IT Governance

Idea In Short

IT governance provides organizations with a formal structure to align IT strategies with business goals, ensure regulatory compliance, and produce measurable, repeatable results across both public and private sector enterprises.

IT governance is a formal framework that provides the structure for organizations to ensure that IT investments are aligned with business objectives. The 1990s and early 2000's witnessed several dot-com bubble bursts, corporate scandals and accounting frauds. Subsequently, regulations as the Gramm–Leach–Bliley Act [GLBA] and the Sarbanes-Oxley Act, mandated formal corporate and IT governance across organizations.

What is IT governance?

Essentially, IT governance provides the structure to align business and IT strategies. By following a formal framework, organizations can produce repeatable, measurable results. This predictability assures organizations that their strategies, goals and implementation measures are consistent and well-aligned. Such formal programs also take stakeholders' interests into account. Furthermore, IT governance accommodates the needs of staff and processes they follow. Hence, IT governance is an integral part of overall enterprise governance.

Why do organizations implement IT governance?

Today, organizations are subject to many regulations. Some regulations, such as the European Union's General Data Protection Regulation (GDPR) and California Consumer Protection Act (CCPA) are global in outreach. Such regulations transcend the geographical perimeter in which your business operates. These regulations govern the protection of confidential customer information, financial accountability, data retention and disaster recovery, among others. Organizations and their leaders are under pressure, not only from shareholders, stakeholders and customers, but also regulatory agencies. Visionary leaders

and their organizations view such regulations, not as impediments, but rather as incentives. They view regulations as opportunities to align their business along the interests of their broader community. Hence, to ensure that they meet the internal and external requirements, many organizations implement formal IT governance programs that provide the framework of best practices and controls.

Who uses IT governance?

Both public- and private-sector organizations employ IT governance. IT governance ensures that their IT functions support business strategies and objectives. In general, any organization that should comply with regulations pertaining to financial and technological accountability should have IT governance in place. Regardless of the industry in which it operates, any enterprise serious about regulatory compliance should have a formal IT governance program. However, implementing a comprehensive IT governance program entails significant planning in both, time and effort. While smaller organizations may choose to implement only the essential IT governance practices, more mature and regulated organisations should choose full-fledged IT governance programs.

IT governance frameworks

The easiest way is to start with an industry-wide framework that's used by thousands of organizations. Such frameworks also include implementation guides to help phase in IT governance programs with minimal disruptions and overhead. The common frameworks are:

COBIT

Published by ISACA, COBIT is a comprehensive framework of:

> globally accepted practices, analytical tools and models

designed for governance and management of enterprise IT. With its roots in IT auditing, ISACA expanded COBIT's scope over the years to fully support IT governance. COBIT is widely used by organizations focused on risk management and mitigation.

ITIL

Formerly an acronym for Information Technology Infrastructure Library, ITIL focuses on IT service management. It aims to ensure that IT services support core processes of the business. ITIL comprises sets of management best practices for service strategy, design, transition (such as change management), operation and continual service improvement.

COSO

This model for evaluating internal controls is from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO's focus is less IT-specific than the other frameworks, concentrating more on business aspects like enterprise risk management [ERM] and fraud deterrence.

CMMI

The Capability Maturity Model Integration method, developed by the Software Engineering Institute, is an approach to performance improvement. CMMI uses a scale of 1 to 5 to gauge an organization's performance, quality and profitability maturity level. CMMI allows for mixed mode and objective measurements to be inserted is critical in measuring risks that are qualitative in nature.

FAIR

Factor Analysis of Information Risk (FAIR) is a relatively new model that helps organizations quantify risk. The focus is on cyber security and operational risk, with the goal of making more well-informed decisions. Although it's newer than other frameworks mentioned here, FAIR has already gained a lot of traction with Fortune 500 companies.

Selecting the appropriate framework

Overall, most IT governance frameworks help determine how your IT department functions. These frameworks provide the metrics that your management needs, including returns on IT investments. Usually, companies use COBIT and COSO for IT risk management and ITIL to streamline service and operations. Although CMMI was originally intended for software engineering, it now involves processes in hardware development, service delivery and purchasing. FAIR helps assess operational and cyber security risks. When reviewing frameworks, your corporate culture plays a crucial role. The framework that best fits your needs and those of your stakeholders is probably the best choice! Moreover, you don't have

to choose only a single framework. COBIT and ITIL frameworks complement one another. COBIT explains why something is done or needed, while ITIL provides the how. Many organisations use both, COBIT and COSO, along with the ISO 27001 to enhance their information security posture.

Summary

One of the most important paths to success is with executive buy-in. As with any significant engagement, keep your communication lines open among the various parties. Measure and monitor the implementation progress and seek outside help, if needed.