MAULDIN & JENKINS
CPAs & ADVISORS

2025 IA Risk Assessment & Annual Audit Plan

October 14, 2025

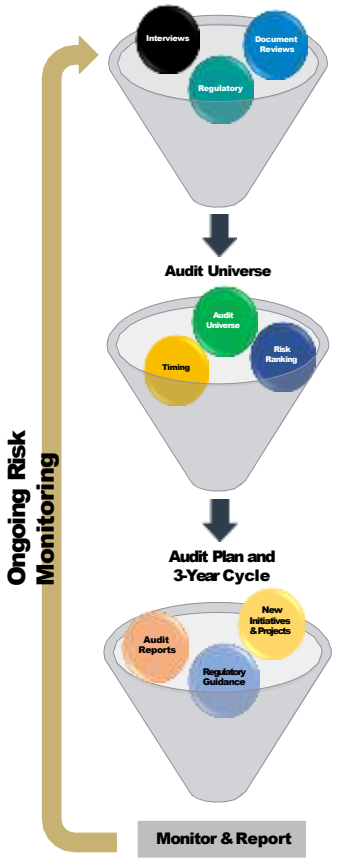
Contents

Executive Summary

- The risk assessment approach consisted of interviews (15) and documentation reviews (87 Government documents uploaded to Suralink).
- Defined the Risk Universe as of June 30, 2025, based on organization charts and annual department budgets.
  - The Risk Universe consists of 92 entities; 2 entities (the City Council and the Mayor's Office) were not rated.
  - Established the Audit Universe (90 rated entities).
- Developed a Risk Taxonomy that consisted of nine categories to organize and group risks by type.
- Based on information gleaned from interviews and the documentation review:
  - Developed the CCG Risk Register, which is a "library" of risks facing the Government, and consists of 630 unique risks. "*Risk*" represents "what can go wrong" in providing public services and the processes supporting the delivering of those services.
  - Identified inherent risk by department and functional activity, then rated each auditable entity by likelihood, impact, and fraud risk.
  - Developed a Risk Assessment tool (Excel document) that records and consolidates the ratings by departments, summarizes the risk assessment results, and serves as a repository for the Government's Risk Register.
  - Results: Identified critical and high-risk departments/offices (6 critical, 32 high); detailed the top 30 risk risks based on a 12-month review of City Council Meeting minutes.
- Developed Observations and Recommendations detailed in the final draft Risk Assessment report.
- Developed tools and processes for developing the Annual Plan and refreshing the risk assessment annually; identified what would be required to implement a risk-based internal audit approach. Debriefed tools, processes, and dependencies with CCG's Internal Auditor.

Project Approach

The Risk Assessment identified, assessed, and prioritized the Government's strategic, financial, operational, and legal & regulatory risks and will be used by the Internal Auditor to develop a risk-based Annual Audit Plan.



Internal Audit Risk Assessment		
1	**Initiation & Planning**	• Conduct initial kickoff meeting with Government project sponsor and key stakeholders. • Identify, confirm, and schedule Interview Requests. • Develop, confirm, and provide Information Request List.
2	**Information Gathering**	• Conduct interviews of management to understand perspectives on strategic initiatives, changes over the past 12 months, and barriers to achieving Government goals and objectives. • Create a tracking list to identify information received and completeness. • Analyze information provided by the Government including source of funds for strategic initiatives and operations, budgets, financial performance, changes, or new requirements for core services, staffing and training as well as citizen feedback and concerns.
3	**Fieldwork & Data Analysis**	• Analyze Government provided information and interview notes. • Score the auditable units in the risk assessment matrix based on the likelihood and the impact of potential adverse events and defined risk factors. • Summarize risk factor scores to create a single score for the auditable unit. Identify potential internal audit activities for the auditable entities scored as high risk.
4	**Validation & Reporting**	• Share preliminary observations with the appropriate stakeholders. • Summarize the approach and results of the risk assessment and solicit feedback. • Based on feedback received, perform additional fieldwork or data analysis as applicable. • Prepare draft report and solicit written feedback. • Develop final report and present results to appropriate stakeholders.

