Audit of Information Technology Governance Processes

Presented To:	Audit Committee
Meeting Date:	March 26, 2024
Type:	Routine Management Reports
Prepared by:	Ron Foster Auditor General
Recommended by:	Auditor General

Report Summary

The report provides a recommendation regarding the results of the Auditor General's Audit of the City's Information Technology Governance Processes.

Resolution

THAT the City of Greater Sudbury approves the recommendations as outlined in the report entitled "Audit of Information Technology Governance Processes" from the Auditor General, presented at the Audit Committee meeting on March 26, 2024.

Relationship to the Strategic Plan, Health Impact Assessment and Community Energy & Emissions Plan (CEEP)

This report supports the strategic goal of asset management and service excellence in planning for sustainable infrastructure that demonstrates a willingness to plan, implement and innovate in accordance with short and long-term priorities.

Financial Implications

No financial implications.

Resources Cited

Corporate Information Technology Strategic Plan - greatersudbury.ca/city-hall/reports-studies-policies-and-plans/report-pdfs/corporate-information-technology-strategic-plan/

2023 Update on IT Strategic Plan - 2023 IT Strategic Plan Update (escribemeetings.com)

Corporate Information Technology Governance Framework - Appendix A of this report

Objective

The objective of this audit is to assess the effectiveness of Information Technology (IT) governance processes.

Background

IT governance is defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals.

IT demand-side governance (ITDG) processes ensure the effective evaluation, selection, prioritization, and funding of competing IT investments; oversee their implementation; and extract measurable business benefits. ITDG is a business investment decision-making and oversight process which is a business management responsibility that addresses items on which IT should work.

IT supply-side governance (ITSG) processes are concerned with ensuring that the IT organization operates in an effective, efficient and compliant fashion. These processes are primarily the responsibility of the Chief Information Officer and focus on what IT should do and what it does.

To be effective, IT Governance Committees must exercise the appropriate mix of IT demand-side and supply-side governance processes to prioritize requests for new technology while ensuring that operational requirements for confidentiality, integrity and availability continue to be met.

Scope and Methodology

The scope of this examined IT governance processes from 2018 to 2023. The methodology included a review of the Corporate IT Governance Framework which is shown at Appendix A, interviews of IT managers and the IT governance team, examination of reports to senior management and Council, attendance at recent meetings and a review of best practice guidance.

Executive Summary

While many important components of IT governance are currently in place and are operating effectively, opportunities for improvement were identified within this audit.

Audit Standards

We conducted our audit in accordance with Generally Accepted Government Auditing Standards which require that we adequately plan audits; properly supervise staff; obtain sufficient, appropriate evidence to provide a reasonable basis for audit findings and conclusions; and document audits. For further information regarding this report, please contact Ron Foster at the City of Greater Sudbury at 705-674-4455 extension 4402 or via email at ron.foster@greatersudbury.ca

Observations and Management Responses:

1. Organization and Governance Structures

Processes/procedures (in italics) have been established that satisfy the following control objectives:

Organizational structures include clear lines of reporting. • *A "Corporate IT Governance Framework" document identifies governance roles and defined responsibilities in a layered governance model from Council, to Executive Leadership Team (ELT), to a delegated IT Governance Team, and to the IT Service area.*
Organizational structures include the operational nature of components & communication protocols.
• *Formal quarterly reports to ELT and annual reports to Council occur.*
IT personnel is capable of allocating resources to meet business objectives
• *Base service needs are being met based on achieved KPI and Activity measures from the 2024-2025 budget. The IT service is not, however, built to meet all new technology demands so capital or operating business cases are submitted when demand exceeds available resources. For the 2023 budget a Cybersecurity Awareness Platform business case was not approved. Awareness is an increasingly important protection. To mitigate risk, priority parts of this awareness platform are being delivered by an approved technology capital project.*
The organization and IT collaborate on resource priorities, initiatives, and investment decisions
• *This is formalized by the previously mentioned IT Governance Framework.*
The IT governance structure is defined in alignment with the IT architecture
• *The IT Governance Framework includes the definition for an Architectural Review Board, to review all technology for fit with our technology architecture standards. This is formally a step in the workflow of new ideas. Architecture considerations include cybersecurity.*

Observation

The annual update on the Corporate IT Strategic Plan that was presented to Council in June 2022 identified supply chain exploits as a notable example of growing cybersecurity threats. The annual budget for 2023 also identified information security as one of the nine significant enterprise risks that informed the budget process. However, the 2023 budget did not sufficiently highlight the need for the approval of a business case to implement an IT security awareness training platform to mitigate these growing risks. As a result, the corporation continued to be exposed in 2023 to emerging risks that could compromise the availability of networks, the integrity of data or the access to assets.

