WHAT IS COBIT? COBIT EXPLAINED



IT management abounds with best practice frameworks. These frameworks offer philosophies and tangible paths forward to improve cost and resource management, measure risk, speed up customer service, and innovate analysis through predictive methods.

COBIT is one such best practice framework, but its scope is unique from most frameworks in that it focuses narrowly on security, risk management, and governance. If you're looking to streamline business processes, sync IT with business needs, alter your IT infrastructure, or manage the multi-cloud, COBIT isn't the answer.

But with most companies relying enormously on IT for business success – sometimes the IT itself *is* the product – COBIT is essential to developing, controlling, and maintaining risk and security for enterprises around the world, regardless of your industry.

Short for Control Objectives for Information and Related Technologies, COBIT was first developed to guide IT governance and management. Its latest iteration, COBIT 2019, has revamped parts of its framework while offering much-needed updates that accounts for ever-present cybersecurity threats and the incorporation of Agile and DevOps practices.

This article serves as a primer to the COBIT framework, understanding the meaning of COBIT, and offering guidance on whether it's the right solution for your enterprise.

What is COBIT in simple terms?

Control Objectives for Information and Related Technologies (COBIT) is a framework for managing enterprise IT systems. COBIT is a collection of best practices and principles, along with tools and models for making sure IT resources and processes align with and support business goals. It was first introduced by the Information Systems Audit and Control Association (ISACA) in 1996, and has gone through many rounds of development since.

What is ISACA?

ISACA stands for the Information Systems Audit and Control Association. This organization was founded in 1969 to support IT professionals in creating IT systems that support the business goals of organizations. ISACA focuses on IT governance, risk management, cybersecurity, and auditing support with standards, guidelines, and best practices.

What are the benefits of COBIT?

COBIT offers models to help maximize the value and trust in IT, and these extended guidelines provide security, risk, reward, business and IT consulting professionals with a more extended framework to help in delivering and maintaining enterprise objectives and strategies. Some of the numerous benefits of COBIT are listed below:

- Helps achieve operational excellence through efficient and effective application of technology and trustworthiness.
- Optimizes the cost of IT services and technology.
- Aids in managing and maintaining IT-related risk.
- Ensures the use of IT effectively and innovatively to align with strategic business goals.
- Maintains high-quality information to help support business decisions.
- Offers full support for IT firms that comply with business-oriented policies, regulations, relevant laws, and contractual agreements.

History of COBIT

International professional association ISACA first released COBIT in 1996 as a set of control objectives to aid the financial auditing community to work better around IT-related structures.

As value and potential beyond auditing became evident, ISACA released a more comprehensive version in 1998 and further expanded it by adding management guidelines in the third version released in the year 2000. Development of the AS 8015: *Australian Standard for Corporate Governance of Information and Communication Technology and the ISO/IEC* 38500 in January 2005 and January 2007 respectively upped the degree of awareness of the need for reliable information and communication technology (ICT) governance components.

In 2011, ISACA released COBIT 5, which remained the standard for seven years. In November 2018, big changes came to COBIT when ISACA released COBIT 2019.

IT innovations lead to change: COBIT 2019

The latest iteration of COBIT modernizes the framework for the immense expansion of IT within the

business world. COBIT 2019 continues to fit in nicely with ITIL, TOGAF, and CMMI, and it serves as a good umbrella framework for unifying processes across an organization.

Within the COBIT Core Model, the heart of COBIT, there are now 40 governance and management objectives. Due to user feedback and IT reliability and needs, COBIT 2019 offers more flexible options for deploying maturity and capability measurements so that IT goals can keep up with data-driven business goals.

