IT RISK MANAGEMENT

IT Overview – Facts & Figures

The Information Technology (IT) business unit at The City of Calgary is one of the largest IT shops in western Canada. City IT provides over 400 enterprise and business systems in support of 30 lines of City business by connecting over 15,000 employees at over 325 sites to serve over 1.1 million citizens. Information Technology manages over $350 million in technology assets including two data centres, first responder's radio system, the municipal area network, and provides corporate telecommunications including call centre technologies. Service and support is delivered in-house and through managed external providers. In 2012 alone, IT delivered over $28 million of business technology related projects.

Attachment 2 **-** IT Facts & Figures, provides some contextual information to assist Audit Committee members with regard to annual operating and capital budgets, assets, employees, number and types of business and enterprise systems. Also, worth noting with respect to governance, a degree of information technology is managed within other City business units; e.g. Supervisory Control and Data Acquisition (SCADA) systems in UEP (water treatment), Transportation (traffic lights) and Public Safety (911).

Information Technology's business philosophy from an organizational perspective is that we are leading edge, not bleeding edge. We are risk adverse (e.g. Municipal Government), are concerned with protection of privacy and safety, as well as ensuring the policy of Triple Bottom Line is adhered to.

Principle Vulnerabilities

Information Technology (IT) follows Council's policies (Attachment 3 -Policies) including the Integrated Risk Management (IRM) policy and framework by ensuring that risk management is integrated into strategic business planning as well as day-to-day operations. Information Technology continues to mature in this regard and to date has developed a risk profile and registry to manage and assess risks. Using the IRM process, business unit risk can be elevated to Department level and then to the Corporate Registry if deemed significant. Business plan strategies and outcomes are reviewed quarterly. Risk identification, management and monitoring stemming from operations, project work, service delivery, etc., is handled through a number of ways within the business unit (see next section).

Attachment 4 - IT Risk Profile identifies IT's risks by category, their assessment in terms of likelihood and impact, the management strategy to mitigate the risks and the position accountable. The majority of IT's risks are under the "Delivery of Service" category related to infrastructure failure, information management and external factors, as well as the "Financial" category related to costs.

From the Chief Information Technology Officer's perspective, the top risks to manage are cyber attacks, system complexity, information management and most recently, potential labour action and increased software licensing costs that may result due the declining value of the CDN to USD dollar.

IT RISK MANAGEMENT

Recent activity related to risk management are the internal audit responses underway (see Note #1), changes being considered to the IT Governance model (Technology Investment Governance audit – see Note #1, AC2013-0085), addressing an external security assessment together with Corporate Security and the development of a corporate information management program.

People & Processes

In accordance with the IRM policy, the responsibility for identifying, mitigating and monitoring risks first is with the Chief Information Technology Office, the IT Management team, business planners, Dept ID owners and finally with all employees.

In addition to Council policies, including IRM, IT also identifies, manages and monitors risk through governance, best practise and processes, external benchmarking and staying current with industry trends, for example:

- Internal audits (see Note # 1 below)
- External audits (Deloitte)
- Maturity assessments (Information Technology Infrastructure Library (ITIL), Asset Management, Enterprise Architecture, etc.)
- External benchmarking (Micromation, Ontario Municipal Benchmarking Initiative - OMBI)
- Security/Operational meetings (threat bulletins, security patches)
- External consulting (penetration tests, assessments – e.g. Ethier, Securis)
- ITIL incident management, problem management process (see Note #2 below)
- Change Approval Board
- IT Project Management Office & Corporate Project Management Framework
- Asset Management Plan and Infrastructure Status Reporting
- Software Solutions Methodology (SSM) – Includes quality assurance/testing
- Governance (ALT/CTC/Project Board/Steering Committees) - See Attachment 5 & Note #3 below
- Information Management (Information Security Classification - ISC)
- Corporate Policies, Principles & Guidelines – See Attachment 3

Note # 1 - Internal audits in progress include:

