CITY COUNCIL AGENDA

CITY OF **Guelph**
Making a Difference

Meeting Room C, Guelph City Hall, 1 Carden Street

DATE   Wednesday, February 18, 2015 – 6:00 p.m.
**   (Dinner served at 5:00 p.m.)**

Please turn off or place on non-audible all cell phones, PDAs, Blackberrys and pagers during the meeting.

Disclosure of Pecuniary Interest and General Nature Thereof

Internal Audit and Risk Management Workshop

1.   **Enterprise Risk Management Training (ERM) Session**
      Presentation: Loretta Alonzo, Internal Auditor

      • Presentation Matrix
      • ERM Framework
      • ERM Policy

2.   **Internal Audit Training**
      Presentation: Loretta Alonzo, Internal Auditor

      • Presentation
      • Handbook

ADJOURNMENT

Council Workshop

Part 1

Enterprise Risk Management

February 18, 2015

What is Enterprise Risk Management? (ERM)

Enterprise risk management (ERM) is a method or process used by an organization to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying specific risks and opportunities, assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and proactively addressing risks and opportunities the City of Guelph will protect the interests of the public and create value for all stakeholders.

What is the purpose of ERM?

- Provide guidance to advance the use of a more corporate and systematic approach to risk management

- Contribute to building a risk-smart workforce and environment that allows for responsible risk-taking while ensuring legitimate precautions are taken to protect the Corporation, ensure due diligence and maintain the public trust

- Establish a set of risk management practices that departments can adopt to their specific circumstances or mandate

What is the ERM Framework?

The ERM Framework consists of the following components:

1. **Risk categories**

2. **Risk Matrix – Impact/Likelihood Scale**

3. **Risk Impact Criteria**

Categories of Risk

Service delivery – Risk of not meeting customer expectations

Employees – Risk that employees, contractors or other people at the corporation will be negatively impacted by a policy, program, process or project including physical harm

Public – Risk that the policy, program or action will have a negative impact on citizens

Physical Environment – Risk that natural capital will be damaged

Reputation – Risk associated with anything that can damage the reputation of the corporation

Financial – Risk related to decisions about assets, liabilities, income and expenses including asset management, capital and operational funding, economic development, theft or fraud

Regulatory – Risk related to the consequences of non-compliance with laws, regulations, policies or other rules

Risk Matrix – Impact/Likelihood Scale

Impact is quantified as:

Scale 4: Catastrophic
Scale 3: Major
Scale 2: Moderate
Scale 1: Minor

Likelihood is quantified as:

Scale 5: Almost Certain
Scale 4: Likely
Scale 3: Somewhat likely
Scale 2: Unlikely
Scale 1: Rare

When impact and likelihood are assessed, a risk rating is calculated by multiplying the impact scale X the likelihood scale.

For example: A specific risk has been assessed as having an **impact** described as "**Major**", **with a scale of 3**. **The likelihood** of this risk occurring has been assessed as "**somewhat likely", with a scale of 3**. The risk rating total is impact multiplied by likelihood, or a **total score of 9.**

6

Risk Matrix – Impact/Likelihood Scale

When the Category, Impact, and Likelihood are presented in a chart format, they create a chart referred to as the **"Risk Matrix".**

The risk matrix assigns colours to the resulting score based on the corporation's risk tolerance as set out below

Impact ⬇					
4 Catastrophic	4	8	12	16	20
3 Major	3	6	9	12	15
2 Moderate	2	4	6	8	10
1 Minor	1	2	3	4	5
Likelihood ➡	1 Rare	2 Unlikely	3 Somewhat Likely	4 Likely	5 Almost Certain

Sample Risk Register

Risk Factor (Issue and Risk)	Initial Impact	Likelihood	Overall Rating
Risk that lack of a detailed project budget and formal monitoring process may result in cost overruns through unauthorized expenditures and/or scope creep.	3.00 Major	3.00 Somewhat Likely	9.00
Risk that the planned road expansion may result in damage to environmentally sensitive wetlands.	3.00 Major	4.00 Likely	12.00
Risk that changes to Guelph Transit schedules will be temporarily delayed due to road construction.	2.00 Moderate	4.00 Likely	8.00
Risk that the new software application for recreation program scheduling will require afterhours IT support resulting in overtime costs of approximately $800.	1.00 Minor	2.00 Unlikely	2.00

End of Part 1 - E.R.M.

