



SUBJECT: Updated inherent risk assessment methodology

TO: Audit Committee

FROM: City Auditor's Office

Report Number: CA-09-19

Wards Affected: Not Applicable

File Numbers: 430-01

Date to Committee: June 5, 2019

Date to Council: June 17, 2019

Recommendation:

Approve the proposed amendments to the inherent risk assessment methodology as outlined in Appendix B of city auditor's report CA-09-19.

Purpose:

Establish new or revised policy or service standard.

An Engaging City

- Good Governance

Background and Discussion:

Audit Unit/Audit Universe

An audit unit is a part of the organization that is exposed to sufficient risk(s) that control, including audit, is appropriate. Audit units can be defined according to: business unit, service line, legal entity, regulatory requirement, processes, programs, functions, or systems; a key risk or key control; and/or a combination of all or most of the above.

The total inventory of audit units is referred to as the audit universe. The audit universe is the basis of audit planning. The current audit universe includes all services and sub-services.

Inherent Risk Assessment

The International Standards for the Professional Practice of Internal Auditing require a risk-based audit plan to assist management in ensuring significant risks are addressed. The risk assessment also supports effective use of audit resources through a targeted audit work plan.

The risk assessment methodology supports consistent measurement of inherent risk as all risk factors, criteria, attributes, and weightings are used to assess each audit unit. Each year, the audit unit's inherent risk profile is reviewed and updated by the manager/service owner. For their audit unit, the manager/service owner is asked to reflect on each criterion and select the attribute which best describes the environment or activities in which they operate. Managers/service owners are encouraged to engage supervisors and other staff in the review and update.

Inherent risk assessment is part art, part science. The art involves the judgment in determining both the relevant attribute for each criterion and a ranking for each factor. The science involves the determination of the overall inherent risk score. This score is determined through the translation of each factor's risk ranking into a pre-determined number, when multiplied by the factor's weighting, results in a score for that factor. The sum of all factor scores is the overall inherent risk score.

The inherent risk assessment methodology was established in 2009 with updates applied in 2011 and 2015.

Strategy/process

It is good practice to periodically review the audit units and risk methodologies.

Audit Universe

The current audit universe includes all services and sub-services. A review of the services/sub-services to organizational activities to corporate functions to major projects concluded that corporate functions should be included in the audit universe. Inclusion of these functions will promote a comprehensive assessment of risks and controls and offer more value to City because of breadth of coverage. Examples of corporate functions include Accounts Payable/Purchasing Card Program, Asset Management, Grant Administration, Fraud Management, Information Management, Physical Security, Privacy, Procurement, and Project Management, to name a few.

In some cases, current sub-services are, in fact, corporate functions. In these cases, risk assessment of services/sub-services will be adjusted to reduce likelihood of double counting. E.g. risk assessment of Financial Management – Transactional Services will

reflect investments and charitable donations only as Accounts Payable/Purchasing Card Program, Accounts Receivable, and GL Transactions & Accounts will be assessed as corporate functions. For information and reference, a list of the audit universe including corporate functions is included in Appendix A.

Inherent Risk Assessment

Given the last review of the inherent risk assessment was in 2015, and the decision to include corporate functions in the audit universe, this drives the need to review the risk assessment factors, criteria and attributes to ensure relevance.

Research of other municipalities and public sector agency risk assessment methodologies was performed. As well, review of publications and material from the Institute of Internal Auditors was conducted to determine latest practices.

The revisions to both the audit universe and the inherent risk assessment methodology were reviewed with a sample of managers and the Burlington Leadership Team to assess relevancy, understanding and applicability.

Summary of Proposed Amendments

Major changes to the methodology affect the factors, criteria, attributes and weighting.

1. Factor and weighting

Factors are the major categories used to characterize inherent risk. One new factor was added, and 2 factors were eliminated.

Factor		Weighting	
Current	Proposed	Current	Proposed
Complexity of Operations	Complexity of Service Delivery	30%	No change
Materiality & Susceptibility to Error/Fraud	No change	25%	No change
Public Exposure	Exposure to Scrutiny	15%	10%
Degree of Change (over last 12 months)	Degree of Change (over last 12 months and expected within next 6 months)	20%	No change
Financial Loss/Cost	Eliminate	5%	0%
Non-Compliance	Eliminate	5%	0%
	People Participation (NEW)	0%	15%

2. Criteria

Criteria are used to give guidance as to what the factor means; how the factor is to be interpreted. Changes to the criteria are identified in **bold italics** and **Text shading** indicates new criterion.

