



PRINCE WILLIAM COUNTY

Prince William County, Virginia Internal Audit – Proposed Internal Audit Plan Calendar Year Ending December 31, 2022

January 18, 2022



PRINCE WILLIAM COUNTY

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 2022.....	5
Appendix: Internal Audit Methodology	10

TRANSMITTAL LETTER



January 18, 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

We hereby submit the proposed internal audit plan for calendar year (“CY”) ending December 31, 2022 for Prince William County, Virginia (“County” / “PWC”), as determined by updating the risk assessment for the County. We will be presenting proposed internal audit plan for CY 2022 to the Board Audit Committee of Prince William County at the scheduled meeting on January 18, 2022.

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, and Director of Finance/CFO 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 AUDIT



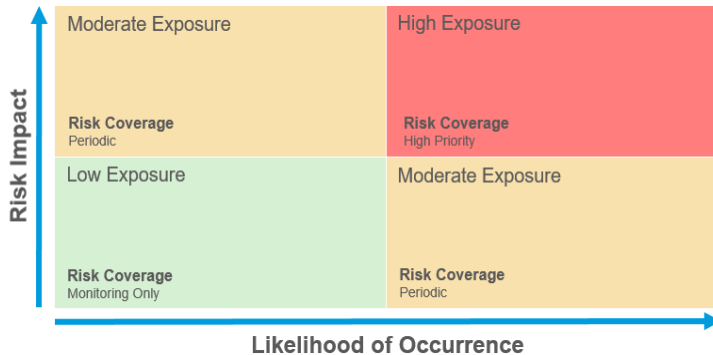
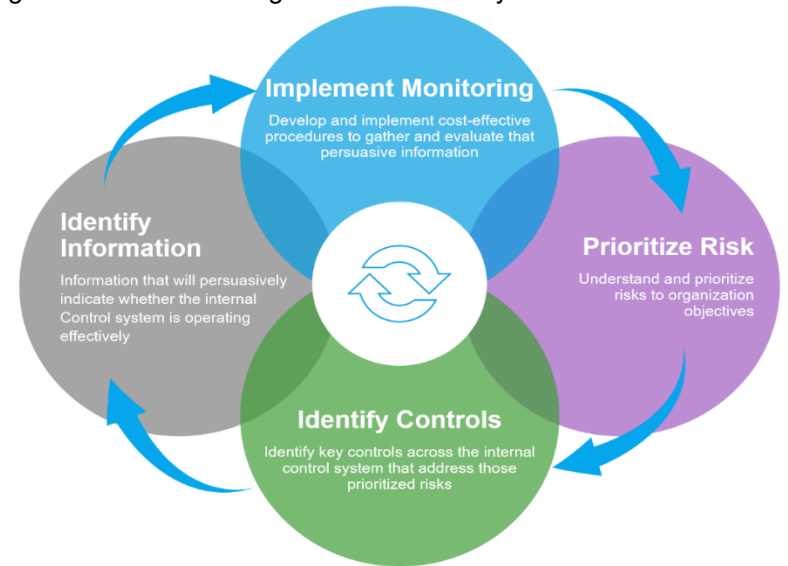
RISK ASSESSMENT METHODOLOGY

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 2022, the fiscal year 2022-2027 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:

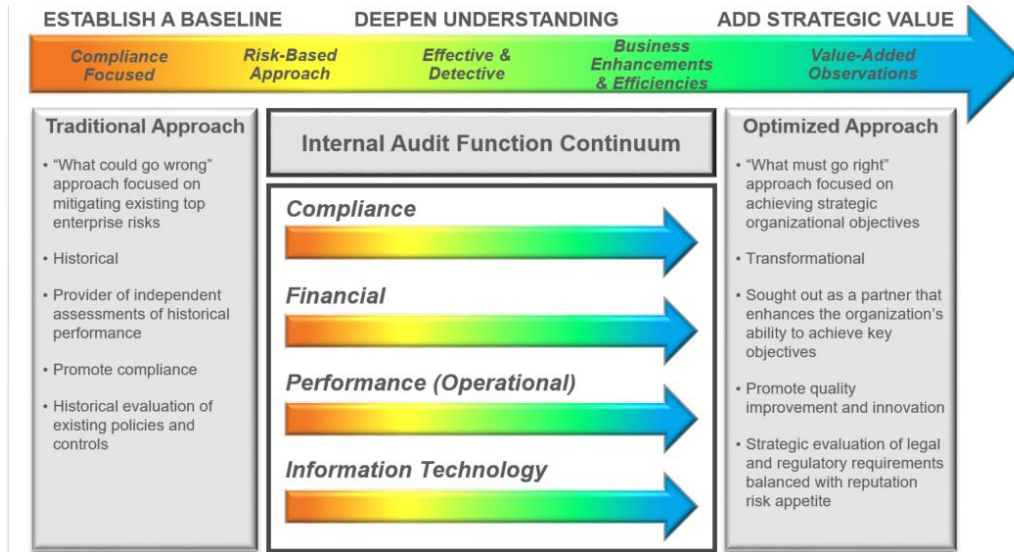
Control Environment	<ul style="list-style-type: none">• Demonstrates commitment to integrity and ethical values• Exercises oversight responsibilities• Establishes structure, authority and responsibility• Demonstrates commitment to competence• Enforces accountability
Risk Assessment	<ul style="list-style-type: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

