's Tax Administration Division within the Finance Department ("Tax Administration Division") is responsible for collecting the majority of the County's revenue. Adequate segregation of duties within control processes is critical for the County to effectively safeguard and administer taxpayer funding. Tax Administration Division operations include complexities due to various teams and individuals that are responsible for a myriad of tax types and different collection processes. The Division has experienced multiple managerial changes since 2020. During 2020, Internal Audit performed limited scope procedures within the Tax Administration Division as part of the Cash Handling internal audit report accepted on July 20, 2020. As a result, during 2021, Internal Audit performed subsequent procedures related to customer services processes as part of the Tax Administration Division internal audit report accepted on April 1, 2022. Internal Audit has not performed a complete segregation of duties review as part of prior procedures performed.

Inherent risks may include: Inadequate controls to detect fraud, waste and abuse; Inadequate segregation of duties; Outdated, inadequate or undocumented policies, and procedures; Non-compliance and inconsistencies with policies and procedures; Errors or misappropriations; and Inconsistency in cash collection and handling processes.

#### **Internal Audit Strategy:**

The purpose of the internal audit will be to conduct a review of the segregation of duties in place surrounding the numerous taxpayer processes. Audit procedures may include a review of controls, policies and procedures, and detailed testing of related processes. We will perform additional procedures as deemed necessary to appropriately assess the operations and control environment.



## PROPOSED INTERNAL AUDIT PLAN – WORKING DRAFT (CONTINUED)

### ***TO BE DETERMINED AUDIT AREA***

As previously discussed, this proposed internal audit plan is *on-line real time* and will be consistently presented in *draft* form because it is a *living document*. As factors change and situations arise, this proposed internal audit plan can and will change. There is a placeholder in the current proposed internal audit plan for a project 'to be determined' to allow for future coverage.



## PROPOSED PROJECT OUTSIDE OF INTERNAL AUDIT PLAN – WORKING DRAFT (CONTINUED)

### ***ARPA Monitoring***

Signed into law on March 11, 2021, The American Rescue Plan Act of 2021 (“ARPA”) provides \$350 billion in additional funding for state and local governments. The local funding portion is approximately \$130 billion, equally divided between cities and counties. Localities will receive the funds in two tranches—the first after the U.S. Treasury certifies the proceeds to each jurisdiction and the second one year later. For counties, the \$65 billion will be allocated based on the County’s population. ARPA specifies several eligible uses and restrictions for the funds that each recipient must comply with, including that funding must be spent prior to December 31, 2024. As with previous COVID-19 relief packages, implementation will be an extensive process as new or updated guidance is developed and released by the U.S. Treasury.

Inherent risks may include: Loss of funding due to failure to adequately monitor the disposition of received funds, including subrecipient spending; Failure to adhere to federal ARPA program requirements; Failure to adhere to internal policies and procedures; Insufficient internal reporting and/or documentation processing for ARPA procedures; Inappropriate expenditure of ARPA funding received.

### **Internal Audit Strategy:**

The primary objective of this internal audit will be to perform monitoring of the application process, reporting requirements, and adherence to any regulatory guidelines, policies and procedures governing the use of ARPA funds received by the County. Audit procedures may include review and assessment of the expenditure of ARPA funds received by the County, including funds spent directly by the County, as well as funds provided to subrecipients.

Note: ARPA funding includes an allowance for administrative costs, such as monitoring. This project will be funded within the allowable costs per ARPA, and not part of the annual internal audit budget allocation.