Risk Assessment Results – Major Changes

Objective:

- Identify the most significant changes that occurred over the past 12 months based on analysis of City Council Meeting minutes.
- Assess how these changes have impacted the Government's ability to achieve organizational objectives and deliver public services,

Impactful Changes by Frequency of Mention	
1	Termination of long-standing City Manager Isaiah Hugley
2	Ongoing investigation of the Finance Department
3	Number of long-tenured, experienced resources electing to retire (brain drain)
4	Number of vacant positions, lack of bench strength, resources in new positions, and the difficulty hiring qualified resources
5	Changes in organizational culture – "no longer feels like a family"
6	Changing priorities and funding environment at the Federal level triggering the need for identifying and obtaining new funding sources
7	Number of large, multi-year Capital Projects leading to new contractors and vendors
8	Lack of ability to service the fleet and manage inventory due to scarcity of certified and experienced mechanics
9	Increase in accidents and damage claims from the use of new equipment to collect solid waste – also impacted by an increase in miles driven in CCG vehicles as well as officer experience level
10	Changes in procedures, processes, and controls
11	Cybersecurity breach and ransomware attack
12	Police excessive use of force settlement

Risk Taxonomy & Risk Register

The Risk Assessment Team developed a Risk Taxonomy grouping risks into nine categories.

Objective:

- Develop a Risk Taxonomy that groups like risks into categories to organize the risks impacting the Government.
- Develop the "library" of risks facing the Government.

	Risk Taxonomy		
	Risk Category Level 1	**Subcategory Level 2**	**# Risks**
1	**Governance**	10	33
2	**Strategic/Reputational**	25	25
3	**Financial**	32	53
4	**Operational**	118	312
5	**Legal & Regulatory**	32	108
6	**Public Health & Safety**	19	65
7	**Technology**	4	5
8	**Information Technology**	3	19
9	**External**	4	11
10	**Total**	**247**	**631**

Barriers to Meeting Goals & Objectives

Objective:

- Identify impediments to achieving the Government's objectives and strategic initiatives and define primary drivers.

What Can Keep Departments from Meeting Objectives by Frequency of Mention	
1	Staffing constraints
2	Limited skills/knowledge/experience/training
3	Financial constraints
4	State and Federal regulations
5	Securing alternative funding sources
6	Infrastructure maintenance
7	Recruiting – access to experienced, certified resources (heavy equipment operators/mechanics)
8	Employment retention and satisfaction
9	Interdepartmental collaboration
10	Resistance to change

Common Themes & Interdependencies

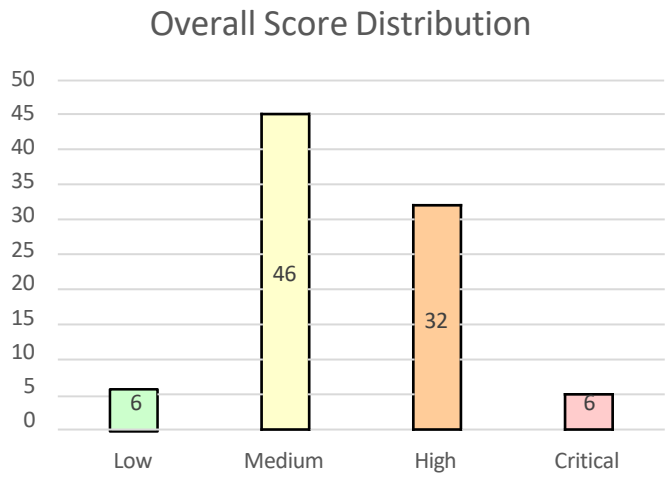
The Government's risk profile is framed by persistent challenges and emerging threats.

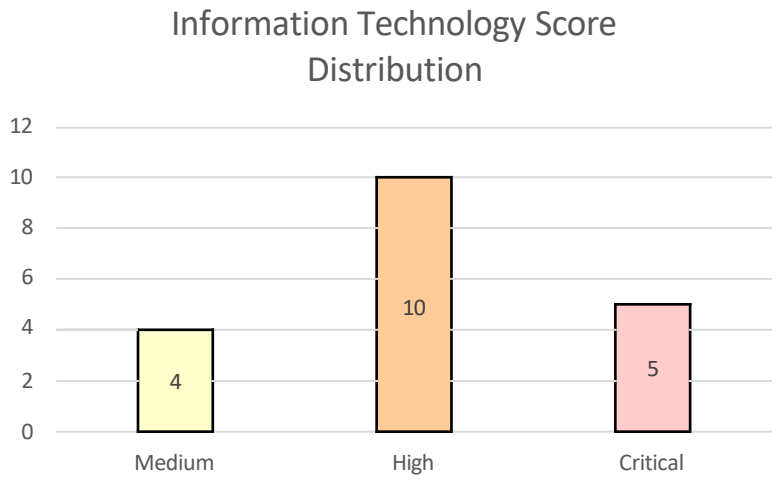
Objective:

- Identify major risk themes and evaluate interdependencies.
- Identify and document emerge risks including new concerns based on market dynamics.
- Evaluate alignment with the Government's strategy and plans.