Questions?

Council Workshop

Part 2

Internal Audit

February 18, 2015

WHAT IS INTERNAL AUDIT?

Internal Audit is a professional, independent assurance and consulting function designed to add value and improve the City of Guelph's operations and systems of internal controls. Internal Audit brings a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control and governance processes.

There is no legislated requirement for an Internal Auditor within the Municipal Act 2001. Ontario municipalities have either an Internal Auditor or have appointed an Auditor General by by-law. Only 2 cities have Auditors General, Toronto and Ottawa.

WHAT IS THE DIFFERENCE BETWEEN AN **INTERNAL AUDITOR** AND AN **AUDITOR GENERAL**?

An Internal Auditor is responsible to **both Council and Management** to provide independent assurance and improve the City's operations and systems of internal control. Their relationship with Management is ideally as business partners.
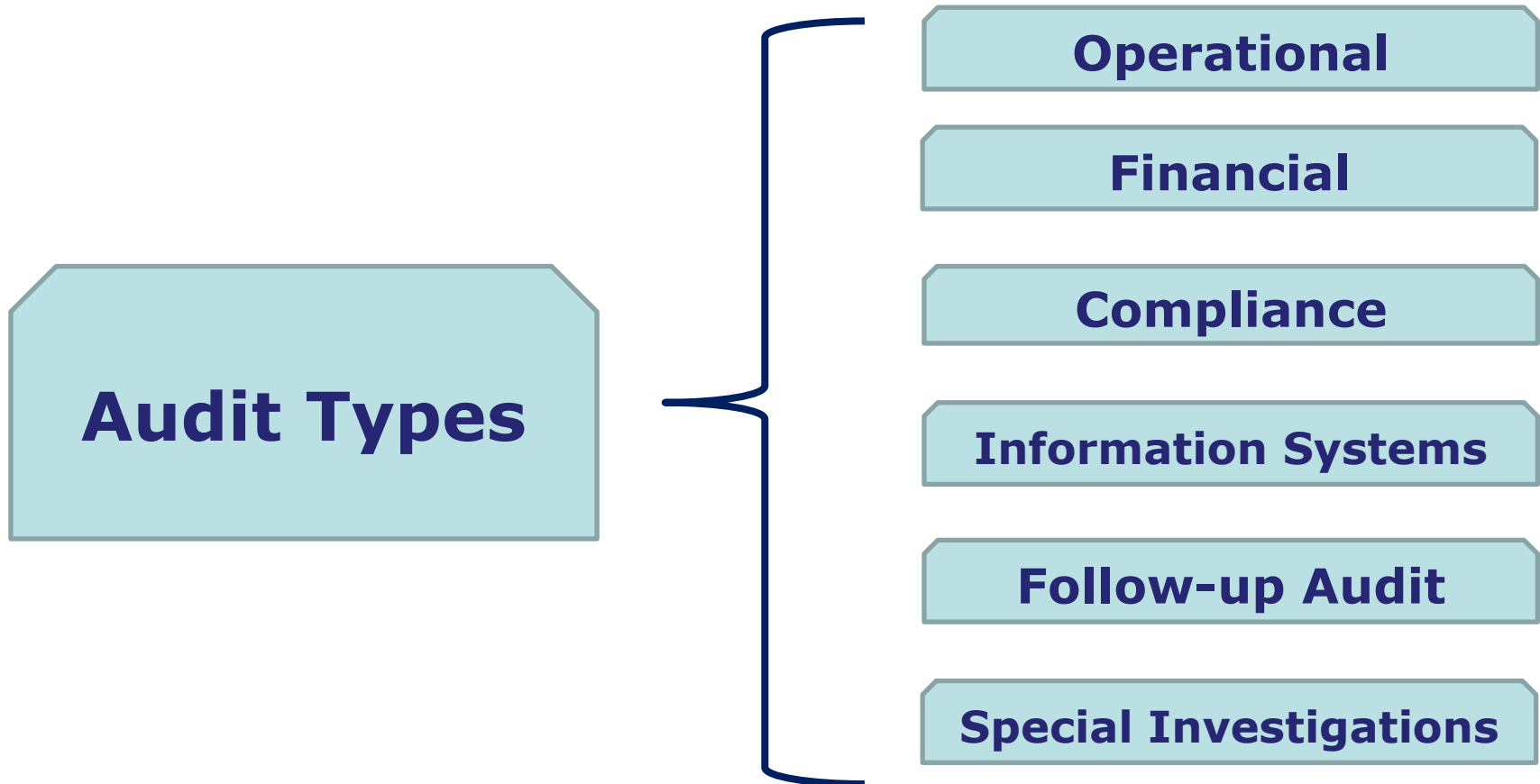
An Auditor General is responsible **only to Council representing the Public**. They typically perform only Value-for-Money type audits. Their relationship with Management is often adversarial.

