Performance Audit of Risk Management Processes

May 10, 2017
Draft Report

Greater | Grand Sudbury
www.greatersudbury.ca
AUDITOR GENERAL

SUMMARY

Objectives

The objectives of this performance audit were to:

- Assess the effectiveness of current risk management processes in the City; and
- Recommend improvements where necessary.

Scope

The scope of this performance audit included a review of current risk management processes within each of the divisions of the City as well as Economic Development and Planning Services.

Report Highlights

A range of different approaches are used to manage risks within different divisions within the City. While some employ formal and systematic risk management practices with great precision, others employ less formal practices which are susceptible to errors. These varied approaches have resulted in inconsistent management of and reporting on significant risks to Council in the past.

In recent months, a more focused approach has been taken to ensure that significant risks are identified and reported to Council on a timely basis. To augment this approach, it is recommended that:

- A formal risk management policy be developed to codify risk management terms and to clarify responsibilities for risk management;

- An enterprise risk management (ERM) process be developed and implemented to standardize the processes for the identification, assessment, and mitigation of risks;

- An annual report on significant non-legal risks be prepared for Council in conjunction with the annual budget and business plans; and

- The ERM implementation plan be tailored to the readiness of the City to adopt these standardized processes and to integrate them with other management processes.

Audit Standards

We conducted our audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we adequately plan for the audit; properly supervise audit staff; obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions; and prepare audit documentation related to the planning, conducting, and reporting for each audit. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit.

For further information regarding this report, please contact Ron Foster at extension 4402 or via email at ron.foster@greatersudbury.ca

Finding 1:

According to the CSA Standards, risk management is the identification, assessment, and treatment of "risks" that may affect an organization, business or municipality, negatively, including those which can occur through accidents, disasters, natural causes, legal or financial liabilities or opportunities, or positively, such as new technologies, business ventures or continual improvement.

A risk management policy has not been developed to define risk management terms and responsibilities for risk management within the City. As a result, responsibilities for risk management are not clear.

Recommendation 1:

A formal risk management policy should be developed to codify risk management terms and to clarify responsibilities for risk management.

Management's Response and Action Plan:

We agree. The recommended policy will be developed and presented to Council by the Chief Administrative Officer for approval before the end of the third quarter.

Finding 2:

A risk management process has not been developed to identify a standard approach for risk identification assessment, mitigation and reporting. As a result, responsibilities for risk management are not clear and different approaches to risk management have been adopted within the City.

Recommendation 2:

A formal risk management process should be developed to standardize enterprise risk management (ERM) processes in the City. The ERM process encompasses risk identification, assessment, mitigation and reporting processes to ensure that significant risks are managed effectively. When reporting on implementation progress, the criteria within Attachment 1 should be referenced. Attachment 2 illustrates the ISO 31000 risk management process which is a component of CSA 31000 which is Canada's national standard for risk management.

Management's Response and Action Plan:

We agree. Management's view is the capacity to understand risk begins with a clear understanding about the services, work processes and projects staff are responsible for delivering. Starting in 2017, an enterprise-wide process and related technology applications will be introduced to facilitate the creation of a "common language" describing the corporation's programs and services. In parallel, Greater Sudbury's participation in the Municipal Benchmarking Network Canada will provide important contextual data to help identify both the factors that influence performance and, where Greater Sudbury may be an "outlier", prompt consideration of whether some change may be needed. These will inform the Executive Leadership Team's judgment in discussions designed to identify and assess risks, which are anticipated to occur as part of the annual business planning process.

Finding 3:

Other than legal risks, Council does not receive an annual report on the major risks faced by the City, how they are currently being managed and what steps, if any, are recommended to further mitigate them.

Recommendation 3:

To complement the periodic reports to Council on significant legal matters, an annual report on non-legal risks should be prepared for Council in conjunction with the annual budget and business plans. Attachment 3 provides an example of an annual report that identified key corporate risks in 2015 in the City of Saskatoon.

Management's Response and Action Plan:

We agree. Discussions about major risks are likely most effective at the start of the annual business planning process. Beginning in 2018, staff will incorporate the recommended report into a meeting about 2019 budget directions.

Finding 4:

The City has a moderate level of readiness to implement ERM processes as members of the Executive Leadership Team are already employing various risk management techniques within their daily management activities. Attachment 4 sets out the City's overall readiness to implement ERM processes. Attachment 5 provides a suggested implementation plan for 2017 to 2019 that can be tailored to the City's needs and circumstances.

Recommendation 4:

An implementation plan that is tailored to the readiness of the City to adopt standardized risk management processes and to integrate them with other management processes should be developed.