	Persistent Challenges	Emerging Threats
1	Community Development	Cybersecurity
2	Crime	Environment Air Quality Stormwater Runoff Pollution
3	Economic Development	External – Climate Change Disaster Preparedness and Mitigation Severe Weather (Floods, Tornadoes)
4	Funding/Financial Management Enterprise Fund Sales Tax Indigent Care	Floodplain Management
5	Employee Health and Safety Worker Comp Claims	Housing
6	Homelessness	Project Management Risk
7	Governance Public Trust Transparency	Poverty and Social Equality Homeless
8	Infrastructure Maintenance Improvements	Public Services Access Social Services Access
9	Investment Capital Projects (Material Costs) Pension Funds	Technology Access Adoption
10	Public Safety	Third-Party Risk
11	Public Services	
12	Socio-Economic Disparities	
13	Workforce Retention & Staffing	

Critical & High Risks





Low Risk Rating (Green) – Scores between 1 – 4
Medium Risk Rating (Yellow) – Scores of 5 or 6
High Risk Rating (Orange) – Scores of 7, 8, or 9
Critical Risk Rating (Red) – Scores > or = to 10

Audit Universe -- Entities by Rating

Inherent Risk	Governance	Enterprise	Operations	Boards/ Committees	Courts	IT	Total
Not Rated	2	-	-	-	-	-	2
Low	-	-	3	3	-	-	6
Medium	1	-	11	25	9	-	46
High	3	1	15	11	1	1	32
Critical	-	2	4	-	-	-	6
Total	**6**	**3**	**33**	**39**	**10**	**1**	**92**

	Critical & High Risk Entities	
	Department/Office	**Risk Score**
1	Finance	14
2	Human Resources	13
3	Tax Commissioner	12
4	Public Works	11
5	Civic Center	10
6	Columbus Police	10
7	Muscogee County Jail	10
8	Clerk of Court & Superior Court	9
9	Inspections & Code	8
10	METRA (Public Transit)	8
11	Parks & Recreation	8

3 Year Audit Plan

Enterprise	Total Hours and Anticipated Report Issuance				
	Q1	Q2	Q3	Q4	Total
Allowance for Credit Losses**		300			300
Controllership - Reporting			350		350
Controllership - Other Functions	250				250
Treasury and Investments				400	400
Enterprise Subtotal	**250**	**300**	**350**	**400**	**1,300**
Audit Count by Quarter/Category	1	1	1	1	4

Observations & Recommendations

The depth and breadth of changes impacting the Government highlights the need to reinforce the Government's decision-making and oversight processes to rebuild public trust and demonstrate transparency and accountability.

	Observation	Recommendation
1.	Existing Governance, Risk and Compliance processes do not appear to provide detailed insight into the effectiveness and efficiency of the internal control environment. • New processes, new policies and procedures, new tools or systems, and management changes are risk factors that suggest the need for independent objective assurance that the business has successfully remediated prior performance or compliance issues. • The opportunity is to manage and mitigate those risks prior to intentional public disclosure by evidencing compliance with effective Standard Operating Procedures ("SOPs") that demonstrate that business processes are operating effectively and key internal control effectively mitigating risk.	**Governance Risk and Control Framework (GRC)** 1. Consider establishing a sustainable GRC framework design to develop a complete picture of the internal control environment and its maturity over time. A GRC framework is required to: • Guide prioritization of financial, operational, and compliance improvements; • Evidence compliance with Government policies and legal and compliance requirements; and • Support the accomplishment of strategic initiatives and objectives.
2.	New leadership in key roles, such as City Manager and Human Resources Director, also creates an opportunity to reset tone and direction at all levels of the organization.	**Governance – Tone at the Top** 2. Reset the tone at the top.
3.	Over the past two years, the focus of the internal audit function has increasingly shifted toward investigation activity and support. • In reviewing the Government's IA Charter, M&J could not find specific language authorizing IA's access to all records, personnel, and physical property that fall within the scope of audits currently authorized by the Council. • The function currently does not maintain an Annual Audit Plan, an audit manual detailing its IA Focus, Positioning, policies, and audit procedures, and has not developed a strategic plan.	**IA Positioning and Focus** 3. Redefine the function's Positioning and IA Focus. Develop and evidence Internal Audit policies, procedures, and practices. • Apply a risk-based audit approach to provide independent objective assurance. • Focus on assessing the completeness and maturity of the internal control environment. • Include specific language authorizing IA's access to all records, personnel, and physical property that fall within the scope of audits currently authorized by the Council. • Reduce the focus on forensic investigations. Establish parameters and standards for investigative activity. • Define and Document Internal Audit processes and standards per the Institute of Internal Audit requirements.

