



AGENDA

Audit Committee
Wednesday, August 14, 2019
6:00 pm – 7:00 pm
City Hall, Room 103

- A. Review and approval of the Wednesday, June 12, 2019 Meeting Minutes

- B. 2018 Work Plan Update
 - Sheriff's Office – Inmate medical services
 - Public Utilities Department — Water Business Office
 - Central Services Department — Fleet Management Program

- C. Development of the Annual Audit Work Plan –
 - Alternative Approach to Audit Selection - Risk Assessments

- D. Items for Discussion at next meeting

Attachments:

1. Draft Minutes from the June 12 meeting
2. Meeting Agenda – August 14, 2019
3. Status of Work Plan Activity
4. Risk Assessment Presentation

The next meeting is scheduled for
Wednesday, September 11, 2019

Note: The Audit Committee Meeting is open to the public. However, public comments are not received unless the Committee Chair requests that an individual provide information to the Committee.

AUDIT COMMITTEE MEETING MINUTES

Wednesday, June 12, 2019

Committee Members Present:

Commissioner Melissa Link, Committee Chair
Commissioner Patrick Davenport
Commissioner Russell Edwards
Commissioner Ovita Thornton

Visiting:

Deborah Lonon, Assistant County
Manager
Glenn Coleman, Assistant Director,
Public Utilities
David Fluck, Director, Central Services
Michael Smith, Community Citizen
Lee Shearer, Athens Banner Herald
Blake Aued, Flagpole
Foster Steinbeck, Red and Black

Staff:

Stephanie Maddox, Internal Auditor
Jill Arquette, Management Analyst
Deborah Allen, Recorder

Member(s) Absent:

Commissioner Allison Wright

Committee Chair Link called the meeting to order at 6:04 pm.

A. Approval of Minutes:

The Committee unanimously approved the Minutes of both the April 10, 2019 and the May 1, 2019 meetings.

B. 2018 Work Plan Update:

Internal Auditor Maddox provided a brief status update on the annual work plan:

- Public Utilities Department – Water Business Office
- Central Services Department – Fleet Management Program
- Sheriff's Office

The Committee reviewed and discussed the submittal of additional information provided by the Sheriff's Office related to follow-up questions from the Audit Committee.

- The Committee requested staff update the audit report highlights in the Sheriff's Office Operational Audit to include additional activity and discussions that have been held.
- The Committee requested staff submit the Operational Audit of the Clarke County Sheriff's Office to the full Commission and to submit the report to the Clerk of Commission for acceptance on the official record at the August voting meeting.
- Staff will contact the Sheriff's Office to initiate the last phase of the audit, a review of the Medical Services Contract.
- The Committee requested staff conduct a follow-up review of the progress of the Sheriff's Office on implementing recommendations in 12 months.

C. General Discussion:

The Committee discussed revising the current audit selection process and asked staff to prepare alternative approaches for discussion at the next committee meeting.

D. Items for Discussion at August 14, 2019 meeting:

Alternative approaches to select audits for the Office of Operational Analysis' Annual Work Plan.

The August 14, 2019 meeting is scheduled for 6 p.m. – 7 p.m. at City Hall.

The meeting adjourned at 7:00 pm.

The above summation is an interpretation of the items discussed and decisions reached at the above-referenced meeting, not a transcript of the meeting. A digital recording of the meeting is available upon request.

AUDIT STATUS REPORT

DATE: August 12, 2019
 TO: Mayor and Commission
 FROM: Stephanie Maddox, Internal Auditor
 Office of Operational Analysis (formerly, the Auditor's Office)
 SUBJECT: Status of 2018 Work Plan Activity

The following table summarizes the current status of each audit according to audit stages. Please find a description of the audit stages below.

WORK IN PROGRESS

Audit	Status		Completion Forecast
	Percentage indicates completion level		
Operational Audit of the Clarke County Sheriff's Office	Pre-Audit Planning – 100 % Discovery Stage – 100% Analysis – 100 % Conclusions – 100% Recommendations – 100%	Final report submitted to Clerk of Commission for acceptance at the August 2, 2019, Mayor and Commission Meeting.	March 2019
NOTE: Audit report completed March 2019; final responses from the Sheriff's Office received May 2019			
Public Utilities Department – Water Business Office	Pre-Audit Planning – 100 % Discovery Stage – 100% Analysis – 100% Conclusions – 95% Recommendations – 95%	Additional follow-up interviews completed with WBO supervisory staff; audit report writing near completion.	August 2019
Central Services Department – Fleet Management Program	Pre-Audit Planning – 100% Discovery Stage – 55% Analysis – 25% Conclusions – 0% Recommendations – 0%	Audit plan finalized; survey results received; review and analysis underway; interviews anticipated to start August 2019.	October 2019

Audit Stages

PRE-AUDIT PLANNING: OOA staff conducts literature reviews, identifies benchmark communities, creates the pre-audit survey(s), and prepares a list of documents to request from various ACC departments related to the audit client.