Factor (Weight)	Criteria	
	Current	Proposed
Complexity of Service Delivery (30%)	<ul style="list-style-type: none"> • Nature of technology/equipment used in service delivery (e.g. sophisticated vs. simple) • Nature of process (e.g. customized vs. routine) • Staff involved in service delivery • Nature of service delivery (e.g. decentralized vs. centralized) 	<ul style="list-style-type: none"> • Nature of technology/equipment used in service delivery (e.g. sophisticated vs. simple) • Degree of customization of process (e.g. customized vs. standardized) • Number of people involved in service delivery • Service delivery sites (e.g. multi-site/counter vs. single site/counter) • Level of exposure to hazardous activity
Materiality & Susceptibility to Error/Fraud (25%)	<ul style="list-style-type: none"> • Gross revenue (excluding recovery from capital) • Gross operating expenditures (including human resource costs and excluding one-time project costs) • Transparency/openness to scrutiny • Staffing levels • Nature of Assets Used in Service Delivery (i.e. tangible/intangible, convertibility to cash) 	<ul style="list-style-type: none"> • Gross revenue (excluding recovery from capital) • Gross operating expenditures (including human resource costs and excluding one-time project costs) • Transparency/openness to scrutiny • Extent of staff complement vacancy • Nature of Assets Used in Service Delivery (i.e. tangible/intangible, convertibility to cash)

Factor (Weight)	Criteria	
	Current	Proposed
	<ul style="list-style-type: none"> • Involvement in known risk areas of misconduct • Dollar value of daily cash deposits 	<ul style="list-style-type: none"> • Involvement in known risk areas of misconduct • Dollar value of daily cash deposits
Exposure to Scrutiny (10%)	<ul style="list-style-type: none"> • Public/customer reaction 	<ul style="list-style-type: none"> • Degree of public/external customer involvement • Degree of internal customer involvement • History of media attention (e.g. newspapers, blogs, op eds, etc.) • Employee Base Involved
Degree of Change (20%) (over last 12 months and expected within next 6 months)	<ul style="list-style-type: none"> • Staff turnover (due to reasons such as retirement, leaves of absence, job rotations, etc.) • Changes to service strategy and/or process (manual and/or automated) 	<ul style="list-style-type: none"> • Staff Turnover - Moved to People Participation factor • Changes to service and/or processes • Technology/equipment change
People Participation (15%)		<ul style="list-style-type: none"> • Staff turnover (due to reasons such as retirement, leaves of absence, job rotations, etc.) • Staff performing “must do” activity(ies) • Difficulty in filling positions (beyond normal recruitment timing)

Factor (Weight)	Criteria	
	Current	Proposed
		<i>Difficulty in attracting candidates</i>

3. Attributes

Attributes are statements to describe certain features or characteristics of the environment. Each attribute is aligned to a risk ranking and each risk ranking is assigned a pre-determined number. New attributes established for each of the 9 new criteria are provided in the following tables categorized by the factor and criterion to which each relates.

Complexity of Service Delivery:

- Level of exposure to hazardous activity

Risk Ranking (Pre-determined Number)				
Very High (100)	High (75)	Moderate (50)	Low (25)	Very Low (1)
Work involves daily exposure to high hazard activity (e.g. use of heavy machinery/ small equipment, working at heights, chemical handling, working in traffic, etc.)	Work involves frequent exposure to high hazard activity (e.g. use of heavy machinery/ small equipment, working at heights, chemical handling, working in traffic, etc.)	Work involves repeated exposure to manual labour (e.g. lifting, pushing, pulling, digging, etc.)	Work involves daily exposure to low hazard activity (e.g. use of computers, desk work, repetitive movement, etc.)	Work involves limited exposure to low hazard activity (e.g. use of computers, desk work, repetitive movement, etc.)

Exposure to Scrutiny:

- Degree of public/external customer involvement

Risk Ranking (Pre-determined Number)				
Very High (100)	High (75)	Moderate (50)	Low (25)	Very Low (1)
Everyday direct involvement of public/external customers	Frequent direct involvement of public/external customers	Periodic direct involvement of public/external customers	Infrequent direct involvement of public/external customers	Rare direct involvement of public/external customers

- Degree of internal customer involvement

Risk Ranking (Pre-determined Number)				
Very High (100)	High (75)	Moderate (50)	Low (25)	Very Low (1)
Everyday direct involvement of internal customers	Frequent direct involvement of internal customers	Periodic direct involvement of internal customers	Infrequent direct involvement of internal customers	Rare direct involvement of internal customers

- History of media attention (e.g. newspapers, blogs, op eds, etc.)