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.

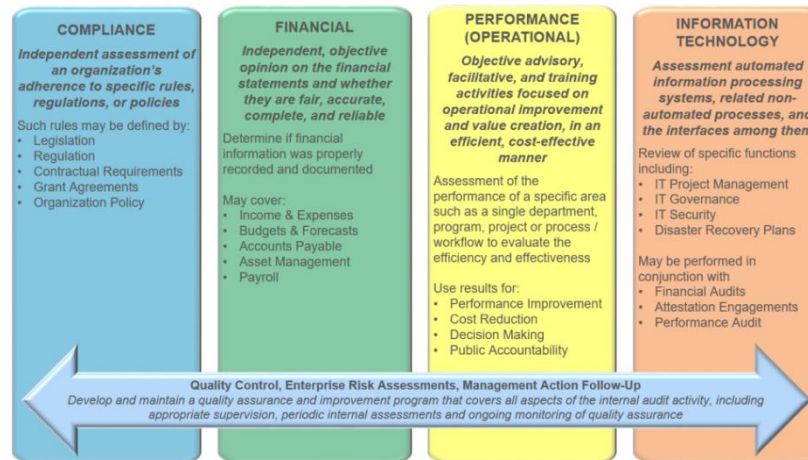


INTERNAL AUDIT CONTINUUM AND TYPES OF INTERNAL AUDITS

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, 2022 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.

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 be reviewed during CY 2022. The below proposed subject areas are in no order.

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 County was allocated ~\$91M of Coronavirus State & Local Fiscal Recovery Funds (“CSLFRF”) by the U.S. Treasury. ARPA specifies several eligible uses and restrictions for the funds that each recipient must comply with, including that funding must be incurred (obligated) by December 31, 2024, but expended by December 31, 2026. 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.

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 is not being stored securely; and Time and resources may be inefficiently spent manually analyzing threats to County systems.

Strategy: The objective of *internal* penetration testing is to assess current security controls to determine the actionable impact from 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 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; rather, the focus is to validate the organization’s security posture and configuration standards through 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.



PROPOSED INTERNAL AUDIT PLAN – WORKING DRAFT (CONTINUED)

General Government Service Level Assessment

As with all government organizations, the County has a fundamental responsibility to be effective stewards of taxpayer money. The County has exercised restraint in allowing for an increase in the number of internal administrative/support personnel, even as the size of the County, the amount of revenues collected, and the number of resultant activities, processes, and procedures has increased. It is an appropriate goal to focus funding on expenditures that promote the continued growth and prosperity of the County, and the well-being of its residents, however, failing to maintain an appropriate level of staffing can have the opposite effect and can reduce the County's ability to effectively execute its mission and objectives.

Inherent risks may include: Loss of revenue through an inability to properly oversee the calculation and collection of County revenues; Misappropriation of assets when personnel are not available to appropriately monitor County vendors and the execution of contractor agreements; Ineffective operation of internal controls that could be skipped or bypassed to expedite the completion of key processes by personnel who may feel rushed or overwhelmed; Reduced services provided to County residents; and Decreased satisfaction from County residents as personnel are not able to complete their responsibilities timely as a result of increased workloads and decreased support.

