HOW-TO

What is IT governance? A formal way to align IT & business strategy

7 things you should know about IT governance, including choosing a framework and how to ensure a smooth implementation.

By Kim Lindros
CIO |
JUL 31, 2017 7:37 AM PDT

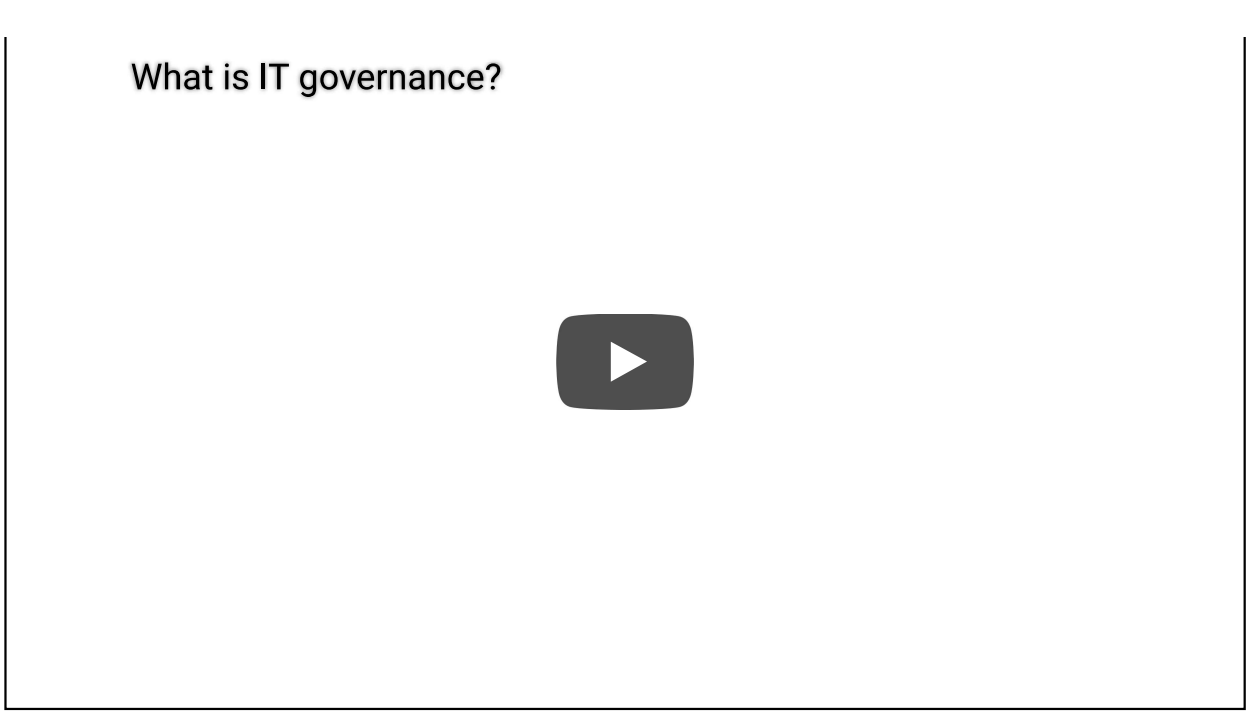
IT governance is a formal framework that provides a structure for organizations to ensure that IT investments support business objectives. The need for formal corporate and IT governance practices across U.S. organizations was fueled by the enactment of laws and regulations, including the Gramm–Leach–Bliley Act (GLBA) and the Sarbanes-Oxley Act, in the 1990 and early 2000s that resulted from the fallout from several high-profile corporate fraud and deception cases.

I reached out to Paul Calatayud, chief technology officer at security management provider FireMon, for his input on IT governance and what's required for successful implementation. Calatayud leads Firemon's corporate development program and provides thought leadership regarding product strategy, product management, and research and development. He's also a SANS Institute instructor and sits on advisory boards for several security-related companies.

[Discover the keys to effective IT governance in the digital era and beware these IT governance myths. | Check out the top GRC certifications. | Get the latest IT advice by signing up for our newsletters.]

1. What is IT governance?

Essentially, IT governance provides a structure for aligning IT strategy with business strategy. By following a formal framework, organizations can produce measurable results toward achieving their strategies and goals. A formal program also takes stakeholders' interests into account, as well as the needs of staff and the processes they follow. In the big picture, IT governance is an integral part of overall enterprise governance.