Management's Response and Action Plan:

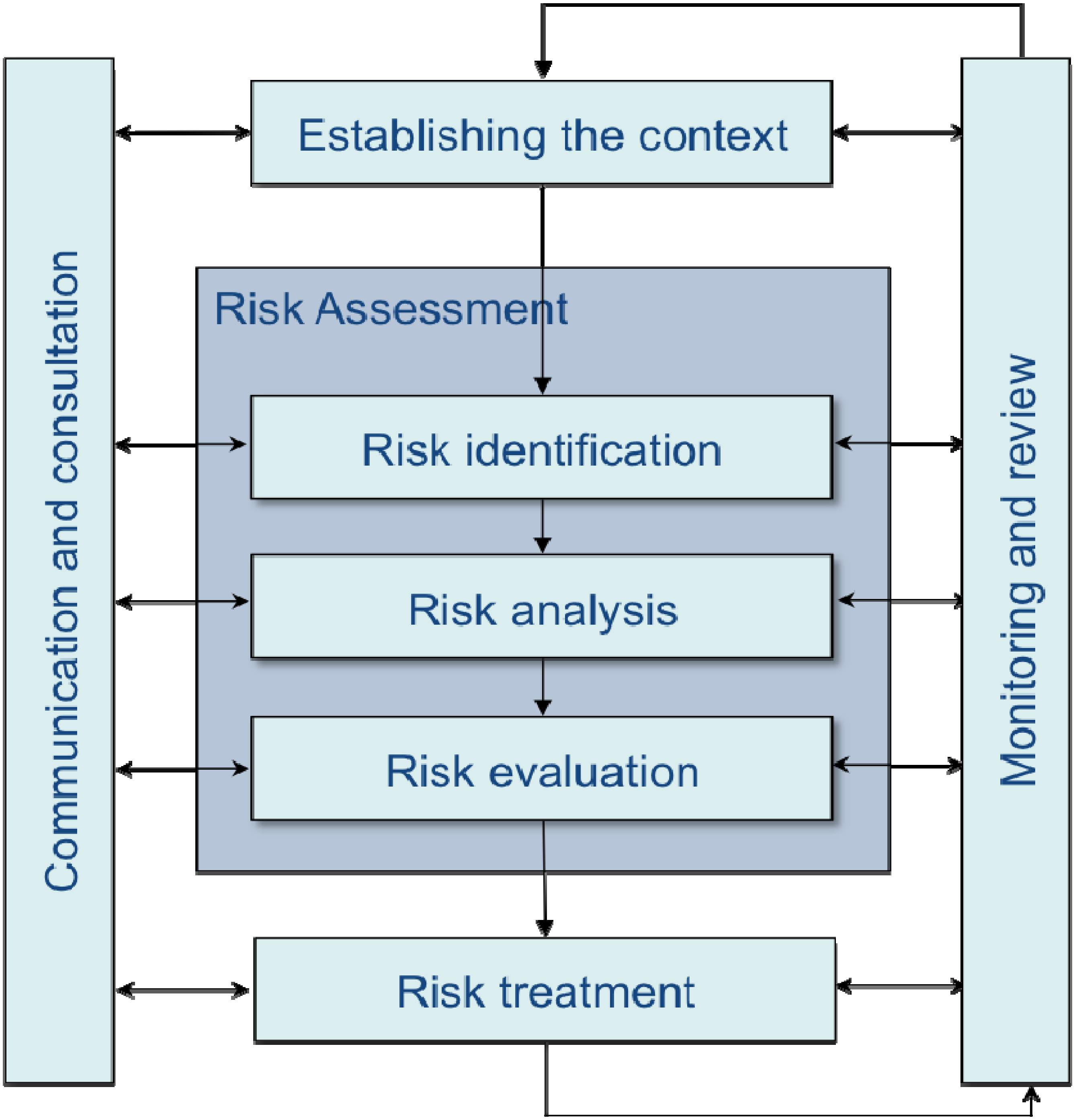
We agree. The suggested implementation plan will be developed and included in the recommended report to Council about a risk management policy, anticipated to be published in the third quarter.

Attachment 1: ERM Maturity Assessment Criteria

Attribute	Leading Practice
Continual Improvement	Formal processes are in place requiring periodic management evaluation of risk mitigation strategies and related internal controls.
	Risk management process is subject to periodic review by internal audit or independent third party.
Full Accountability	The ERM Framework and/or ERM Policy are in place. The framework includes key elements such as the ERM Philosophy & Principles, Organizational Structure & Accountabilities, Corporate Wide Risk Definitions, and Risk Management Processes and Reporting.
	Accountabilities for risk management and risk ownership are clearly established and communicated.
Decision Making	Corporate risk policies have been established to manage specific key risk exposures.
	Executive Management actively engage in the assessment of risk as part of formal decision making processes.
	Risk assessment occurs on a regular basis. Risk analysis is formally integrated into strategic and operational planning at both the corporate and business unit levels. Risk assessments are conducted for key investment opportunities or organizational change events (e.g., new initiatives and services, systems implementation and major projects).
	Appropriate risk assessment tools have been developed and are being used – e.g., common risk vocabulary, formal risk assessment criteria and risk classification scheme.
	Risk mitigation strategies are designed and implemented based on a prioritization of risks.
Continual Communications	The organizational risk culture – including risk tolerance – is robust and well understood.
	An enterprise-wide risk profile exists that reflects risk prioritization and is accompanied by detailed discussion at the management and Board levels.
Governance	Council has ultimate oversight of risk management activities.