TYPES OF AUDITS

There are 6 basic types of audits that may be conducted by an internal auditor.

Each type of audit has a different purpose and approach.

They vary in complexity or scope and may sometimes be combined or overlapped.

Audit Types

- Operational
- Financial
- Compliance
- Information Systems
- Follow-up Audit
- Special Investigations

OPERATIONAL AUDIT

a.k.a. Performance Audit, Value for Money Audit, Management Audit)

- Systematically examine the City's programs, functions, and activities

- May include analyses and recommendations with respect to continuing or discontinuing a service or program

- Measure and assess performance and operation of management while focusing on key objectives

- Recommendations encourage the use of best practices while promoting public accountability, efficiency, and effectiveness

- Scope of these audits can include <u>some or all</u> of - efficiency, effectiveness, accountability, relationships, protection of assets, compliance with legislative and corporate policies, culture, organizational structure, staffing levels, technology, or span of control evaluation

FINANCIAL AUDIT

- Review of financial processes

- Examples: Cash control, accounts payable, accounts receivable, payroll, inventory controls, and investment compliance

- Designed to provide Council and management with the assurance that adequate and effective financial controls are in place in order to safeguard City assets

- May be performed by the Internal Auditor in conjunction with the External Auditors

- Control reviews or audits are also within the scope of financial audits

COMPLIANCE AUDIT

Compliance audits are smaller in scope than operational audits and are designed to review and evaluate compliance with established policies and procedures as well as any relevant statutory and/or legal requirements.

INFORMATION SYSTEMS AUDIT

- Provide assurance that the City's information technology infrastructure and computer applications contain adequate controls and security to safeguard assets and mitigate risk

- Provide assessments on overall security, controls, business continuity, and disaster recovery plans

- Post implementation audits for new system conversions

FOLLOW-UP AUDIT

Standard 2500 of the Professional Practice of Internal Auditing states that one of the primary responsibilities of professional auditors is to ensure that proposed management action plans have been effectively implemented. These are typically conducted approximately one year following the original audit.

SPECIAL INVESTIGATIONS

(a.k.a. forensic accounting or auditing)

Fraud or theft investigations are audits that usually involve an examination of specific components of an operation or a program. These audits may result from requests from Audit Committee, Council, CAO, Managers or information received from employees, vendors or citizens. Other types of investigations may include reports of inappropriate conduct or other activities by a City employee.

CONSULTING / ADVISORY SERVICES

Internal Audit also provides consulting or advisory services at the request of management. The nature and scope of the consulting engagement are subject to agreement with the client and are intended to add value by improving governance, risk management, and control processes.