Observations & Recommendations (Cont'd)

	Observation	Recommendation
4.	Should the Government choose to shift the focus and positioning of the IA function, it will likely necessitate the need to formalize and build out Audit Committee processes and procedures. • The AC Charter does not provide for a confidential forum for the committee to obtain information on sensitive and critical business issues, such as personnel issues, without management or the public present. • Training for the Audit Committee, the City Council, and management will be required to understand the full implications of applying a risk-based internal audit approach in conjunction with a sustainable Governance Risk & Control (GRC) framework.	**AC Processes** 4. Formalize Audit Committee processes. Procedures, and practices. Expand the AC Charter to define AC roles and accountabilities based pm leading practices. • Conduct Executive Sessions for the specific purposes permitted by the Georgia OMA and ORA and establish Executive Session procedures. • Identify and conduct Governance and internal control training for the City Council, Audit Committee, and Government leadership. • Provide GRC/ internal control training to Audit Committee, City Council, Mayor's Office and senior CCG leadership. • Conduct annual Audit Committee Self-Assessments.
5.	Although requested, M&J did not receive detailed process documentation at the department level. We note that does not mean the process documentation does not exist, but may suggest that process flows identifying process inputs, outputs, systems, and tools used, internal controls, and KPIs are not widely used.	**Process Analysis and Maturity** 5. Apply a quality tool, such as Business Process Optimization or Process Analysis and Maturity, at the department level to measure process effectiveness and maturity and facilitate continuous improvement to assist in mitigating funding, recruiting, and staffing challenges
6.	The Government does not have a policy requiring Information Technology to be involved in the evaluation and supporting of technology focused projects and purchases.	6. An IT policy should be created by an IT Steering Committee, and a Council Member or designee assigned as Chair. This committee should have the authority to create policies related to Information Technology governance and standards.
7.	The Government has not established an IT Steering Committee that evaluates risks (including cybersecurity oversight), creates Technology policies, monitors compliance with policies, or monitors key performance metrics for the IT Department.	7. The Government should consider evaluating this gap to determine if FTE(s) or consultants should be obtained to complete these tasks and maintain going forward.
8.	There appears to be a gap in necessary human resources to prevent, detect, and respond to cybersecurity events daily and provide 24/7/365 monitoring). In addition, the IT Department does not have a Security Information and Event Management (SIEM) tool or system – a foundational and standard cybersecurity tool necessary to detect and respond to cyber security events and incidents.	8. The government should consider evaluating these gaps to determine what model or method should be used to close this gap – an FTE and SIEM as a Service (hybrid model) or the outsourcing all cybersecurity monitoring to Managed Security Service Provider. (Continued on the next page)

Observations & Recommendations (Cont'd)

	Observation	Recommendation
8.	There appears to be a gap in necessary human resources to prevent, detect, and respond to cybersecurity events daily, providing 24/7/365 monitoring). In addition, the IT Department does not have a Security Information and Event Management (SIEM) tool or system which is a foundational and standard cybersecurity tool necessary to detect and respond to cyber security events and incidents.	• Within one calendar year, the Government should conduct or contract an Internal and External Network Penetration Test. This should include Penetration Testing on the government's public facing websites, wireless access points, and include a credentialed vulnerability scan. • Within two years, the government should conduct a full NIST 800-53 Audit to determine if Policies, Procedures, and Controls are in place and operating effectively. This audit should include without exception, Information Security controls and Business Continuity / Disaster Recovery controls.