The above criteria are taken from CSA 31000 which is Canada's national standard for risk management. This standard incorporates the ISO 31000 international risk management standard.

Attachment 2: ISO 31000 Risk Management Process



Attachment 3: Key Corporate Risks from City of Saskatoon's 2015 Report

Tier	Risk Type		Risk Ranking
1	FIN	The lack of regional growth plan that includes all of the City's neighbors could restrict the city's growth in the future	High
1	FIN	There may be limitations on non-property tax revenue options and taxing powers, resulting in an over-reliance on property tax.	High
1	InfOp	The current investment in infrastructure renewal and maintenance over the last ten years may not have been adequate. Some areas need fresh infrastructure investment: Roads	High
1	InfOp	While making capital investment decisions, adequate funding for asset lifecycle costs may not be getting identified.	High
1	InfOp	The City carries the risk of over/under investing within its future infrastructure and not being aligned to economic scenario within the City/Province.	High
1	InfOp	The City may not be delivering expected level of service to citizens or internal stakeholders: Transit	High
1	InfOp	The current investment in infrastructure renewal and maintenance over the last ten years may not have been adequate. Some areas need fresh infrastructure investment: Transit	High
1	InfOp	The City may not be delivering expected level of service to citizens or internal stakeholders: IT	High
1	InfOp	The City may not have adequate business continuity planning and or emergency preparedness in place.	High
1	IT	Some IT systems and hardware may be outdated resulting in inability to meet business needs.	High

Attachment 4: Risk Management Readiness

	Risk Naive	**Risk Aware**	**Risks Identified**	**Risks Managed**	**Risks Optimized**
Use of Standards, Policies, Tools & Techniques	No use	Awareness	Some utilization	Moderate utilization	Full utilization
Knowledge of Risk Management Discipline	Little	Awareness	Some knowledge	Sound knowledge	High Degree
Risk Management Activities Undertaken	No formal activities	Some activities	Framework adopted but not fully implemented	Formal program in place	Risk management embedded in decision-making of organization
Awareness of Benefits and Value of Risk Management	Uncertain	Awareness of need for common processes	Awareness of need for common processes and potential benefits	Deployment across the organization	Risk management into business planning and strategic thinking

The current levels of readiness are shaded in the above table.

Attachment 5 – Suggested Implementation Plan

KEY STEPS FOR 2017	Target
1. Establish governance process	Q1 2017
2. Develop vision, principles, framework, process and policy	Q2 2017
3. Establish the scope of the program	Q2 2017
4. Develop detailed implementation plan	Q2 2017
5. Develop training program	Q2 2017
6. Obtain support from Executive Leadership Team	Q2 2017
7. Obtain approval from Audit Committee and Council	Q2 2017
8. Launch program	Q3 2017
9. Deliver training to Audit Committee	Q3 2017
10. Deliver training to Executive Leadership Team (ELT)	Q3 2017
11. Deliver training to directors within each division	Q3 2017
12. Identify and assess strategic risks & mitigation plans for each division	Q3 2017
13. Review strategic risks & mitigation plans with ELT	Q3 2017
14. Prepare report for Audit Committee on strategic risks	Q4 2017
15. Address strategic risks within business plans for 2018	Q4 2017
16. Address strategic risks within budgets for 2018	Q4 2017

KEY STEPS FOR 2018	Target
1. Deliver workshops to Infrastructure Department	Jan 2018
2. Update strategic risks & mitigation plans for Infrastructure Department	Feb 2018
3. Deliver workshops to Community Services Department	Mar 2018
4. Update strategic risks & mitigation plans for Community Services Department	Apr 2018
5. Deliver workshops to Corporate Services Department	May 2018
6. Update strategic risks & mitigation plans for Corporate Services Department	June 2018
7. Update strategic risks & mitigation plans for EMS Department	July 2018
8. Update corporate risk register and mitigation plans with ELT	Aug 2018
9. Update business plans and budgets for 2019 to address strategic risks	Oct 2018
10. Develop continuous improvement plan with ELT	Nov 2018
11. Prepare report for Audit Committee and Council	Dec 2018

KEY STEPS FOR 2019	Target
1. Report to Audit Committee and Council on ERM program	Jan 2019
2. Deliver workshops to Infrastructure Department	Jan 2019
3. Update strategic risks & mitigation plans for Infrastructure Department	Feb 2019
4. Deliver workshops to Community Services Department	Apr 2019
5. Update strategic risks & mitigation plans for Community Services Department	May 2019
5. Deliver workshops to Corporate Services Department	June 2019
6. Update strategic risks & mitigation plans for Corporate Services Department	July 2019
7. Update strategic risks & mitigation plans for EMS Department	Aug 2019
8. Update corporate risk register and mitigation plans with ELT	Sept 2019
9. Update business plans and budgets for 2012 to address strategic risks	Oct 2019
10. Prepare report on strategic risks for Audit Committee and Council	Dec 2019