Strategy: In the County's efforts to streamline general government operations while maintaining appropriate service levels in an increasingly challenging economic environment, the objective of this assessment will be to identify opportunities for improvement to the general government organization and staffing. The assessment will include comparisons with other jurisdictions. We will perform additional procedures on-site as deemed necessary a part of this assessment.

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.

Strategy: The purpose of this 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.



PROPOSED INTERNAL AUDIT PLAN – WORKING DRAFT (CONTINUED)

GASB 96 SUBSCRIPTION-BASED INFORMATION TECHNOLOGY ARRANGEMENTS

In May of 2020, the Governmental Accounting Standards Board (“GASB”) issued Statement No. 96, Subscription-Based Information Technology Arrangements (“SBITA”), which will be effective for fiscal years beginning after June 15, 2022. GASB 96 provides guidance on the accounting and financial reporting for SBITAs for government end users. A SBITA is defined as a contract that conveys control of the right to use another party’s (a SBITA vendor’s) information technology (IT) software, alone or in combination with tangible capital assets (the underlying IT assets), as specified in the contract period for a period of time in an exchange or exchange-like transaction. The two major components of the statement are the subscription asset, and the subscription liability. GASB 96 will have a huge impact on government-related entities.

Inherent risks may include: Inability to appropriately identify all related arrangements; Records are inaccurate or incomplete; SBITAs are not adequately tracked and properly recorded; Failure to adhere to requirements of the standard; Inefficient or inadequate internal compliance monitoring procedures.

Strategy: The purpose of this project will be to provide the County with technical assistances with the implementation of GASB 96.

CONTRACT ADMINISTRATION

Contract administration encompasses all contractual agreements. It includes those activities performed from the time a contract has been executed until the work has been completed and accepted, payment has been made, and disputes have been resolved. Although certain aspects of the procurement function are centralized within Procurement Services, many of the high-risk areas, such as, contract monitoring are decentralized to the individual departments/contract owners.

Inherent risks may include: Outdated, inadequate or undocumented policies, and procedures; Inadequate controls to detect fraud, waste and abuse; Inadequate segregation of duties; Non-compliance/improprieties with Code of Virginia and County policies for solicitation and procurement; Unreported conflicts of interest; Vendor favoritism; Non-performance of vendors; Inappropriate spending due to non-compliance with contract terms; Non-compliance and inconsistencies with policies and procedures; and Failure to meet select contract provisions.

Strategy: The purpose of this internal audit will be to assess whether the system of internal controls over contract administration is adequate and appropriate for promoting and encouraging the achievement of management’s objectives for effective contract monitoring and administration. The scope of our work will include the following: Contract execution; Contract administration process analysis; Vendor monitoring procedures; Analysis of high-risk areas for existing contracts; and Testing of compliance and internal controls.



PROPOSED INTERNAL AUDIT PLAN – WORKING DRAFT (CONTINUED)

PUBLIC SAFETY COMMUNICATIONS SERVICE REVIEW AND STAFFING LEVELS

The office of Public Safety Communications (“PSC”) is responsible for managing the flow of information for the County’s public safety agencies for both 9-1-1 emergency and non-emergency situations. PSC employees are telecommunicators who receive, and process calls using secured Computer Aided Dispatch terminals to enter, clear, and modify confidential data in the Virginia Criminal Information Network and the National Crime Information Center, and answer multi-lined phone systems to assist police officers and other jurisdictions with various law enforcement, fire, and emergency rescue tasks. They are all required to be certified as Emergency Medical Dispatchers – a certification that must be renewed every two years.

Inherent risks may include: Undocumented or outdated business continuity plan in the event of a network failure; Inadequate system of controls in place to protect confidential data; Inadequate process for monitoring the issuance of employee licensures and certifications, re-certifications, and expirations; Improperly trained employees; Inefficient use of County resources due to under- or overstaffing of personnel during a shift; and Failure to meet established performance metrics that could adversely impact emergency response.

Strategy: The purpose of this internal audit will be to assess the appropriateness of current staffing levels in the PSC, proportionate to the volume and length of calls received during each of the three shift schedules. The audit will also include an examination of the documented policies, procedures, and related system of controls surrounding employee training and certification, consumer data protection, and business continuity plans.

Insurance Coverage

The County maintains insurance coverages to protect against the risk of financial loss due to different types of adverse events that could occur, related to categories such as property damage, the operation of County vehicles, injury to persons, and data breaches. An insurance coverage review provides insight to the County’s current exposure and coverage surrounding its own operations.