Developing the Annual Plan

Risk Assessment result drive prioritized audit areas and direct the development of the scope and objectives for individual audits. .

- A three-year Audit Plan should be viewed as a working document that identifies the specific audits and audit areas planned for fiscal years 2026 – 2028.
- The Internal Auditor may need to adjust the plan at key points during the year, most often at the end of the 2nd and 3rd quarters, to address emerging risks that could significantly impact the Government's achievement of its objectives.

In determining the FY2026 audit activities, the Internal Auditor will:

- Review specific risks and functional areas and
- Consider risk-based priorities as well as other factors
  - requirements by law or regulation
  - timing of department activities
  - requests from City Council and management.

Annual Audit Plan Development		
1	**Tie Audits to Risk Assessment**	• Clearly demonstrate how the selected audits address the highest-priority risks.
2	**Allocate Resources**	• The plan should show how limited audit resources (staff hours, budget) are directed against the most critical areas.
3	**Obtain Approval of the Plan and Changes**	• The Audit Committee approves the annual audit plan – as well as any proposed changes during an audit year – to ensure alignment with their priorities and reinforce the department's independence.
4	**Ensure Adaptability**	• The plan should be adaptable to respond to emerging risks, changes in CCG operations or services, and requests from the City Council or management • Leading practice is to establish a reserve of hours for City Council requests.

Risk-Based Internal Audit Approach

"Success" is defined by meeting stakeholder's expectations, continuously increasing the efficiency and effectiveness of the organization's risk coverage, and by driving continuous improvement of the internal control environment.

Right Sized

- The Internal Audit function is sized and staffed not only against the size of the organization and the value of its assets, but also against the organization's risk appetite, the state of the internal control environment, and regulatory mandates.

IA Focus

- Address regulators and other stakeholders' expectations; align audit scope against regulatory requirements, SOPs, and key internal control design and operational effectiveness.
- Identify the "risks that matter" relative to the organization's strategy, risk profile, and investments.
- Conduct proactive, value-added reviews that measure the effectiveness of key internal controls..