Recommendation

Provide information about exposures arising from cybersecurity risks within the annual security report to Council and identify costs in business cases to address these sensitive risks within in-camera sessions to maintain confidentiality about these risk exposures.

Management Responses and Action Plans

We agree. Additional resources may be required in the future to mitigate cybersecurity risks. The in-camera

approach will help explain these risks.

2. Executive Leadership & Support

Processes/procedures (in italics) have been established that satisfy the following control objectives:

The vision, mission, and strategy of the organization collectively provide the direction for IT investment. • *The 2019-2027 Strategic Plan includes, 'technological leadership' in the mission statement, 'Innovation' as a value, 'innovation and cost-effective service delivery' is a stated goal. The overall Strategic Plan also references the IT Strategic Plan.*
IT budget is communicated to senior management. • *In addition to the City budget system, the IT Governance process includes monthly review of progress and expense tracking on technology projects.*
Budgets are controlled and monitored. • *Project budgets and progress on project milestones and on service KPI are monitored by the IT Governance Team.*
Organizational leadership understands the investments that have been made in IT. • *For approved projects, the investment amounts are presented each month to the IT Governance Team.*
IT initiatives are properly aligned with organizational objectives. • *The City's budget approval process requires statements of alignment, value and risk for all budget added technology projects. For in-year initiatives that are done within existing budget the IT Governance process uses the City's capital project prioritization tool to score initiatives based on their alignment, value and risk mitigation*.
IT governance helps champion innovation within IT and the entire organization. • *The formal approaches to this are: 1. projects communicate and train on new technologies; 2. communications within and from the IT Governance Team to organizational leaders, including once annually to Council; 3. 'Program Committees' (explained in the IT Governance Framework) communicate amongst key users of the City's large systems (e.g. PeopleSoft).*

As the control objectives for this area have been met, no recommendations have been provided.

3. Strategic & Operational Planning

Processes/procedures (in italics) have been established that satisfy the following control objectives:

The organization has defined roles that include accountability, authority, and decision-making. • *The IT Governance Framework lists roles and responsibilities to support IT Governance.* • *New initiatives are prioritized using City budget prioritization tools that incorporate strategic alignment, value and risk.* • *A Program Committee exists for cybersecurity governance.* • *The Enterprise Risk Management registry for IT risks is managed by IT Service Division.*

Observation

Although risks associated with individual IT projects are monitored by the IT Governance Team, the IT risk register for the IT function as a whole is not shared with the IT Governance Team. As a result, some IT risks may not be considered adequately in strategic and operational plans.

Recommendation

Advise the IT Governance Team about risks within the annual risk assessment process for the IT function.

Management Responses and Action Plans

We agree to add monitoring and evaluating the IT risks within the enterprise risk register to the IT Governance process. As background, currently the enterprise register is reviewed, updated and monitored by the IT service area and this generates project submissions to the IT Governance Team. Also, risk is a factor in prioritizing all projects that are approved by the IT Governance Team.

4. Service Delivery & Measurement

Processes/procedures (in italics) have been established that satisfy the following control objectives:

IT delivers on its plans, budgets, and commitments. • *The IT Governance Team established a set of measures that are presented to ELT quarterly. Also, the Governance Team reviews the portfolio of technology project monthly.* • *The IT Directors performance plan aligns with the IT Governance measures.*
The IT department reports performance metrics to key stakeholders. • *The dashboard of operational measures is reviewed with the IT Director monthly.*
IT performance is reported in IT and business terms. • *Project progress dashboards present summary information on what the project will deliver and a summary of current status.*
Performance metrics are based on changing business needs. • *Performance metrics are reported to the IT Governance Team.*

As the control objectives for this area have been met, no recommendations have been provided.