Risk Ranking (Pre-determined Number)				
Very High (100)	High (75)	Moderate (50)	Low (25)	Very Low (1)
Subject of regular and sustained media attention	Subject of frequent media attention	Subject of minimal or short-lived media attention	Subject of infrequent media attention	Never been subject of media attention

- Employee Base Involved

Risk Ranking (Pre-determined Number)				
Very High (100)	High (75)	Moderate (50)	Low (25)	Very Low (1)
Every employee involved	More than three-quarters of employees involved	Half of employees involved	More than one-quarter of employees involved	Less than one-quarter or one group of employees involved

Degree of Change:

- Technology/equipment change

Risk Ranking (Pre-determined Number)				
Very High (100)	High (75)	Moderate (50)	Low (25)	Very Low (1)
Implemented new software/hardware/equipment to support service	Major upgrade or update to <u>all</u> software/hardware/equipment to support service	Major upgrade or update to <u>some</u> software/hardware/equipment to support service	Minor upgrade or update to all or some software/hardware/equipment to support service	No changes to software/hardware/equipment to support service

People Participation:

- Staff performing “must do” activity(ies)

Risk Ranking (Pre-determined Number)				
Very High (100)	High (75)	Moderate (50)	Low (25)	Very Low (1)
Only one person knows how “must do” activity(ies) are performed. i.e. <u>OR</u> key person dependency	2 people know how “must do” activity(ies) are performed	3 people know how “must do” activity(ies) are performed	4 people know how “must do” activity(ies) are performed	5 or more people know how “must do” activity(ies) are performed

- Difficulty in filling positions (beyond normal recruitment timing)

Risk Ranking (Pre-determined Number)				
Very High (100)	High (75)	Moderate (50)	Low (25)	Very Low (1)
Takes 8 or more months longer	Takes 6 – 7 months longer	Takes 4 – 5 months longer	Takes 2 – 3 months longer	Takes less than 1 month longer

- Difficulty in attracting candidates

Risk Ranking (Pre-determined Number)				
Very High (100)	High (75)	Moderate (50)	Low (25)	Very Low (1)
Had to go back to market > 2 times after original recruitment <u>OR</u> > 2 offers made and declined	Had to go back to market 2 times after original recruitment <u>OR</u> 2 offers made and declined	Had to go back to market 1 time after original recruitment <u>AND</u> 1 offer made and declined	Had to go back to market 1 time after original recruitment <u>OR</u> 1 offer made and declined	Filled position from original recruitment <u>OR</u> no offers declined

A complete version of the updated inherent risk assessment methodology is available in Appendix B.

Next Steps

The updated inherent risk assessment will be applied to each audit unit to create an inherent risk profile and each audit unit risk profile will be updated annually. As an example, Internal Audit’s risk profile (contained in Appendix C) demonstrates how the inherent risk assessment is applied.

An annual work plan and a rolling 3-year work plan (with a base of 2020) will be developed in consultation with service owners and senior management based on:

- Higher inherent risk audit units subject to audit earlier than lower inherent risk audit units.
- Audit units related to the same service or delivered by the same staff will be subject to internal audit in different years.
- Other factors as required.

As per existing practice, the City Auditor will seek approval of the annual audit work plan from the Audit Committee.

Financial Matters:

Not applicable.

Connections:

Not applicable.

Public Engagement Matters:

Not applicable.

Conclusion:

The audit universe is a practical way to categorize the operations of the City and the inherent risk methodology is a key component in developing a risk-based audit work plan. The proposed amendments to the inherent risk assessment bring the methodology up to date and tailor it to the City and its operating environment.

Respectfully submitted,

Sheila M. Jones, CIA, CFE, CGAP, CRMA, CCSA

City Auditor

905-335-7600 ext. 7872

Appendices:

- A. CA-09-19 Appendix A: City of Burlington Audit Universe
- B. CA-09-19 Appendix B: Inherent Risk Assessment Methodology for City of Burlington
- C. CA-09-19 Appendix C: Example of Inherent Risk Assessment – Internal Audit Risk Profile

Report Approval:

All reports are reviewed and/or approved by Department Director, Director of Finance and Director of Legal. Final approval is by the City Manager.