CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

IT and Data Governance

TECHNOLOGY SPOTLIGHT

> ***"If I was to choose one factor that most contributed to the success of IT, it is IT governance."***
>
> **—Peter Weill, chairman of the Center for Information Systems Research, Massachusetts Institute of Technology**

Description

IT governance is the management and control of the information technology environment, including the data needed for the benefit of the organization and its stakeholders. IT governance is the responsibility of the board of directors and executive management and forms an integral part of enterprise governance. IT governance requires the establishment of the leadership, organizational structures, policies, processes and internal controls that enable IT to meet the stakeholders' and organization's strategy and objectives. Put simply, IT governance is the people and processes supporting decision-making for technology initiatives. Effective IT governance results in balancing enterprise value creation with risk mitigation.

Corporate and IT Governance

The Organisation for Economic Co-operation and Development (OECD) defines enterprise-wide or corporate governance as the system by which organizations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among various participants: the board of directors, board subcommittees, executive management, management, shareholders and other stakeholders. It sets the directorial and managerial tone; establishes goals; manages objectives; establishes culture and values; and spells out the processes, procedures and rules for decision-making. Furthermore, corporate governance also provides the structure through which the organization's objectives are established and the means of attaining those objectives. It establishes metrics for key performance and goal indicators as well as a process to escalate findings and initiate changes and improvements.

An important enabler of successful IT governance is regular communications with key stakeholders regarding the status of strategic and tactical IT plans. This communication results in meaningful dialogue that creates transparency and identifies areas where risk could escalate: operational delays, cost overruns, benefits realization, stakeholder disengagement, scope changes, technology challenges and lack of resources. Furthermore, enabling IT to have a "seat at the table" results in clearly articulated and pragmatic communication with the steering committee, audit committee, risk committee and the board of directors while providing the organization with sufficient and timely understanding of the value and risks of IT for effective board and senior management governance.

Frequently IT strategic and tactical plans are prepared in isolation from enterprise strategic plans or as a one-time exercise, and without regular communication and monitoring. This results in misaligned IT plans that fail to support existing, new or planned enterprise initiatives. The focus on IT operational issues instead of broader strategic issues could lead to missed opportunities to create new enterprise value. IT governance, when implemented appropriately and effectively, would enable IT to drive or lead corporate initiatives and enterprise strategies.

EXAMPLE OF COLLABORATION BETWEEN BUSINESS AND IT TO SUPPORT VALUE CREATION:

An online retailer identified the strategic need to grow sales and increase profitability but found it difficult to do because of competition. Management used both the company's internally generated market data as well as data purchased from external researchers to find the buying patterns and behaviours that would identify the opportunities for carrying out the corporate strategy. An external cloud service vendor was engaged to collaborate with the business and IT groups to customize product content, create client-specific discounts, and provide additional product suggestions. By utilizing sophisticated business intelligence and leveraging internal and external IT systems and data, this online retailer was able to provide its customers with matched product offerings that met their needs while increasing customer satisfaction and reducing product returns. The company met its business growth strategy by exceeding its sales and profit targets, reducing the cost of returns and increasing customer loyalty. Furthermore, IT collaborated closely with internal marketing, legal, finance and operational teams as well as with the external cloud provider to ensure compliance with all laws and regulations.

When effectively implemented, IT governance creates an environment where the organization can fully leverage its IT assets to create and sustain value, provide competitive advantage, and ultimately help achieve strategic goals. Effective IT governance also increases the likelihood IT will deliver services within scope and budget. Unfortunately, many businesses struggle to understand and govern the IT organization, processes and activities. As a result, the failure to fully realize the potential benefits of IT's people, processes, technologies and initiatives can lead to a loss of value and an increase in business risks.

Importance

IT Governance

The role of IT has evolved as a result of the emergence of technology, data and information as enablers of innovation and business value creation. Strong IT governance is required to effectively utilize IT resources in support of business strategy and to mitigate new and emerging risks. Establishing an effective IT governance enables the business to create the appropriate culture and operating model. When IT governance is implemented effectively, value is derived from IT investments and operations. The enterprise's vision, strategy, programs, initiatives and plans are aligned with the plans and tactics needed for their realization. Because the people, processes and technology are operating together to move the enterprise forward, the enterprise is able to meet or exceed it goals.

WHAT ROLE DO CPAs PLAY IN IT GOVERNANCE?