5. IT Organization and Risk Management

Processes/procedures (in italics) have been established that satisfy the following control objectives:

The level of IT-related risk that the enterprise is willing to take to meet its objectives is defined. • *The organization provides oversight of IT risk management and control activities.* • *The organization's risk management strategy includes IT-related risks.* • *There is a process in place to assess, address and communicate IT risks to key stakeholders and executive management during the project, change, and release management processes.*
A disaster recovery plan exists and is tested on a periodic basis. • *The IT Governance process includes disaster recovery but not business continuity.* • *The Disaster Recovery Plan (DRP) was updated in 2022 and last tested in 2023.* • *The DRP prioritizes the recovery of systems by the critically of service they support.*

- *No electronic records classification in-place to prioritize actions based on criticality of data.*

IT projects are delivered on time and on budget.

- *IT Governance has a consistent project reporting process and monitors all projects monthly. Actions that result from monitoring are recoded in IT Governance minutes.*

The IT risk profile is updated frequently.

- *The IT risk profile is updated as part of the Enterprise Risk Management process.*

Asset classification determines what level of control is required over its handling and use.

- *Asset classification is considered in the prioritization of systems recovery processes.*

Observation

IT staff have initiated a project to ensure all City service areas are fully aware of the asset classification of their systems in the disaster recovery plan, the restoration times, and the impact on their business continuity plans.

Recommendation

Complete the project to assure all City service areas are aware of and provide input to the disaster recovery plan.

Management Responses and Action Plans

Agreed. This action is being tracked by the IT Governance Team for completion in 2024. As further background, input was sought from service areas when the disaster recovery plan was originally created.

Corporate Information Technology Governance Framework

Great service experiences powered by technology and data, available anywhere, anytime.

Version: 1.1
Updated: December 20, 2018

Corporate Information Technology Governance Framework

The Information Technology Governance Framework is defined as “the processes and structures which inform, direct, manage, and monitor how the organization makes the best and most effective use of data and technology.”

Contents

The Vision 4

Guiding Principles 4

The Framework 4

- Structure 4

Decision Making Groups 4

- Roles and Accountability Summary Table 5
- Inter-relationships 6

Policies & Standards 6

Processes & Methods 6

- Projects Processes 6
  - Project Intake / Selection 7
  - Resource Management 7
  - Project Execution 7
- Corporate IT Governance Team Process 7
- Program Processes 7
- Architectural Review Board (ARB) Processes 7
- IT Operations Processes 7

Measurement and Monitoring 7

- Project and Portfolio Management 7
  - Balancing the Portfolio: Run, Grow, Transform 7
  - Service Level Measurement 7

Appendix A - The Guiding Principles Responsibility Matrix 8

Document Revision Log

Version	Summary of the Revision	Revised by	Date
1.0	Initial release approved by ELT	Peter Taylor	September 18, 2018
1.1	All arrows on the 'Inter-relationships' chart made 2-way to reflect 2-way communications	CITGT	December 20, 2018

The Vision

The 2018 Corporate Information and Technology Strategic Plan (CITSP) introduces a new approach to technology governance that reflects broader Corporate Services changes towards taking an enterprise view that focuses on what is better for the City as a whole.

Along with that new approach the Strategy introduces a new vision for the role that technology will play at the City:

Great service experiences powered by technology and data,
available anywhere, anytime.

The vision encapsulates several important ideas;

- That the City exists to deliver services to the community that are efficient, accessible, easy to use, and cost-effective and technology serves that mission
- That the City intends to modernize how it delivers services by taking advantage of technologies; thereby creating effective organizational collaboration and improved customer experiences
- That the City intends to become data driven, including digitizing data, in order to derive insights that inform good decisions to the benefit of the community

Guiding Principles

A series of IT Guiding Principles have been developed to support the Corporate Information and Technology vision. The principles set the structure for the City's approach to technology. They will be used to assist decision makers in following a consistent and correct path.

A summary of these principles along with their implications was included as Appendix A - The Guiding Principles Responsibility Matrix. The appendix also identifies which principles are most relevant to the different decision making groups that are defined in this Framework.

