# IT Risk Profile

| RISK CATEGORY | RISK | ASSESSMENT | | MANAGEMENT STRATEGY | | ACCOUNTABLE |
|---|---|---|---|---|---|---|
| | | LIKELI HOOD | IMPACT | REDUCE LIKELIHOOD | REDUCE IMPACT | |
| | **Infrastructure failure** | | | | | |
| Delivery of Service | Disaster or loss (Flood, Shaw Court Fire, Telus service interruption) | MED | HIGH | • New data centre at Emergency Operations Centre reduces likelihood of event affecting core services;<br>• New network design and deployment provides resilience to protect against any single point of network failure. | • Resilience by way of redundancy and fail-over mechanisms into infrastructure;<br>• Protect Corporate data through back-ups and off-site storage;<br>• IT works with Internal Audit to review business continuity in audit plans;<br>• Detailed asset information and systems configurations;<br>• Suitable insurance coverage | Manager, Operations |
| | Business & Enterprise System Failures (911-Public Safety System, etc.) (email, PeopleSoft Financial & HR Payroll) | LOW | HIGH | • Resilient system design;<br>• Eliminate single points of failure;<br>• Project Mgmt methodology includes risk assessment process;<br>• Systems are developed according to Software Solutions methodology;<br>• Strict change management controls;<br>• Appropriate vendor service and support level agreements. | • Manual back-up procedures;<br>• Full data back-ups and keep copies offsite;<br>• Third party resilience plans;<br>• Detailed asset information and systems configurations;<br>• IT Crisis Management process. | Manager, Application Support |
| | Failure/Interruption of third party providers / services - especially important moving to Public Safety Systems. | MED | MED | • Detailed understanding of third party resilience and disaster recovery plans;<br>• Include in risk assessment of any Cloud-based services deployed. | • Build out City network to connect first responder locations;<br>• Communication protocols deployed. | Manager, Operations Manager, Innovation &Collaboration |
| | **Information Management** | | | | | |
| | Volume of data impedes access, recovery | HIGH | HIGH | • Implementation of Information Governance and related Information Management practices will define key roles in the business units allowing them to establish good information and records management practices in their daily operations. | • Implementation of Enterprise Content Management (ECM) environment will reduce storage needs, improved productivity and ability to provide quality customer service;<br>• Information sharing will eliminate need to create multiple copies and recreate content;<br>• Automated disposition reduces legal risk, every action fully audited;<br>• Faster, easier access to content and improved search capability;<br>• Staff will be able to access their information anytime, anywhere, from any device. | Manager, Innovation &Collaboration |
| | Exposure of information (access, intentional damage, accidental loss, device loss, privacy breach – Payment Card Industry) | MED | HIGH | • Conduct Privacy Impact Assessments for publishing external data and when assessing outsourced services;<br>• Assess other categories beyond personal information (Intellectual Property, Information Security Classification (ISC) higher codes) and manage risk accordingly;<br>• Payment Card Industry (PCI) compliance;<br>• IT & Corporate Security conduct periodic risk assessments;<br>• Security awareness training | • Mobile devices have no sensitive information exposed and limited access to enterprise;<br>• Full data back-ups and keep copies offsite;<br>• Develop and deploy Information Management program. | Manager, Operations Manager, Innovation & Collaboration Manager, Corp Security |