INTERNAL AUDIT REPORTING PROCESS

22
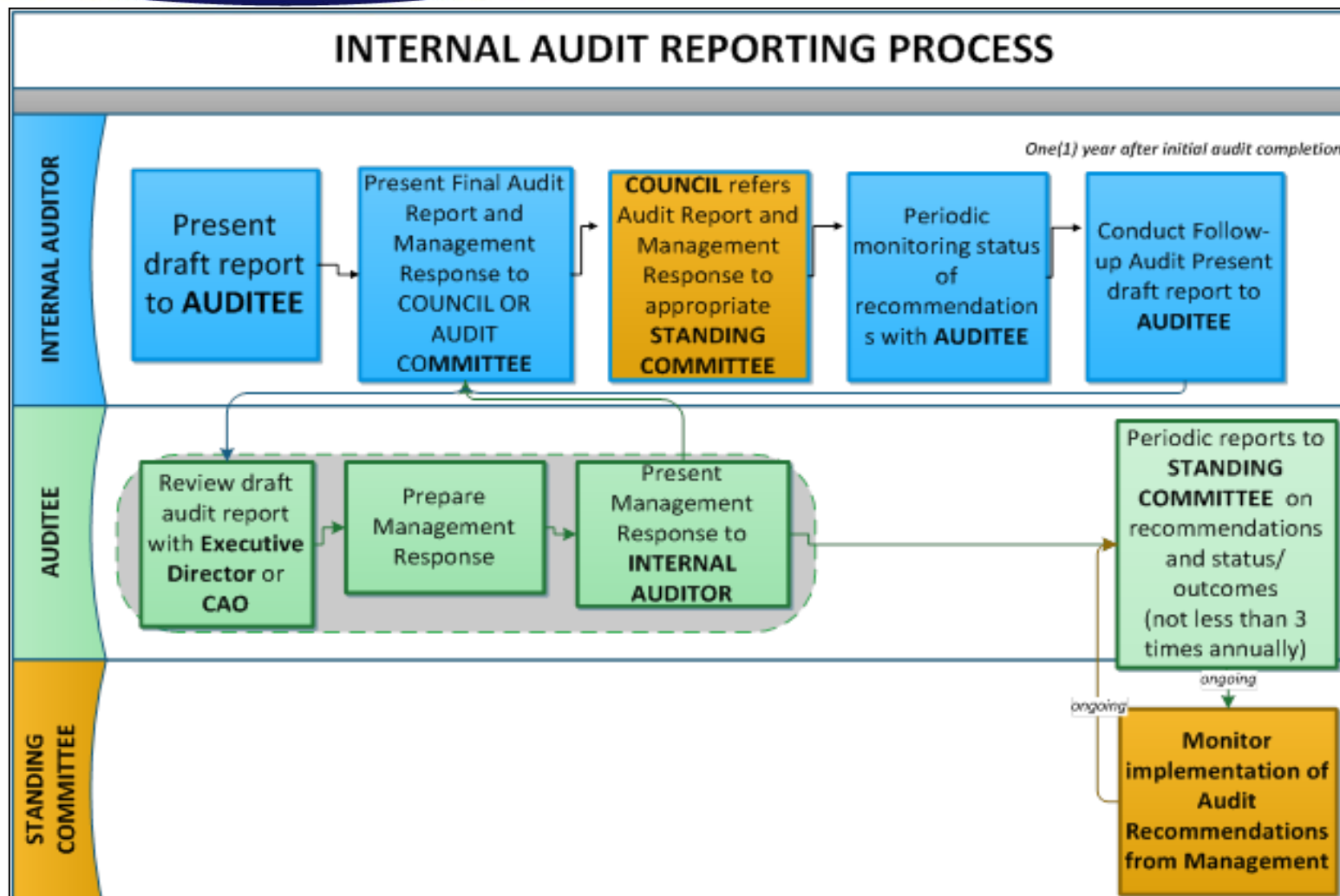
INTERNAL AUDIT CHARTER

The Internal Audit Charter defines the Mandate, Scope, Authority, Independence, Responsibility, and Reporting Structure for the internal audit function.

It is reviewed at least once during each term of Council. A copy of the Charter is included in the Audit Handbook.

End of Part 2 - Internal Audit

Questions?