AUDIT	REPORT #	DATE
Cellular Phone & Mobile Device	AC2012-0121	March 14, 2012
Technology Investment Governance	AC2013-0085	Dec 12, 2012
IT Network Access Security	AC2013-0447	May 7, 2013
PeopleSoft HCM Application Security	AC2013-0446	May 8, 2013

AUDIT	REPORT #	DATE
IT Hardware Inventory Management	AC2013-0522	June 7, 2013

Server Virtualization Audit is in progress

Note # 2 - The Information Technology Infrastructure Library (ITIL) is a globally recognized collection of best practices for information technology service management that focuses on aligning IT services with the needs of business. ITIL describes processes, procedures, tasks and checklists that are not organization specific, used by an organization for establishing integration with the organization's strategy, delivering value and maintaining a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement and measure. It is used to demonstrate compliance and to measure improvement.

Risks are addressed within several processes in ITIL; there is, however, no dedicated Risk Management process. ITIL calls for "coordinated risk assessment exercises."

Attachment 6 - identifies the ITIL Process Owner and Process Manager accountable for the various processes within the process domains.

Note # 3 – The IT Governance model is currently being revised with Corporate Technology Committee (CTC) in accordance with recommendations from the Technology Investment Governance audit (see Note #1, AC2013-0085). The changes under development include a distributed governance approach for business unit accountability (PPM processes), integration with the Corporate Technology Plan and enterprise architecture and security touch points.

Trends and Case Studies

The following information is intended to be helpful to Audit Committee members as to what trends are coming as well as lessons learned from past events (Case Studies).

Some key trends and challenges to be aware of include mobility, Bring Your Own Computer (BYOC), Cloud Computing, 'Internet of Things' and e-Government. Other concerns include mergers and acquisitions (e.g. Blackberry) and consumer driven expectations (Drop Box) challenging enterprises to maintain controls.

In addition to maintaining the City Technology Plan, IT engages with industry in a number of ways: subscription to online research and consulting from industry analysts, active participants in the Canadian Municipal Information Systems Association (MISA), the Canadian Cloud Council, Canadian Information Technology Professionals (CIPS), the Calgary CIO roundtable and many other forums.

Industry trends affecting The City:

- Mobile workforce/reduced real estate costs – Tomorrow's Workplace (Program underway)
- Bring Your Own Computer (BYOC) - research and policy development underway
- Cloud computing - Cloud strategy in place, and now carefully consuming some services
- "e-Government movement;" citizen expect transparency, eServices, participatory government – currently developing go forward Digital Strategy
- "Internet of Things" and how they relate to:
    - Cloud computing
    - Remote sensing and controls
    - Cyber Security
    - Outages we have experienced (Case Study)
- Business Technology; shifting to more business unit control and autonomy of IT, requires:
    - Distributed/Federated governance
    - Guardrails/Rules

Case Studies

Information Technology has experienced five crisis events since June 30, 2011 including one major incident. Post mortems following these events have provided useful information to guide IT in the future. Examples as follow:

Flood - June 20, 2013 – lessons learned (full debrief collected by CEMA):

- Ability to communicate is key in any event
- Crisis Management Plan is exercised regularly
- Critical systems are resilient
- Insurance claims, made easier with good asset information
- Ability for staff to work remotely – not tied to physical location

Shaw Court Fire – July 11, 2012 – lessons learned:

- Complexity – who knew City could be affected
- Why Cloud based services are a concern
- Need to understand your service provision from end to end (external resilience)
- Don't expect external organizations to do the communication to your stakeholders

Internal change error – January 22, 2014 – lessons learned:

- No change order used for a non-production
- Now require a second administrator to check when making any change to Virtual Storage environment

In general, deeper knowledge with respect to business resilience is required for any third party service that is part of the eco-system of an important service. This is especially important to consider when moving to a Cloud or internet-based service. Public safety systems require special consideration in this regard.

Physical access to critical infrastructure needs to be tightly controlled. Access points often need to be shared with other agencies, partners or providers. Having good access and change control mechanisms are challenges, examples include access to radio towers and fibre optic network.