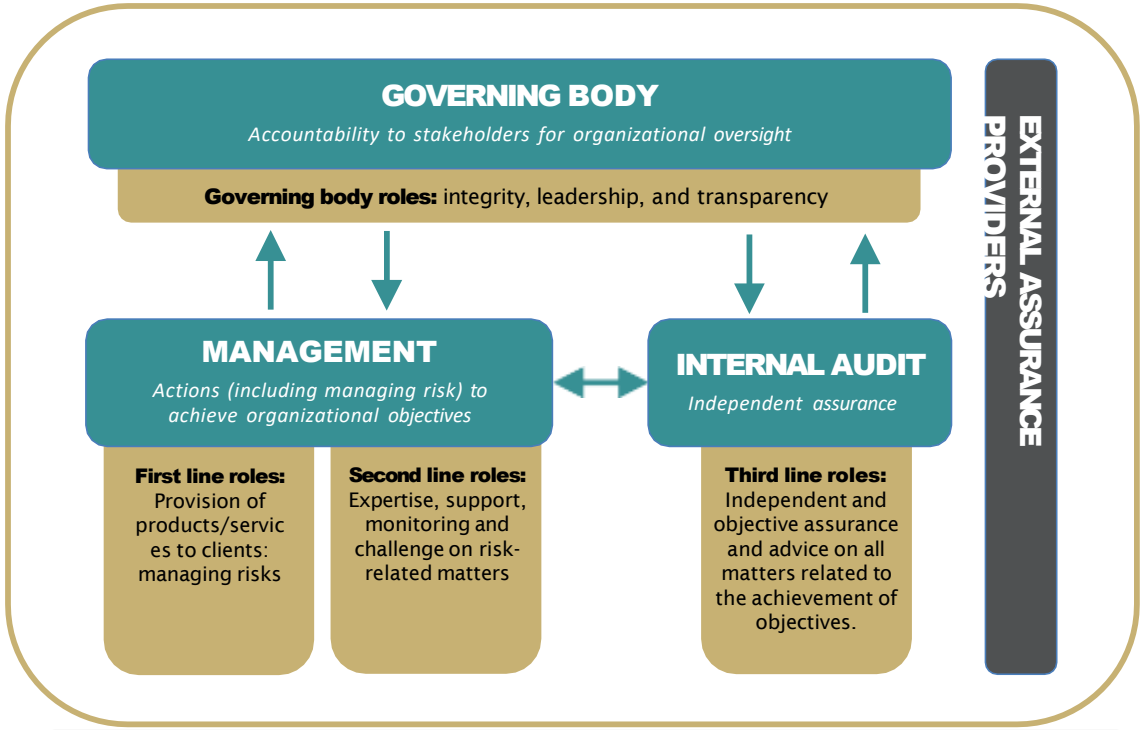
Fit For Purpose

- The audit scope dictates the skill, experience, and expertise required of auditors.
- Each audit should be delivered by resources with the subject matter expertise to effectively assess risk and compliance and provide valued-added recommendations.

The Role of Internal Audit

*The Three Lines of Defense Model serves as a defining concept of risk management by defining specific risk for managing risk with the organization.**

- Changes to the organizations 's risk and control environment are driven by both external and internal risk drivers.
- Internal risk drivers can include strategic priorities, introduction of new services, and budget.
- For example, new strategic priorities and services require new processes and systems that introduce new risks. Further, they create interdependencies that require assessment.
- Emerging risks also require identification and assessment to understand their impact on the efficiency and effectiveness of the internal control environment.
- Internal Audit's role is to provide Independent and objective assurance and advice on the achievement of the Government's objectives.



- *First Line of Defense* – Operations process & control owners
- *Second Line of Defense* – Legal, Compliance, CISO, risk owners
- *Third Line of Defense* – Internal Audit

*Source: Institute of Internal Auditors

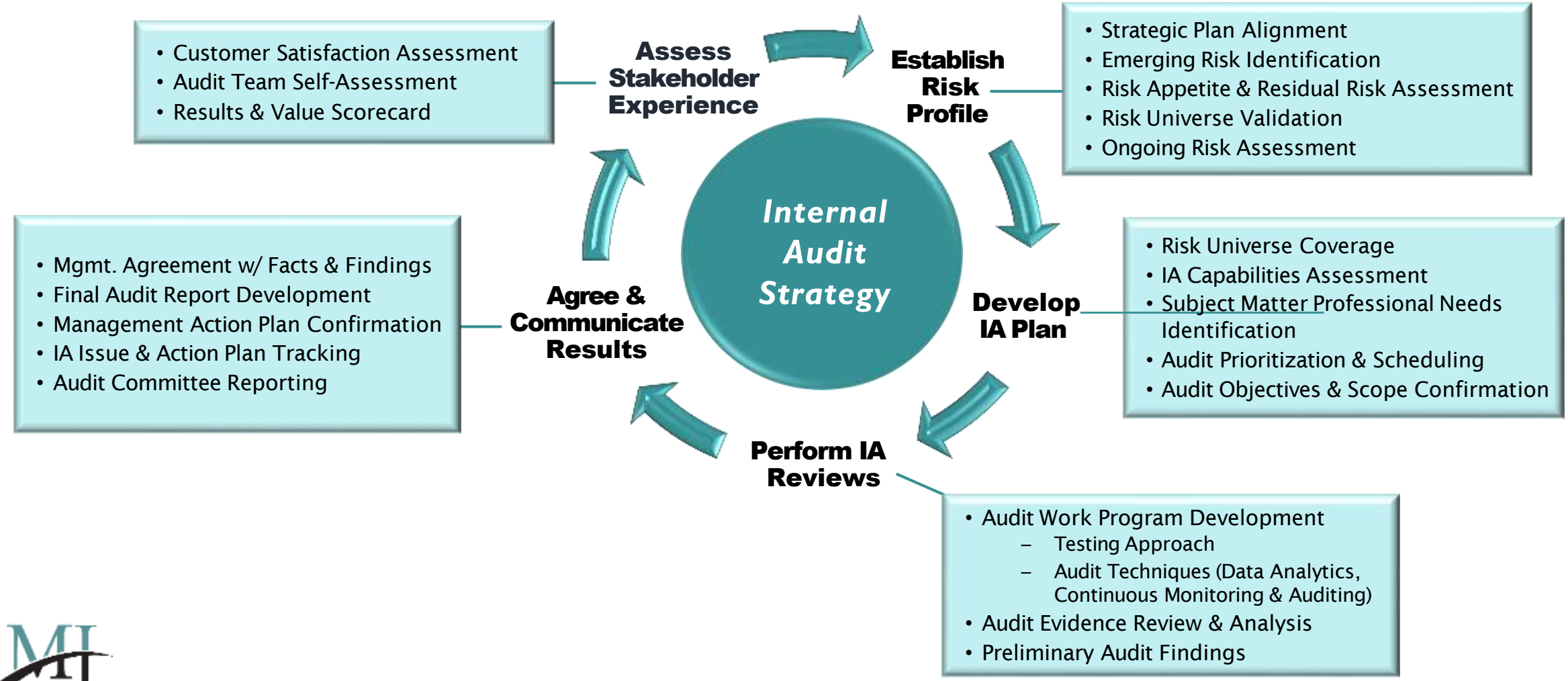
Foundational Elements – Effective IA Functions