According to ISACA, COBIT 2019 has several new goals, too, including but not limited to the following:

- Improved alignment with global standards and best practices to encourage COBIT's relevance
- New open-source model allows for global feedback, hopefully resulting in faster, more agile updates and improvements
- More guidance and prescriptions to make COBIT a best-fit governance system, not one that works against the enterprise
- Better measurement tools to align with CMMI

The COBIT 2019 guidebooks significantly revamp prior versions, resulting in four key guides:

- Introduction & Methodology
- Governance & Management Objectives
- Design Guide
- Implementation Guide

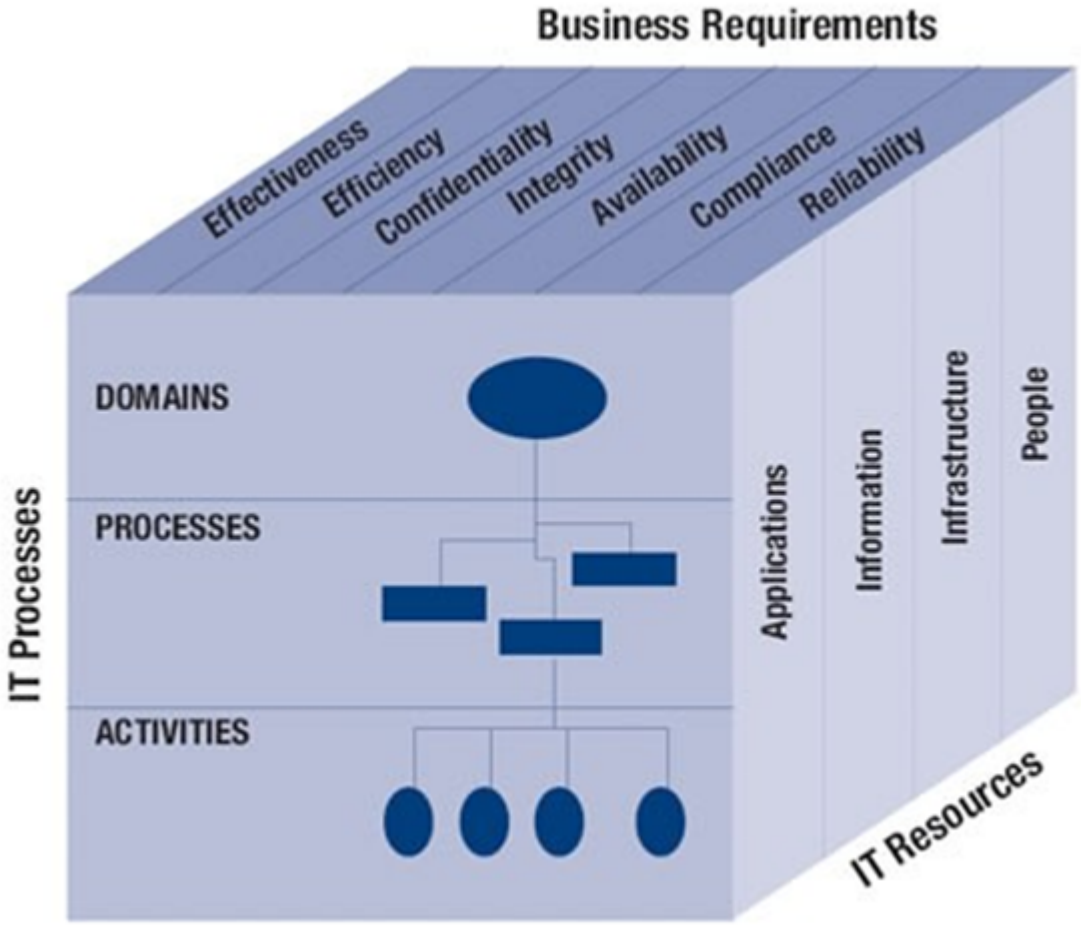
COBIT structure

From the highest level, COBIT creates a three-level structure comprised of the following segments:

1. **Business requirements** (information criteria of COBIT), including metrics such as integrity, effectiveness, availability, efficiency, compliance, confidentiality, and reliability
2. **IT resources**, including infrastructure, applications, information, and people and
3. **IT processes**, divided into domains processes

The COBIT cube

The affiliations between these components are exemplified by the COBIT cube.