At the board and committee levels, CPAs need to understand IT governance, but rarely would they be part of the IT governance structure and process itself. Typically, the board and/or committees would be responsible for approving overall risk tolerance levels, including IT risks such as privacy, cybersecurity, and business continuance. They would also approve the allocation of resources, including IT resources, and the overall strategies and performance goals, including IT-specific goals and objectives, for the organization. From this perspective, CPAs need a broad understanding of IT issues and trends.

CPAs also play a critical role in IT governance issues at the program and project levels. These programs could be IT-driven initiatives that impact the operations of the organization, such as cybersecurity. For example, the decision to shut down operations if a cyberthreat is imminent could impact the safety or staff or customers. This decision cannot be made by the IT function alone. The CPA needs to ensure proper representation of senior executives is in place and that the process for these types of program is tested regularly to ensure preparedness when actual emergencies occur.

At the project level, CPAs should be part of the project governance team alongside IT and the business requesting the project. CPAs should support the development of business cases and budgets, ensure representatives from both IT and business are on the project team, but recognize that the overall decision-making remains with business.

Without CPAs in place to ensure proper governance, IT programs and projects may become solely IT driven and lack business support. If this happens, the project may fall out of alignment with the enterprise's vision and strategy and likely become doomed to fail.

Data Governance

Data is very valuable to businesses due to the emergence of sophisticated analytic techniques and computing power that enable data-driven decisions. The rising prominence of data and its association with the IT environment makes it another area where IT must play a critical role. So when it comes to IT governance, data governance must also be considered. Although many may say the data is “owned” by business, data ownership needs to be customized to fit the culture and structure of the whole organization. Some may argue that because of IT’s expertise in safeguarding an organization’s IT assets, data ownership should fall to it. However, regardless of which part of the organization owns the data, it is important to treat data as one of the organization’s most valued assets. Appropriate internal controls must be put in place to protect these assets from cyber attacks, theft, misappropriation, and non-compliance with privacy laws and other regulations. This is where IT plays an important role as a strategic partner in enhancing the integrity, security and completeness of data to support data-driven decision-making and manage data as a key strategic asset.

Business Benefits and Considerations

The business benefits of implementing an IT and data governance program include:

- more effective alignment and execution of IT and enterprise strategies
- creation of value through the realization of stakeholder and enterprise-wide goals and objectives
- technical and systems support for compliance with laws and regulations
- strengthened security for data and IT assets
- improved collaboration and data sharing resulting in better business decision-making
- reduced costs through more effective risk management as a result of IT initiatives
- enhanced accountability for IT program and portfolio management.

To fully realize these benefits, organizations need to have a strategy in place to mitigate some of the common pitfalls of ineffective IT and data governance programs. The table below summarizes these risk areas and suggests appropriate mitigation strategies.

Risk Areas	Risk Mitigation Strategies
A comprehensive and holistic IT and data governance strategy is lacking.	• Develop and adopt an IT and data governance strategy based on a recognized standard or framework aimed at the whole enterprise. • For IT governance frameworks, consider International Standards Organization (ISO) 38500:2015, COBIT 2019 which integrates several frameworks including ISO 38500 and data management frameworks. • Consider the use of the Data Governance Institute (DGI) data governance frameworks. Many well recognized software vendors have published white papers on data governance, including Microsoft, IBM, SAS, and Oracle.
The company is unable to comply with new and emerging laws and regulations that require sophisticated systems and processes for compliance monitoring.	• Consider the need for monitoring compliance with applicable laws and regulations (*Personal Information Protection and Electronic Documents Act*—PIPEDA; *The Privacy Act, Health Insurance Portability and Accountability Act* - HIPAA, EU General Data Protection Regulation - GDPR, the 2020 California *Consumer Privacy Act*, etc.). • Consider implementing and testing new/revised procedures for compliance with applicable laws and regulations. (e.g., data deletion requirements for structured and unstructured data).
The company lacks programs and plans to support planned IT and data governance initiatives.	• Develop tactical calendarized IT plans with key milestones to ensure enterprise alignment with the IT strategic plan, including adoption by IT and the user community.
The vision of IT and its contribution and value to the stakeholders and enterprise are not well understood.	• Create an IT communication plan, perhaps an IT steering committee comprised of major stakeholders and IT experts prominent in enterprise-wide communications.
IT and data governance lack the appropriate scope, penetration or support throughout the organization.	• Establish a cross-functional data governance council that includes the following key roles: data steward, data architect, data-quality lead, technology lead, application lead, business leaders and subject matter experts. • Create and sustain an IT governance awareness campaign supplemented by key stakeholder training.