The Framework

The Framework presented in this document ensures that the City is working on the right projects, in the right way, and that decisions and resources are suitably aligned with the CITSP vision. In support of that goal the Framework needs to enable monitoring and evaluation of progress and outcomes.

Structure

The Framework is made up of four elements, discussed in greater detail in the following sections:

- Decision making groups (e.g. accountability, inter-relationships)
- Policies & standards (e.g. architecture, procurement, security)
- Processes & methods (e.g. project approval, prioritization, execution)
- Measurement and monitoring (e.g. Key Performance Indicator (KPI))

Decision Making Groups

Organizations often view decisions about technology as complicated, technical and "best left to the experts in IT". However, decisions about technology often reflect fundamental questions about how service gets delivered:

- How do we want to use technology in our business?
- What technology do we want to use, and how do we want to use it?
- How much should we spend on technology?
- What do we need to tackle first?
- How secure do we want to be?
- What should be available first in the event of a disaster event?

These are not just decisions for technologists in the IT Division; they are important business decisions for leaders of the organization to address.

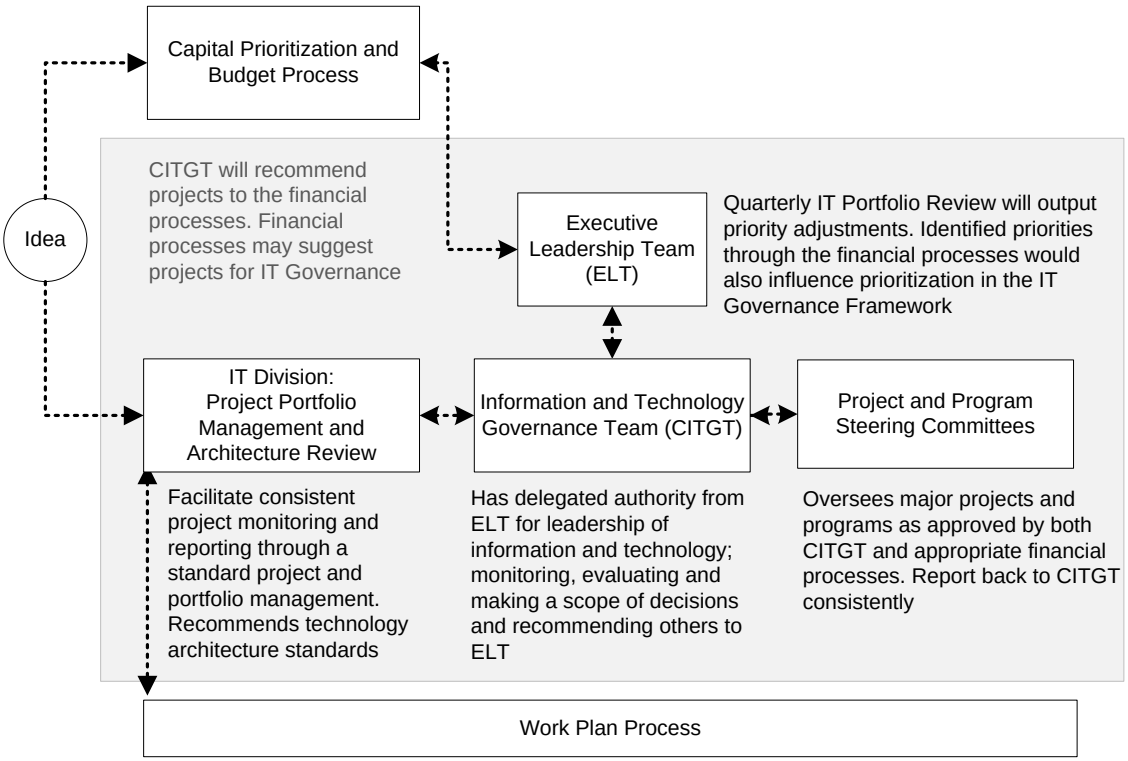
The Roles and Accountability Summary Table (below) identifies the decision making groups and their decision making responsibilities within the IT governance framework. These decision making groups are designed to align with and support already existing City leadership groups.