Each of the elements are critical to maintaining an effective internal audit function.

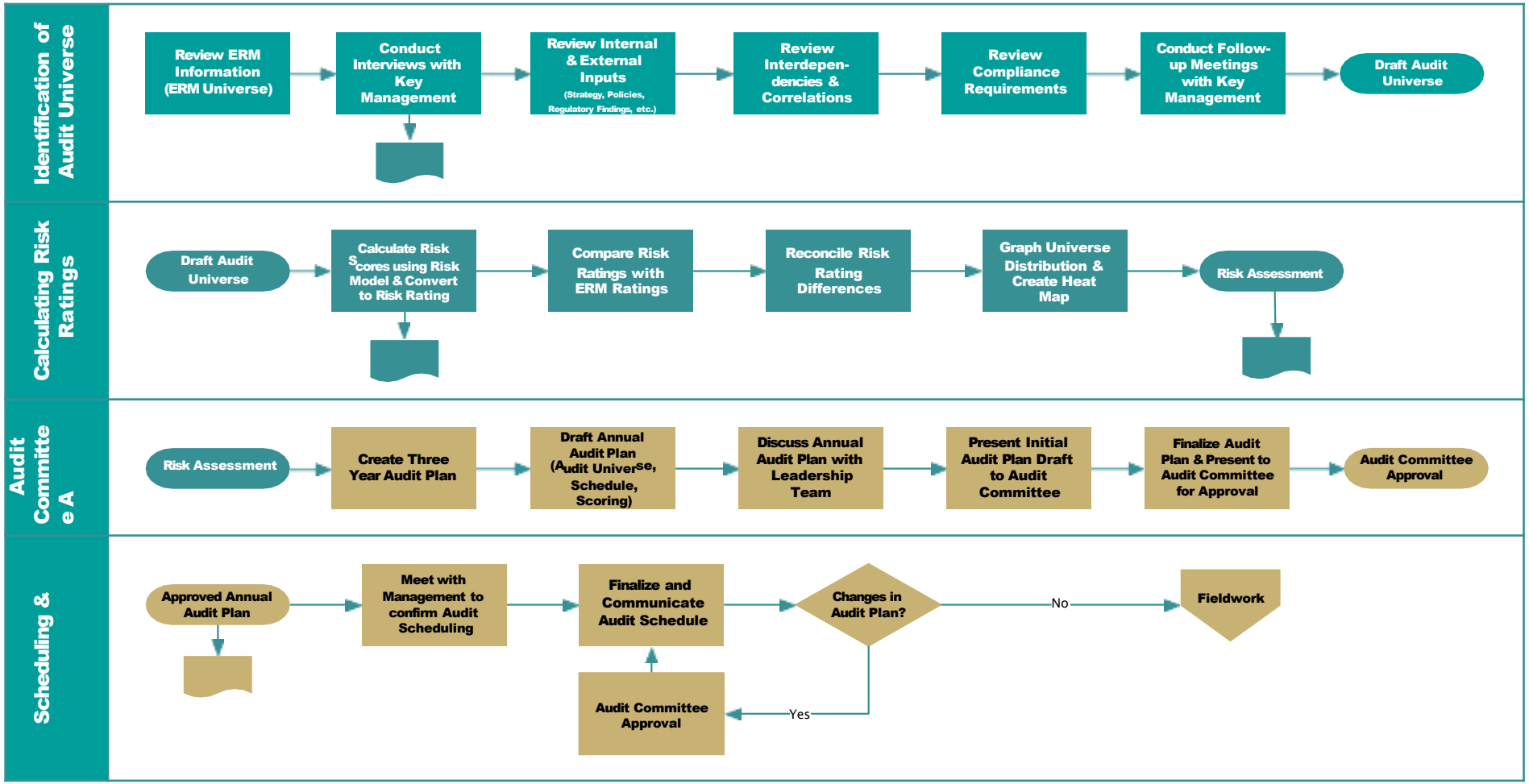
Additional enhancements to the organization's internal audit function build upon the effective execution of each of these foundational elements.