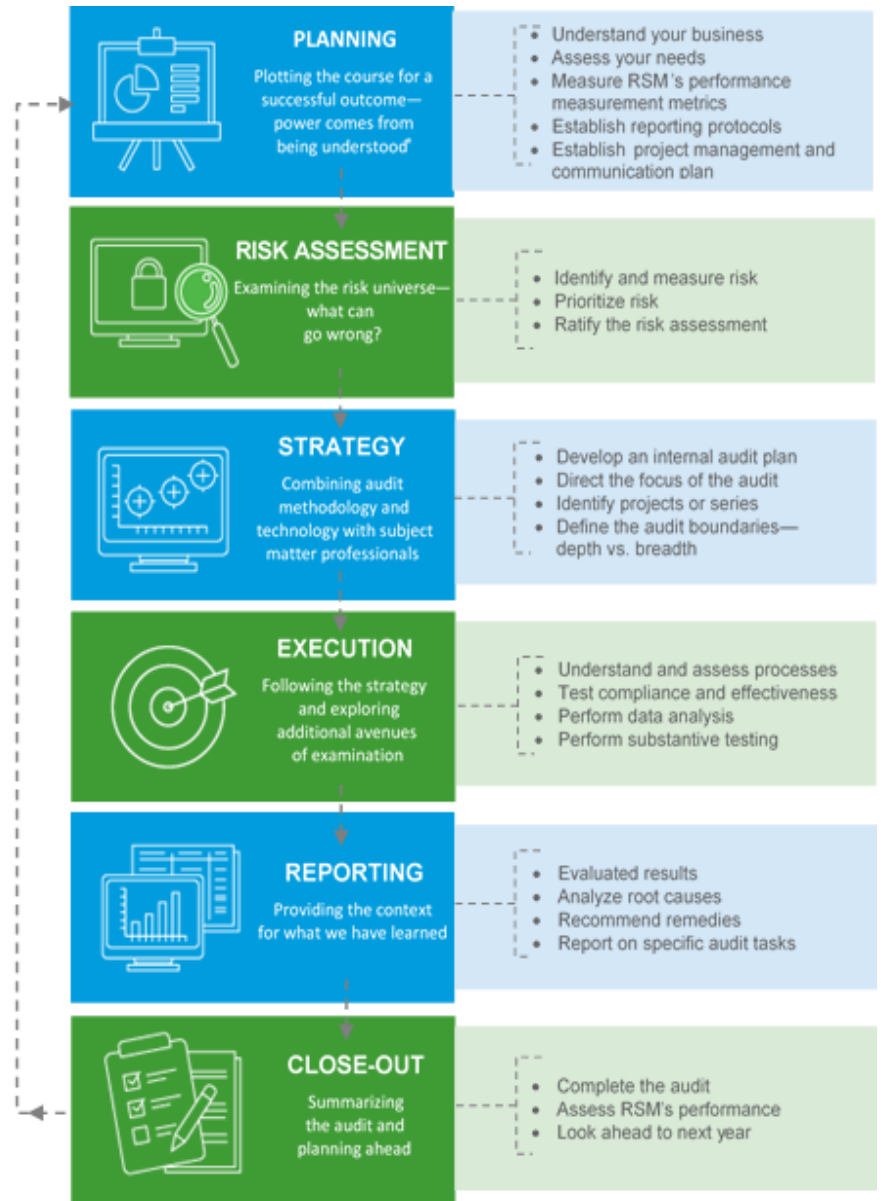



## APPENDIX: INTERNAL AUDIT METHODOLOGY

A strong, high-functioning internal audit process has a balance of all types of internal audits and reviews. These should include systematic audits selected through the risk assessment process and ad hoc audits as new facts emerge, or by request from the BOCS or the County Executive.

RSM has a comprehensive internal audit methodology with a holistic approach to assessing the County's most critical risks. There is no one-size-fits-all internal audit project; therefore, we have a flexible methodology that helps internal audit evolve from a necessary process to assume a more strategic role within the County. A high-level overview is included in the matrix below.

We leverage proven processes and advanced technology to help mitigate risk, monitor compliance, and add value to the County. Our methodology is grounded in understanding the County's needs and working with the County to develop a responsive approach to meet and exceed those expectations. In addition, we integrate quality assurance and project management resources to increase visibility into internal audit projects, providing real-time results and insight into progress.





RSM US LLP  
1861 International Dr.  
Suite 400  
McLean, Virginia 22102  
321 751 6200  
[www.rsmus.com](http://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/aboutus](http://rsmus.com/aboutus) for more information regarding RSM US LLP and RSM International.

© 2022 RSM US LLP. All Rights Reserved.