OOA staff schedules a pre-conference meeting with the audit client/department leadership to discuss the audit process, the timing of fieldwork, and answer any questions.

DISCOVERY: Interviews, information validation, observations and surveys. As this stage is critical to the preparation of a complete and meaningful audit, it consumes the majority of time involved.

ANALYSIS: Assigning meaning/value to the information; determining what it reveals related to the scope of the audit. Defines systems, processes and practices in terms of effectiveness and efficiency.

CONCLUSIONS: Identifies and describes constraints and opportunities regarding developments and implementation of needed improvements.

RECOMMENDATIONS: Suggests action that can be taken in consideration of the constraints and opportunities.

Risk Assessment

UNIFIED GOVERNMENT OF ATHENS-CLARKE COUNTY
OFFICE OF OPERATIONAL ANALYSIS
AUGUST 2019

Auditing Responsibility

According to the Institute of Internal Auditors (IIA) International Standards for the Professional Practice of Internal Auditing, Section 2120.A.1 – The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

What is a Risk Assessment?

Risk assessment, as defined by the IIA, is a systematic process for assessing and integrating professional judgments about probable adverse conditions and/or events.

An Internal Audit Risk Assessment is the identification, measurement, and prioritization of risks for the purpose of selecting and developing auditable areas.

Definitions:

Risk

The possibility of an event occurring that will have an impact on the achievement of objectives and is measured in terms of impact (severity) and likelihood (probability).

Risk Management

A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

Risk Appetite

The level of risk that an organization is willing to accept.

Office of Operational Analysis (OOA) Risk Assessment vs. Safety & Risk Management

OOA Risk Assessment

- Focus: Assessing a departments level of operational risk to determine audit necessity.
- The purpose of a risk assessment conducted by OOA is to identify and assess a departments operational risks. Based on the results of an assessment, Audit Committee members may make an objective decision as to which audits should be conducted by OOA.

Safety & Risk Management

- Focus: Employee and property safety
- The Safety & Risk Division of HR manages insurance, injury, and illness claims against and generated by ACC for damage to persons and ACC property, provides safety training (e.g. trench safety, CRASE, DDC, CPR/AED/First Aid, etc.), conducts safety audits of ACC facilities, and handles workers compensation claims.

Step 1: Identify Risks

What is included in a Risk Assessment?

- A questionnaire is developed to compile information on the potential departments to be audited (auditable units) and to address all risk factors.
- The following information may be requested from the departments in the questionnaire:
 - Description of the departments activities and functions.
 - Business objectives, risks, and exposures.
 - Systems utilized.
 - Lists of major vendors and estimated annual payments.
 - Total expenditures for a designated period of time.
 - Budgets for a designated period of time.
 - Number of authorized employees.
 - Number of vacant positions and length of time the position(s) have been vacant.
 - Questions to address specific risk factors listed by OOA.
 - Additional risks identified by the auditable unit.

Risk Factors

Risk factors are developed using knowledge of the Athens-Clarke County Unified Government and best practices in internal auditing.

Each risk factor is scored based on the impact and likelihood of the risk occurring to the department being audited.

- **Likelihood** – *The measure of the probability of an unfavorable event occurring.*
- **Impact** – *The measure of the consequence of an unfavorable event occurring.*

Risk Categories

The impact of each risk factor is based on three categories: financial, operational, and/or compliance, and the impact each will have on ACC.

The overall goal of the risk scoring approach is to ensure that OOA includes high-risk areas in the audit plan and considers routine audits on those areas.

The three risk categories are defined as follows:

- **Financial Risk** – *Impact related to revenues, expenditures, assets, liabilities, and equity decisions.*
- **Operational Risk** – *Risk is exposed if operating objectives are not being met through the effective and efficient use of resources. This includes potential for fraud, business disruptions, customer service, and safety.*
- **Compliance Risk** – *Risk is exposed if operating (or potentially operating) outside of applicable laws and regulations.*

Step 2: Measure Risks

Risk Assessment Criteria

- The primary purpose of a risk assessment is to **identify** risks, **assess** them, and **reduce** them to an acceptable level.
- Before operational risks can be assessed, the risk criteria and risk factors from which to **measure** and **score** must be established and defined.
- To achieve this, a measurement system that includes a **baseline** (an organization's acceptable risk level) **and a method of scoring** (a risk scoring system) must be established.
- The **criteria** are derived from the organization's culture and industry, external and internal context or controls, applicable laws, standards and other requirements.

