



Blog

What Is the COBIT Framework? IT Governance and Management



In this article

What Is COBIT?



Have questions for Legit? Ask here!

Yes

No



When you hear about IT governance, it might sound like something only big banks or massive enterprises care about. But the truth is, any organization that relies on technology needs to manage risk, stay compliant, and make smart decisions about its systems.

The Control Objectives for Information and Related Technologies (COBIT) framework gives companies a practical roadmap for handling IT operations securely and efficiently. It bridges the gap between technical teams and business goals to help organizations build a stronger cybersecurity foundation—without compromising operations.

Here's a guide to COBIT and why it matters.

What Is COBIT?

COBIT, which stands for Control Objectives for Information and Related Technologies, is a security and governance framework that helps businesses manage information technology environments. Often referred to as the COBIT security framework, it provides a set of standards that organizations can use to strengthen risk management, align IT operations with broader business goals, and improve accountability across the enterprise.

ISACA (originally the Information Systems Audit and Control Association)—a global organization focused on advancing digital trust and cybersecurity practices—developed the COBIT model. By [sponsoring and maintaining COBIT](#), ISACA offers companies a practical, structured approach to governing information and technology in fast-moving digital environments.

A Brief History of COBIT

ISACA first developed COBIT in 1996 to help financial auditors manage growing IT environments. In its early days, it focused tightly on control objectives for financial reporting, giving auditors a way to understand how technology impacted business operations.

As IT matured, so did COBIT. By 1998, ISACA released an expanded version that stretched beyond [security audits](#), offering broader IT governance and management guidance.



Over the next two decades, COBIT kept evolving to meet new business and

cybersecurity demands. COBIT 5—released in 2012—marked a significant shift by integrating COBIT standards like the International Organization for Standardization (ISO) and Information Technology Infrastructure Library (ITIL) into a unified governance framework. It became a flexible tool for managing risk, improving performance, and aligning IT with business goals.

Then came COBIT 2019. This update made the framework even more adaptable, introducing six governance principles (up from five in COBIT 5) and adding new design factors that let organizations tailor the framework to their needs. Rather than sticking to a static model, COBIT supports continuous improvement, keeping pace with evolving technologies and regulatory pressures.

Why Is COBIT Important?

Cybersecurity today demands more than just locking down systems. Organizations need a structured way to build trust, manage risks, and demonstrate control to regulators and leadership. ISACA's COBIT contributes by aligning technical operations with business goals, helping companies protect sensitive information and maintain clear accountability across IT environments.

In addition, COBIT addresses one of cybersecurity's most significant challenges: communication gaps between technical teams, business leaders, and auditors. COBIT provides a shared model that defines goals and tracks performance. This clarity supports stronger governance practices and helps organizations stay ahead of evolving regulatory demands, such as the Sarbanes-Oxley Act (SOX) and other industry standards.

The 6 COBIT Principles

ISACA built the COBIT framework on six governance system principles to make sure IT efforts create value, manage risks effectively, and stay flexible as business needs evolve.

1. Stakeholder Value

Effective governance starts with delivering value to stakeholders. COBIT encourages organizations to align IT efforts with stakeholder needs, prioritize business outcomes, and maintain a link between technology initiatives and enterprise goals.

2. Holistic Approach



Strong governance looks at the bigger picture. COBIT promotes a holistic approach that considers all aspects of the enterprise—people, processes, information, technologies, and infrastructure. Managing these elements together builds a more resilient and integrated system.

3. Dynamic Governance

Business environments change fast, and governance systems need to keep up. COBIT's dynamic governance principle encourages organizations to regularly reassess and adjust governance practices to address new risks, opportunities, and regulatory demands.

4. Governance Distinct From Management

Governance and management play different roles, and COBIT separates them. Governance sets direction, monitors performance, and evaluates outcomes, while management executes day-to-day operations. Keeping these functions distinct strengthens accountability across the organization.

5. Enterprise Needs

No two businesses face the same risks or goals. COBIT recognizes this by emphasizing that governance systems must be tailored to each enterprise's unique needs, including size, industry, compliance requirements, and risk appetite.