Roles and Accountability Summary Table

Accountability	IT Principles			IT Architecture			IT Infrastructure			Business Application Needs			IT Investments		
I = Informed, C= Consulted, D = Decision:	I	C	D	I	C	D	I	C	D	I	C	D	I	C	D
City Council: Endorse Strategy and approve IT investments	●									●					●
ELT (Executive Leadership Team): the authority to keep the City focused on corporate objectives. Enforce the guiding principles as desired corporate behaviour. Set objectives and KPI's.			●								●			Recommends	
CITGT (Information and Technology Governance Team): has delegated authority from ELT for oversight of all Information Technology including: monitoring, evaluating and recommending decisions to ELT. Members represent the CGS corporation not CGS departments.		●				●	Non-strategic		strategic	●				Recommends	
Project or Program Steering Committees: recommended by CITGT and approved by ELT to provide focused governance of enterprise systems, information processes or projects. They intake enhancement requests, develop plans and recommend initiatives within an CITGT/ELT approved scope. They monitor progress, resource usage and outcomes.	●			●			●			●			●		
Department Directors: define business requirements, establish departmental IT priorities. Active project accountability, resourcing, change management leadership.	●						●				●	●	●		
IT Division: responsible for IT Management including facilitating information for the decision groups above. Specific IT Management functions related to governance are: 1) **Architectural Review Board (ARB)** to develop and recommend technical standards and advise on project proposal to ensure fit with standards; 2) **IT Planning and Delivery** to assure consistent monitoring across the complete portfolio of projects and programs; 3) **IT Operations** to assure customer service, reliability, efficiency and security of technology.	●				Recommend			●	Operational	●			●		

Inter-relationships

The IT Governance Framework integrates to other decision making processes such as City Budget, Capital Prioritization and Work Plan. The following graph illustrated the inter-relationship between key corporate processes and organizational groups:



As an annualized resource planning process, Work Plan is updated yearly with both approved projects as well as those with anticipated approvals. The Work Plan may reveal projects which need to be evaluated through financial processes and IT Governance Framework.

Policies & Standards

The IT Division will author policies and standards to be reviewed by CITGT and to ELT for final approval. Once approved the IT Division is responsible for applying and enforcing the policies and standards.

A non-exhaustive list of policies and standards includes:

- **Acceptable use:** Provides the parameters, obligations and responsibilities associated with access to and use of City technology
- **IT Security:** Defines how the City operates a secure and reliable technology `
- **Availability and reliability of critical system:** Defines the systems deemed critical to the operations of the City and the level of investment to assure their uptime and performance.
- **Backup, and Disaster Recovery (DR):** Defines the backup and recovery plans for computer systems that store City data. This policy is also designed to prevent the loss of City data and systems in the event of an equipment failure or destruction
- **IT Service Level Standards:** Defines the corporations expected service levels from the IT Division and the methods for monitoring them.

Processes & Methods

In addition to the IT Policies and Standards the City will develop playbooks to guide effective execution of technology projects and operations of the corporate technology program. Process and methods to be defined are:

Projects Processes

Projects will move through multiple stages before being approved for scheduling and execution.

Project Intake / Selection

The IT Division will operate a project intake process to develop ideas in partnership Business Units and bring project proposals to CITGT. CITGT will recommend prioritization and scheduling to ELT.

Resource Management

The IT Division will be responsible for collating the proposed technology project resource needs (departmental and IT staff) and matching this to available capacity. This information will be made available to CITGT to support the evaluation and scheduling of projects.

Project Execution

The IT Division will assure project management best practices and consistent reporting are adopted for technology projects to assure effective execution and consistent reporting across all projects. The process shall require approval by CITGT/ ELT of changes to approved scope, schedule or costs when thresholds are exceeded.

Corporate IT Governance Team Process

A Terms of Reference shall be created defining the roles and responsibility of the team delegated by ELT to oversee corporate IT governance.

Program Processes

Program committees shall be proposed for each of the City's key technology platform's to assure that the City sustains and evolves the use of these key technologies. All program committees shall follow a consistent process, a process recommended by CITGT and approved by ELT. This process shall include an annual allotment of resources and regular progress reports to CITGT and to ELT.

Architectural Review Board (ARB) Processes

The IT Division will operate an ARB process to advance technology standards review all technology initiatives for fit with the current architectural standards. As required the IT Division will recommend adjustments to project approaches or adjustments to our architectural standards for CITGT approval.