Sample Risk Factors Categorized

Risk Categories: **O** – Operational Risk Impact; **F** – Financial Risk Impact; **C** – Compliance Risk Impact

Risk Factors	Risk Category	Weight	Description
Compliance with Regulations, Laws, Policies, and SOPs	O, F, C		Impact of compliance risk increases with more reliance on federal and/or state laws, regulations, and funding, and prior issues.
Inventory	F		Risk of asset misappropriation, depreciation of obsolete items, or nonexistent items recorded as inventory.
Handling of Cash	O, F		Impact and likelihood or risk increases with more cash collection and less resources to monitor.
Departmental Changes	O, F		A dynamic change in employees increases the probability of inefficiencies as well as errors occurring.
Quality of Internal Control System	O, F, C		Reliability of internal control system is important in detecting and preventing operational and systemic errors.

Sample Risk Factors

- **Compliance** with Regulations, Laws, Policies and SOPs
- Objectives/Projects
- Service User **Experience**
- Business Continuity
- **Publicity**/Reputation
- **Injury**
- Audit **History**, Prior Audit Results
- Inventory
- Handling of **Cash**
- Instances of Fraud, **Waste**, & Abuse
- **Complexity** of Transactions
- Departmental Changes
- **Information Technology** Changes
- **Quality** of Internal Control System

Step 3: Prioritize Risks

Risk Identification

Some categories in which to identify risk:

- People, processes, systems, and events.
- Employment **practices** and workplace safety.
 - **Turnover** rates
 - Vacancy rates (position **vacancies** and time vacant)
 - Tenure of the department/division and senior management
 - Staff size in relation to activity volumes
 - Reliance on key staff and **management succession**
- **Fraud**.
 - Internal fraud
 - External fraud
 - **False** expense claims
- Compliance with laws, regulations, contracts, policies, and procedures.
 - External/criminal **threats**

Risk Identification (continued)

- Effectiveness and efficiency of operations.
 - Organizational **changes**
 - Complexity
 - Activity volumes
 - New or changing product or process
 - **Customer** satisfaction
 - Degree and complexity of projects
 - Processing, storage, and data **communication**
- Reliability and integrity of financial and operational systems and information.
 - **Misuse** of systems
 - Misuse of confidential information
 - Access control and security
 - Volume, severity, and duration of system **outages**
 - Volume, severity, and type of security incidents
 - System response time
 - Mainframe and **network availability**

Understanding the Operational Area of an Audit

People

- What is the department's position within the organization?
- What is the department's organizational structure?
- Are there clear, direct, and sufficiently high reporting lines?
- What data, reports, or responsibilities flow across departments?
- Are departmental activities and management's roles clearly defined?
- What is the experience level and expertise of management and key staff?

Processes

- Workflow processes
- Dependencies and interfaces with other departments and/or external service providers
- Transaction volumes and dollar amounts
- Risk and control assessments
- Procedures
- Monitoring of reports

Systems

- Major systems and components (hardware and software)
- System interfaces (internal and external)
- Outsourcing vendors
- Security

Sample Scoring – Risk Factors Likelihood (probability) and Consequences (severity)

Rating	Likelihood	Description
5	Frequent	Represents a risk with a 90% or greater chance of occurrence and will significantly impact the achievement of departmental goals and objectives.
4	Probable	Given the current work environment, there is a 65% up to 90% chance of risk occurring with a possibility of repeated incidents.
3	Occasional	Represents an area or problem that has a 35% up to 65% chance of occurring and may prevent achieving departmental goals and objectives.
2	Remote	Represents an area that has a 10% to 35% chance of occurrence with little impact on achieving the department's goals and objectives.
1	Improbable	Represents an area with less than a 10% chance of occurrence and has little to no impact on achieving goals and objectives.