All the processes are listed under four domains:

- PO: Plan and Organize
- AI: Acquire and Implement
- DS: Deliver and Support
- ME: Monitor and Evaluate

COBIT framework explained

COBIT business orientation and form of operation comprises of linking business goals to IT goals, providing info metrics and maturity models for ascertaining the level of accomplishments and noting the interrelated responsibilities of business and IT process owners. To completely understand the scope of the mode of operation of the COBIT framework, two main parameters are provided:

- **Control** is the form of procedures, practices, policies, and organizational structures designed to provide an acceptable level of assurance that business objectives and strategies will be attained and undesired incidents will be detected and corrected in a quick, concise manner.
- **IT Control Objective** is a statement of the level of acceptable results to be attained by implementing control procedures concerning a particular IT operation.

There are two distinctive classes of control models available today:

- Those of the business control model class (e.g., COSO and CoCo)
- The more focused control models for IT (e.g., DTI)

COBIT aims to close the gap that exists between the two.

Apart from being more encompassing for management, COBIT also operates at a higher level than pure technology standards for information systems management. IT governance is defined as a structure put in place to control and direct an enterprise in achieving its goals by adding value while assessing and balancing the risk versus return over IT and its processes. The basic underlying concept of COBIT framework is that control in IT is attaining by focusing on information that is required to support the business objectives or requirements, and by treating the information as a result of the combined application of IT-related resources that need to be managed by IT processes.

What are the principles of COBIT?

The six COBIT principles lay out the important aspects of IT enterprise governance:

- Meet the needs of stakeholders by aligning IT governance systems with their requirements, creating value through balancing benefits, risks, and resources.
- Effective IT governance systems should be holistic, composed of several separate components so that all factors are considered.
- Ensure that your governance system is dynamic by continuing to assess and improve it to stay relevant as the business and environment evolves.
- IT management that focuses on operations and IT governance that focuses on oversight should be separate, with defined roles that do not overlap.
- Define and prioritize IT governance system components, tailored to meet the needs of the enterprise.
- Cover all IT functions, data, and technology as a unified whole within the governance system, to meet the goals set by the enterprise.

What are the components of COBIT?

COBIT components include:

- **Framework.** Organize and categorize IT governance objectives and good practices by IT domains and processes before associating them with their respective business requirements.
- **Process descriptions.** A reference process model and common language for everyone in an enterprise.
- **Control objectives.** Use this complete set of high-level requirements for effective control of each IT process.
- **Management guidelines.** Assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.
- **Maturity models.** Assess maturity and capability per process and helps to address gaps.

Who uses COBIT?

Because COBIT 2019 is an enterprise framework, three types of people typically engage with the COBIT framework directly:

- **Management.** COBIT helps enterprise managers balance risk versus reward and control investments in an ever-changing IT world.
- **Auditors.** COBIT aids auditors in realizing an acceptable opinion on the rate of assurance on the subject matter being audited and offers advice to management on internal controls.

- **Users.** Enterprise users – typically in-house IT employees – may engage with COBIT principles in order to ensure the security and controls of IT services provided by internal or external parties.

Though not officially designated, business process owners can use COBIT to render more effective service in controlling IT processes.

COBIT certification

Users of COBIT 2019 may seek certification to ensure COBIT compliance within their enterprises. There are three options:

- **COBIT Bridge.** This 1-day course is aimed at users already certified in COBIT 5, to get them up to date on COBIT 2019.
- **COBIT 2019 Foundation.** This 2-day course requires no prior COBIT knowledge and culminates in a certification exam.
- **COBIT 2019 Design and Implementation.** Just launched with the latest version, this certification teaches how to design a customized, best-fit governance system for your company.

In August 2019, ISACA along with The Institute of Internal Auditors (IIA) is hosting a Governance, Risk, and Control Conference, with pre-conference Bridge certification options.

COBIT with other IT frameworks and processes

Enterprise IT managers frequently deploy other IT-specific frameworks and processes. Luckily, COBIT's concepts and structures play well with other popular options, including:

- CMMI
- TOGAF

Uniquely, COBIT places more focus on ***what* to do** rather than ***how* to do it,** often delegating how-to issues to other tools, frameworks, and methodologies.

Alternative governance frameworks

All governance frameworks have the same objective: implementing the best operating techniques for minimal financial losses from compliance failures. These frameworks aim to make it easier for enterprises to undergo and pass regulatory audits. Control frameworks and security standards are often exchangeable terminologies.