2. What's the relationship between IT governance and GRC (governance, risk and compliance)?

According to Calatayud, IT governance and GRC are practically the same thing. "While GRC is the parent program, what determines which framework is used is often the placement of the CISO and the scope of the security program. For example, when a CISO reports to the CIO, the scope of GRC is often IT focused. When security reports outside of IT, GRC can cover more business risks beyond IT."

[Related: Learn more about GRC]

3. Why do organizations implement IT governance infrastructures?

Organizations today are subject to many regulations governing the protection of confidential information, financial accountability, data retention and disaster recovery, among others. They're also under pressure from shareholders, stakeholders and customers.

To ensure they meet internal and external requirements, many organizations implement a formal IT governance program that provides a framework of best practices and controls.

4. What kind of organization uses IT governance?

Both public- and private-sector organizations need a way to ensure that their IT functions support business strategies and objectives. And a formal IT governance program should be on the radar of any organization in any industry that needs to comply with regulations related to financial and technological accountability. However, implementing a comprehensive IT governance program requires a lot of time and effort. Where very small entities might practice only essential IT governance methods, the goal of larger and more regulated organizations should be a full-fledged IT governance program.

SIGN UP

5. How do you implement an IT governance program?

The easiest way is to start with a framework that's been created by industry experts and used by thousands of organizations. Many frameworks include implementation guides to help organizations phase in an IT governance program with fewer speedbumps.

The most commonly used frameworks are:

- **COBIT**: Published by ISACA, COBIT is a comprehensive framework of "globally accepted practices, analytical tools and models" (PDF) 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. The latest version is COBIT 5, which 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 five 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. According to Calatayud, "allowing 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, Calatayud points out that it's already gained a lot of traction with Fortune 500 companies.

6. How do I choose which framework to use?

Most IT governance frameworks are designed to help you determine how your IT department is functioning overall, what key metrics management needs and what return IT is giving back to the business from its investments.

Where COBIT and COSO are used mainly for risk, ITIL helps to streamline service and operations. Although CMMI was originally intended for software engineering, it now involves processes in hardware development, service delivery and purchasing. As previously mentioned, FAIR is squarely for assessing operational and cyber security risks.

When reviewing frameworks, consider your corporate culture. Does a particular framework or model seem like a natural fit for your organization? Does it resonate with your stakeholders? That framework is probably the best choice.

But you don't have to choose only one framework. For example, COBIT and ITIL complement one another in that COBIT often explains why something is done or needed where ITIL provides the "how." Some organizations have used COBIT and COSO, along with the ISO 27001 standard (for managing information security).

7. How do you ensure a smooth implementation and positive results?

One of the most important paths to success is with executive buy-in. Calatayud recommends forming a risk management committee with top-level sponsorships and business representation. "To ensure it's an effective program, it needs to be supported by a broad set of line of business leaders." He also recommends sharing results with the board or audit committee to "develop real attention when items begin to get ignored."

As with any significant project, you should always keep communication lines open between various parties, measure and monitor the progress of the implementation, and seek outside help if needed.

More on IT governance:

- Rethinking IT governance for agility and innovation
- The keys to effective IT governance in the digital era

- 7 IT governance myths
- Top 10 GRC mistakes — and how to avoid them
- The top 6 governance, risk and compliance (GRC) certifications
- What is GRC and why do you need it?
- What is ITIL? Your guide to the IT Infrastructure Library
- What is COBIT? A framework for alignment and governance
- What is CMMI? A model for optimizing development processes

Next read this:

- *The 3 IT processes CIOs need most*
- *IT navigates the 'Great Resignation'*
- *13 most difficult-to-fill IT jobs*
- *7 ways to rebuild a failed IT organization*
- *7 toxic team behaviors IT leaders must root out*
- *10 technologies that will disrupt business in 2021*
- *7 management books every CIO must read*
- *7 IT hiring trends for 2021*
- *7 new rules of project management*
- *Customer experience: The new IT imperative*

Kim Lindros is a full-time content, online curricula and classroom training developer with a focus on security, Windows, and business topics. She has also contributed to several books on Windows technologies, applications and IT certification.

Follow