Risk Factor	Negligible	Minor	Moderate	Major	Catastrophic
Compliance with Regulations, Laws, Policies and SOPs	Minor non-compliance with internal standards. Small number of minor issues requiring improvement.	Singular failure to meet internal policies or SOPs. Minor recommendations which can be easily addressed by management.	Repeated failure to meet internal standards or follow protocols. Important recommendations that can be addressed with an appropriate management action plan.	Repeated failure to meet external standards. Failure to meet local, State, and/or Federal regulations. Critical report or substantial number of significant findings and/or lack of adherence to regulations.	Gross failure to meet external standards. Repeated failure to meet local, State, and/or Federal regulations. Severely critical report with possible major reputational or financial implications.
Objectives/ Projects	Barely noticeable reduction in scope, quality or schedule.	Minor reduction in scope, quality or schedule.	Reduction in scope or quality of project; project objectives or schedule.	Significant project over-run.	Inability to meet project objectives. Reputation of the organization seriously damaged.

Risk Values

(likelihood x severity)

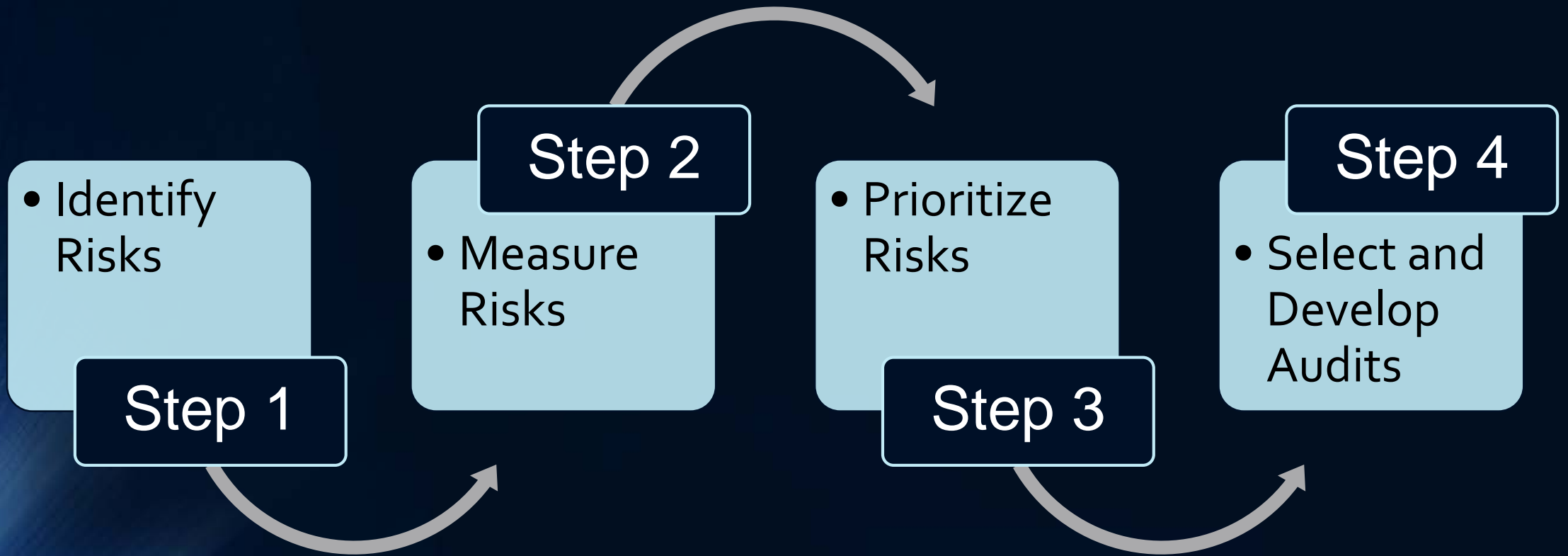
Likelihood of Risk	Level of Severity				
	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Frequent (5)	5	10	15	20	25
Probable (4)	4	8	12	16	20
Occasional (3)	3	6	9	12	15
Remote (2)	2	4	6	8	10
Improbable (1)	1	2	3	4	5

Step 4: Select and Develop Audits

Audit Selection

- Questionnaires are developed to compile information and to identify if any departmental risks exist and if so, to what level.
- Using established risk factors and criteria, levels of risk indicated through the questionnaires are measured.
- Audit Committee prioritizes risks identified and the level of severity.
- Audit Committee selects audits to be conducted by OOA.

Risk Assessment Process Overview



Key Points

- A risk-based audit planning approach adds value to an internal audit.
- Risk identification is the most important step in the process.

Questions?

The background is a dark blue gradient with a series of curved, parallel lines that create a sense of depth and movement. A bright, glowing light source is visible on the right side, casting a soft glow across the scene.