Taking COBIT's definitions as a basis for our parameters, COBIT classifies a framework as a Control Framework, which is described as a tool for business process owners that expedites and accelerates the discharge of their responsibilities through the provision of a supporting control model.

	ITIL	COBIT	ISO/IEC 20000
What is it?	A set of best practice publications for IT service management	A business framework for the goverance and management of enterprise IT	An international standard for IT service management system requirements
How long is it?	Five core publications totalling about 1800 pages, plus complementary publications	Core publication of 94 pages, plus 230 pages for enabling processes, and further publications	Part 1 (service management system requirements) has 36 pages, there are other parts covering other aspects
How is it seen in the market?	ITIL has a focus on internal processes. Recent versions have incorporated a service lifecycle and more focus on value and customers	COBIT comes from a history of audit and compliance. The latest version has moved towards IT service governance and management	ISO/IEC 20000 is an international standard, and the main focus is on achieving certification to demonstrate compliance to the standard
Who is it generally used by?	Any organization providing internal or external IT services. It is most commonly used in operational IT departments	Internatl IT organizations of large enterprises. COBIT is often used by strategic teams and people responsible for audit and compliance	IT organizations who want to demonstrate that they meet an externally defined standard
What is it mainly used for?	Helping to define operational IT service management processes	Defining audit and compliance requirements for IT	Demonstrating that the IT organization meets a recognized standard

On the other hand, COBIT describes a standard as a business practice or technology product that is generally accepted and endorsed by the enterprise or IT management team. There are various security standards and control frameworks that could easily substitute COBIT even if they are not as effective.

The following are security standards and control frameworks interchangeable with COBIT that can address information security requirements:

- **Federal Information Security Management Act of 2002 (FISMA),** which ensures the usefulness and efficiency of security controls over information resources that support federal operations and assets. The law also allowed for the funding of NIST to develop and improve

the least necessary controls essential for the provision of adequate security.

- **Federal Information System Controls Audit Manual (FISCAM),** which is issued by the General Accounting Office for the use of Information Systems auditors to assess the IT controls used in financial statement audits. This is not an audit standard but auditors often test the control environment in government audits using this specification. There has been increased emphasis on the use of NIST 800-53 controls and the NIST 800-53A Assessments. However, FISCAM is still utilized by government auditors and, therefore, it is advisable to understand the contents.
- **Health Insurance Portability and Accountability Act (HIPAA),** which is a federal rule that requires a series of administrative, technical, and physical security procedures for entities to use in order to assure the confidentiality of Protected Health Information (PHI). The standard was purposely non-technology specific and intended to provide scalability to small providers and large providers alike.
- **ITIL,** which comprises a set of best practices and policies for IT core operational processes such as change, release and configuration management, incident and problem management, capacity and availability management, and IT financial management. The primary contribution of ITIL is to show how controls can be implemented for service management IT processes.
- **ISO/IEC 2700:** This is the international standard for information security management. If you are running IT services, these requirements should be incorporated in the design of your management system.
- **Agile:** The Agile software development methodology splits projects into short phases, each of which delivers valuable outcomes towards the larger product and end goal. Agile has become immensely popular and widely used in ITSM improvement projects.
- **Kanban:** The Kanban methodology helps manage works in progress, to optimize and make the use of resources more efficient. Kanban can provide an excellent way to handle the workload of technical people in an IT department, ensuring that you get maximum value from your limited resources.
- **PRINCE2 and PMI:** These project management methodologies ensure value for money.

Is COBIT right for every enterprise?

As with any framework or best practice protocol, the structure is only that: a path forward. Successful implementation that results in necessary business results for your enterprise rely on a mix of widespread in-house adoption, data-driven analytics, and the right mix of people and culture. Change is not easy and change takes time – both are key factors in whether COBIT can help support your improved IT governance and security. Reading a guidebook or taking a certification course aren't enough unless the entire enterprise can promote the changes, employees can embrace the new direction, and the COBIT-inspired structure actually fits your company's needs.

Additional Resources

For more on IT frameworks and IT management, check out these BMC Blogs resources:

- BMC Business of IT Blog
- BMC Security & Compliance Blog