# IT Risk Profile

| RISK CATEGORY | RISK | ASSESSMENT | | MANAGEMENT STRATEGY | | ACCOUNTABLE |
|---|---|---|---|---|---|---|
| | | LIKELI HOOD | IMPACT | REDUCE LIKELIHOOD | REDUCE IMPACT | |
| Delivery of Service | | MED | HIGH | <ul><li>provided to all new IT employees and contractors as part of orientation;</li><li>Employees with above normal access take regular training on security access privileges;</li><li>Two-factor security/access.</li></ul> | | |
| | **External** | | | | | |
| | Cyber attack (Wilful attack on public infrastructure; public safety, transportation, water treatment, etc.) | MED | HIGH | <ul><li>Research and education to have a better understanding of exposure and likelihood;</li><li>Conduct deeper expert assessment to understand likelihood;</li><li>Monitor industry bulletins and warnings.</li><li>Protect physical access points;</li><li>Cyber security - transfer of IT Security to Law Corporate Security in Q2 2012 which provides: greater scope of skills and knowledge to protect public infrastructure and a single point of contact on security issues for more rapid responses;</li><li>Testing of internet-related vulnerabilities is a mandatory component for any external facing application.</li></ul> | <ul><li>Education for affected business units;</li><li>Corporate Disaster Recovery Plan;</li><li>Full data back-ups and keep copies offsite;</li><li>Mitigate based on exposure findings.</li></ul> | Manager, Corp Security Manager, Operations |
| | **Other** | | | | | |
| | Inadequate system controls | MED | HIGH | <ul><li>Conduct annual internal and external audits of systems risk and controls;</li><li>Access audit logs regularly reviewed;</li><li>Monthly vulnerability scans are completed on internal servers and results are communicated to appropriate operational area.</li></ul> | <ul><li>City Auditor's Office conducts periodic risks and control audits of IT.</li></ul> | CITO |
| | Vendors/third parties. merger and acquisition or insolvency - Blackberry | LOW | MED | <ul><li>Monitor industry news;</li><li>Approved vendor list in procurement process.</li></ul> | <ul><li>Alternate/additional service providers and suppliers for all critical infrastructure.</li></ul> | CITO |
| | Disaster Recovery plan | MED | HIGH | <ul><li>Review and update IT Disaster Recovery Plan;</li><li>Testing IT Disaster Recovery Plan;</li><li>Alignment with Corporate Disaster Recovery Plan.</li></ul> | <ul><li>IT Crisis management;</li><li>Build out alternative Disaster Recovery site.</li></ul> | Manager, Operations |
| Strengthen the Workplace | Staff availability (not enough to meet demands, not right skill sets, Labour action, attrition rates, demographics) | MED | HIGH | <ul><li>Supplement resources with limited term staff or contractors with right skill sets;</li><li>Organization realignment;</li><li>Review workforce measures and statistics.</li></ul> | <ul><li>Deploy LABC Plans;</li><li>Continue to align with HR Strategy and work plan by aligning staff to work on projects based on their skill sets and career dialogues;</li><li>Increase retention and attraction;</li><li>Market analysis;</li><li>Succession planning;</li><li>Entry level positions and summer/co-op opportunities being developed as part of IT business plan.</li></ul> | CITO |
| Legal Compliance | Unstructured data risk - FOIP response, eDiscovery | MED | MED | <ul><li>Information Security Classification (ISC), Records Management policy communicated/training, email campaign.</li></ul> | <ul><li>Develop and deploy Information Management Program, including ISC – information security classification applied.</li></ul> | Manager, Innovation &Collaboration |

# IT Risk Profile

| RISK CATEGORY | RISK | ASSESSMENT | | MANAGEMENT STRATEGY | | ACCOUNTABLE |
|---|---|---|---|---|---|---|
| | | LIKELIHOOD | IMPACT | REDUCE LIKELIHOOD | REDUCE IMPACT | |
| Reputation / Trust | Confidential, sensitive information exposed. | LOW | MED | • See Information Management Risks. | • See Information Management Risks. | |
| Financial | Software licensing non- compliance | LOW | MED | • Asset management database up to date;<br>• Vendor audits. | • Periodic license discovery / reconciliation with asset inventory. | Manager, Operations |
| | USD/CDN $ exchange | HIGH | MED | • Contingency plans;<br>• Budget adjustment. | • Budget adjustment. | CITO |
| | ROI not captured or benefits delivered | MED | MED | • Detailed business case and governance review;<br>• Project Portfolio Management . | • Response to Governance Audit, recommendations to ALT;<br>• Project Portfolio Management | CITO |
| | Growth – increasing gap in infrastructure lifecycle replacement. | MED | MED | • Communicate gap annually and accurately;<br>• Investigate Cloud alternatives to move cost to operating budget/recovery. | • Capital budget submission reflects infrastructure gap. | CITO |
| | Intellectual Property loss | LOW | MED | • See Information Management Risks. | • See Information Management Risks. | |
| | Complexity – exhibits itself in cost of upgrades, enhancements and integration with other systems. | MED | MED | • Systems configuration maps;<br>• Services Orientated Architecture (SOA); | • Response to Governance Audit, recommendations to ALT. | CITO |
| | High software costs relative to other organizations (indicated by benchmarking) | HIGH | MED | • Aggressive vendor negotiations;<br>• Licensing data from Asset Management system accurate;<br>• Usage statements to business clients;<br>• Leverage enterprise investment through Corporate governance. | • Reduce size and cost of Software Stack through business strategies and actions - OPTIC program, Open Source opportunities, Cloud Strategy. | Manager, Operations |