The Internal Audit Annual Cycle

The Risk Assessment should be refreshed annually to address changes in new fiscal year's Strategic Plan, Budget, and priorities. A new, de novo Risk Assessment should be conducted every three to five years.



Internal Audit Plan Development – End-to-End Process



Internal Audit Activities by Phase

Phase	1. Audit Planning	2. Audit Kick-off	3. Audit Fieldwork	4. Audit Findings & Recommendations Development	5. Audit Report Development & Issuance	6. Audit Assessment & Audit Committee Reporting
Process	**Form Team & Plan Audit**	**Analyze Information & Conduct Audit Kick-off**	**Conduct Fieldwork**	**Develop Findings & Recommendations**	**Develop & Issue Audit Report**	**Debrief & Assess Audit**
Internal Audit Activity	• Identify & assemble Audit team • Draft ***Planning Memo*** • Send ***Announcement Memo*** • Issue ***Information Request & Interview Request List*** • Develop ***Communication Plan***	• Receive & review client information • Understand process & procedures; identify risks • Draft ***Audit Program*** • Hold ***Entrance Meeting*** with Management • Update ***Planning Memo***, modify ***Audit Scope & Program*** as necessary	• Execute ***Audit Program*** • Conduct ***Status Update Meetings*** with client management on issues & observations • Document ***Preliminary Issues*** in the ***Findings Summary*** • Organize interview notes, testing results, and evidentiary support in ***Work Papers***	• Discuss ***Preliminary Issues*** with process & control owners • Validate ***Identified Issues*** with process & control owners / management • Draft ***Recommendations*** to address issues & discussed with process & control owners / management	• Issue ***Draft Report*** to management • Request ***Management Responses*** • Update ***Draft Report*** with management responses • Finalize Management Responses • Issue ***Final Audit Report*** • Hold ***Closing Meeting***	• ***Audit Debrief*** conducted • ***Engagement Assessment*** completed
Audit Metrics	▪ ***Planning*** starts four weeks in advance of fieldwork ▪ ***Announcement Memo*** sent three weeks in advance of fieldwork ▪ ***Information Request List*** **sent** two weeks in advance of fieldwork; ***Interview Request List*** one week in advance ▪ ***Document Request List*** sent two weeks in advance of fieldwork	▪ ***Planning Memo*** and ***Audit Program*** completed and reviewed prior to fieldwork	▪ ***Fieldwork*** completed within six calendar weeks ▪ ***Weekly Status Updates***	▪ ***Findings*** detailed in proper business context & in priority order ▪ ***IA Liaison*** input obtained on findings ▪ ***Work Paper*** reviews completed within two days of submission ▪ ***Fieldwork*** completed prior to closing meeting ▪ ***Budget*** met or below	▪ Re-writes limited to three drafts ▪ ***Draft Report*** issued within 10 days of fieldwork completion (with management responses) ▪ ***Final Report*** issued within 15 days of fieldwork completion ▪ Audit issues entered (Issue Tracking database)	▪ ***Engagement Assessment*** completed within 15 days of report issuance ▪ ***Audit Results*** summarized for Audit Committee Reporting and incorporated into the Internal Audit Value Scorecard

Continuous Improvement

Continuous Enhancement in FY2025 and Beyond

To attain an improved and effective control environment, the Government's client-facing service delivery and support processes need to be continually monitored, analyzed, and assessed.

Internal Audit advises stakeholders on risk and control matters based on the Government's overall risk profile. The actions shown below drive continuous improvement in the control environment across the Government and a corresponding reduction in the overall risk profile.