IT Operations Processes

To enable oversight of IT the IT Division shall report to CITGT on the reliability, customer service, efficiency and security of IT Operations.

Measurement and Monitoring

Project and Portfolio Management

IT Division is responsible for reporting on the status of all technology portfolio projects in a way that provides visibility into the projects and provides CITGT with information to help intervene when necessary to keep projects on track.
All Project and Program Steering Committees will report to the portfolio. This includes those for larger initiatives executed in partnership with the IT Division and, smaller divisional project being executed without the direct involvement of the IT Division.
Green, Yellow, Red stop light indicators shall be employed measuring deviations from scope, schedule and/or cost. Thresholds for these indicators shall be defined by CITGT and approved by ELT.

Balancing the Portfolio: Run, Grow, Transform

ELT shall provide direction to CITGT on target allocation across investment categories: **Run**, to keep existing City technology and business services operational; **Grow**, provide expansion to existing technology and; **Transform**, new organizational capabilities or fundamental processes changes.

Service Level Measurement

A first task of CITGT and IT Divisions shall be to establish service level requirements for: customer service, reliability, efficiency and security of technology. Subsequently these will be

Appendix A - The Guiding Principles Responsibility Matrix

A series of IT Guiding Principles have been developed to support the vision. They assist decision makers in following a consistent and correct path. This table identifies relationship between principles and area of responsibility for each group:

Principles	**Implications**	Council	ELT	CITGT	Project and program stg	Department Directors	IT Division
1. The customer is the end user	• When developing solutions or services involve the customer (internal or external) in co-design – ensuring that their input meaningfully contributes to better design • Process mapping and customer journey mapping should be used on projects to ensure that the voice of the customer is heard • Test solutions with customers (in a beta or pilot stage) before launching them				●	●	
2. Services should be demonstrably better as a result of investments in technology	• Suitable due diligence is required to fully evaluate projects before funding and resource commitments are made • Business cases will be required for projects • Post implementation reviews will be conducted to ensure that anticipated business benefits are achieved – project sponsors will be held accountable for achieving benefits • Benefits tracking process will allow the City to understand the overall ROI for IT investments	●	●	●			
3. Enterprise systems should be deployed if they meet at least 80% of business needs	• Detailed requirements are needed to support assessment process • Any exceptions will be escalated to ELT for evaluation • Re-use of existing enterprise systems (CityWorks, PeopleSoft) will be encouraged			●	●		●
4. Data is an asset	• Increased open-ness toward data sharing • Data quality with clearly allocated roles, responsibilities and accountabilities		●	●			●
5. Our approach to technology reflects our desire to be an employer of choice	• Supporting a range of device types – including frequent recalibration of needs and expectations from management and staff. Working with a representative 'tech-savvy' forum to ensure that technology provisions are keeping pace with expectations and needs		●	●			

Principles	Implications	Council	ELT	CITGT	Project and program stg	Department Directors	IT Division
	• Supporting mobile and flexible working – Wi-Fi • Modern collaboration tools and capabilities – online meetings, messaging, presence						
6. An enterprise-wide perspective will define technology priorities	• A new governance model will be used to agree priorities, supported by a ranking and prioritization scheme • Single annual technology project portfolio • Some groups will be disappointed when their initiatives are not prioritized		●	●			
7. Technology investments must be supported by key indicators showing short and long-term value earned	• Processes to support value calculation (ROI, NPV) that reflect monetary and non-monetary value will be developed and applied to project proposals.			●	●	●	
8. Technology is a means to an end – success is the result of collaboration	• Err towards over- not under-inclusion • Quantify outcomes as part of the project justification process • Focus is upon outcomes and end-to-end services and process design, not on technology implementation • Increased cross functional working			●	●	●	●
9. Architecture and standards drive decision making	• Architecture review board to develop and set standards, which will be endorsed by CITGT • Architecture review board to review proposals against architecture and standards – proposals that don't meet standards may need to be adjusted, may be rejected or may need a formal exception to be made.			●	●		●
10. Timely results and appropriate project oversight are key	• Adoption of project management methodologies, including Agile project techniques for projects that are suited to Agile delivery – ensuring that the project approach provides enough, but not too much structure.				●		●