Inherent risks may include: Unforeseen exposure in a specific business unit or department without coverage, or with deficient coverage; Overlapping coverage; Overpaying premiums; and Inadequate controls to detect contractor non-compliance with insurance requirements.

Strategy: The purpose of this assessment will be to understand the current internal and third-party insurance coverage options, compared to the existing insurance coverages of the County. The assessment will include determining if there is possible overlap of coverage between policies and to identify possible coverage gaps.

Note: this assessment would be specific to liability/indemnification insurance coverages and would not include Health and Workers Compensation insurance. In addition, we will not provide any coverage recommendations, and the assessment will not include a review for insurance premium overpayment.

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.

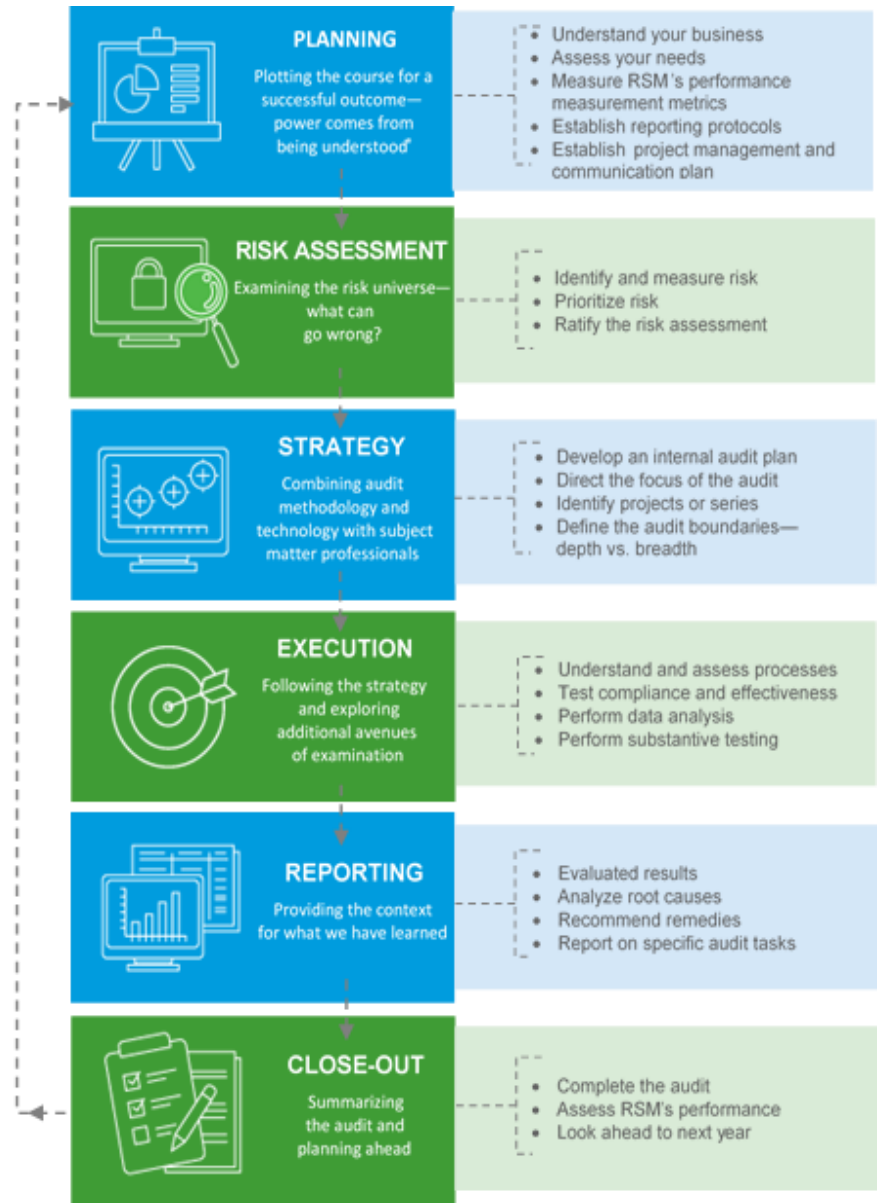



APPENDIX: INTERNAL AUDIT METHODOLOGY

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

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 for more information regarding RSM US LLP and RSM International.

© 2022 RSM US LLP. All Rights Reserved.