Risk Areas	Risk Mitigation Strategies
IT initiatives are not aligned with stakeholders' goals and the enterprise's strategic plans, goals, objectives and initiatives.	• Implement an IT strategy that includes tactical and annual plans that align with key stakeholders' objectives and the enterprise's strategic plans, goals, objectives, and initiatives.
Governance-level performance-monitoring practices have not been implemented.	• Select key goals and performance indicators and establish a monitoring process to report and evaluate performance and maturity levels to stakeholders.
Monitoring and remediation activities are not documented and, accordingly, IT and data governance activities are not reported.	• Implement a process to record monitored activities and to provide these records to the appropriate persons through dashboards and/or periodic reports for follow-up and remediation. • Monitor the effectiveness of the data-governance council by reviewing the improvements and accuracy of reporting, reduction of redundant and duplicate data sources, and centralization and storage of data in one data warehouse or data lake.
IT has not adopted a portfolio management approach to managing IT initiatives, resources and projects.	• Select and implement an IT portfolio management approach as part of the IT governance initiative.
IT does not have the opportunity or does not take advantage of opportunities to interact with the board of directors, board subcommittees and executive management.	• Ensure IT makes periodic scheduled reports to the board, board subcommittees, and executive management to ensure the risks, complexities and challenges are well understood and monitored. • Let stakeholders know they will receive regular and timely reporting from IT.
The IT plans do not include value creation and risk management.	• Include value management and risk management (ISO 31000 or COBIT 2019) in the scope of the IT strategic plan, including value and risk management initiatives. • Evaluate emerging risks and new technologies that will help to reduce these risks.
IT has not appropriately aligned the people, processes and technologies with the risk of non-compliance with laws and regulations.	• Ensure IT is aligned with the enterprise's risks of non-compliance with laws and regulations. Establish IT people, processes and technologies that will reduce the residual risks of non-compliance to an acceptable level.

Risk Areas	Risk Mitigation Strategies
IT has not appropriately evaluated and managed the risks of outsourced service providers.	• Monitor the risks of outsourced IT services, including cloud services such as Software As a Service (SaaS) and Infrastructure As a Service (IaaS) by obtaining a Service and Organization Controls reports (SOC 1 or SOC 2) from the service provider. • Evaluate whether the SOC report together with the enterprise's internal controls is sufficient to reduce the enterprise's risk appetite to an acceptable level.
IT does not have the opportunity to monitor, manage and reduce cybersecurity risks to a level acceptable to the stakeholders.	• Select and implement a cybersecurity framework. Monitor the operational effectiveness of internal controls against the cybersecurity framework. • Consider the NIST Cybersecurity Framework, CIS Critical Security Controls. • Consider cybersecurity insurance to cover residual risk above levels acceptable to stakeholders.
IT does not have the ability to monitor and manage the risks associated with cloud providers.	• Obtain from the cloud provider a self-assessment using the Cloud Controls Matrix from the Cloud Security Alliance. • Obtain a SOC 1 (Type 2) or SOC 2 (Type 2) audit report from the cloud provider to determine whether sufficient controls have been established at the cloud provider to reduce the risks to an acceptable level for the services provided for your organization. • Review the user-entity controls identified in the report above and determine whether your organization's user-entity controls in combination with the controls identified in the SOC 1 or SOC 2 audit report are sufficient to reduce your organization's risks to an acceptable level. • Establish key performance metrics that are predictive (if possible) to monitor your cloud vendor's performance. Include these performance metrics in the service level agreement (SLA) and monitor compliance with the agreed metrics.

Conclusion

The importance of information technology to an organization's strategy and objectives have increased significantly. Organizations looking to realize the full potential of their information technology assets need to have people, process and technology working together towards the same organizational goals. Having an effective IT and data governance program is key to making that happen.

This publication is part of the **Technology Spotlight series**.

The entire series covers technology trends that impact CPAs and are available on our website.

DISCLAIMER

This paper was prepared by the Chartered Professional Accountants of Canada (CPA Canada) as non-authoritative guidance. CPA Canada and the authors do not accept any responsibility or liability that might occur directly or indirectly as a consequence of the use, application or reliance on this material.