6. End-to-End Governance

IT governance shouldn't operate in a silo. COBIT extends governance across the entire enterprise, covering all information and technology and integrating IT governance into overall business governance.

While the six governance system principles guide how organizations use COBIT, COBIT 2019 also introduced a separate set of governance framework principles. These principles explain how ISACA structured the framework: It's based on a conceptual model of components and relationships, remains open and flexible to adapt to future needs, and aligns with major industry standards, frameworks, and regulations.

Although these framework principles shape the structure of COBIT, the six system principles mentioned above remain the foundation for applying COBIT to real-world enterprise governance.



Difference Between COBIT 5 and COBIT 2019

COBIT 5 and COBIT 2019 share the same mission—aligning IT goals with business strategies. But COBIT 2019 introduced several important updates. One significant change is adding a sixth principle focused on tailoring governance systems to enterprise needs.

COBIT 2019 also expanded the number of governance and management objectives, increasing from 37 to 40 processes and updating terminology to shift from "manage" to "managed." These updates reflect a push toward greater customization and agility as technology and business needs continue to evolve.

Beyond process changes, COBIT 2019 also introduced new governance framework principles, replaced the older "enablers" terminology with "components," and shifted its performance management model to the CMMI Performance Management Scheme, which uses maturity models. Another key addition is the design workflow, which helps organizations customize and prioritize their governance systems based on specific design factors like enterprise goals, risk profiles, and compliance requirements.

With these updates, COBIT 2019 is more dynamic, scalable, and better equipped for today's fast-paced IT and cybersecurity challenges.

Comparing COBIT to Other Frameworks

Many IT and cybersecurity professionals mention COBIT alongside other major IT security frameworks. While all aim to improve technology management and risk reduction, each has a different focus.

Here's how COBIT compares to some of the best-known options:

COBIT Vs. ITIL

COBIT and ITIL help organizations better manage IT, but they approach it differently. COBIT is a governance framework—it focuses on aligning IT with business goals, managing risk, and creating accountability. ITIL instead zeroes in on IT service management (ITSM), offering detailed practices for delivering IT services efficiently.

Another difference is compliance. COBIT audits are typically performed by ISACA Certified Information Systems Auditors (CISAs), while ITIL often relies on third-party assessment tools like the Third-Party Risk Assessment Initiative (TIPA).



COBIT Vs. TOGAF

The Open Group Architecture Framework (TOGAF) focuses on designing and managing enterprise IT architectures. It helps businesses build IT environments that support their long-term strategies.

COBIT, by contrast, aims to properly govern the use of IT and the risks tied to it. While TOGAF lays out the system blueprint, organizations use COBIT to manage, secure, and evaluate their systems. Some organizations use TOGAF and COBIT together—one to design IT architecture, the other to manage and govern it.

COBIT Vs. ISO/ECI 27001

[ISO/ECI 27001](#) is a specialized framework focused on information security management systems (ISMS). It defines controls and requirements to protect information confidentiality, integrity, and availability.

COBIT takes a broader governance view. It oversees security alongside other IT domains like operations, compliance, and performance. Many organizations combine ISO 27001 with COBIT, using ISO for detailed security practices and COBIT to govern the broader IT ecosystem.

While COBIT focuses on broad IT governance, many organizations also explore frameworks and regulations that address specific cybersecurity and compliance needs. Standards like the [NIST Cybersecurity Framework](#) and [PCI DSS version 4](#) provide detailed guidance on managing security risks. New laws like the [EU Cyber Resilience Act](#) are reshaping industry compliance expectations.

Integrating these standards alongside COBIT helps businesses build stronger, more resilient governance strategies.

Enhance COBIT Compliance With Legit Security

COBIT allows organizations to manage IT risks, align technology with business goals, and stay ahead of changing compliance demands. But maintaining strong governance systems—especially with evolving challenges like [securing CI/CD pipelines](#) and [addressing CISA attestation](#)—takes more than just a framework.

Legit Security streamlines COBIT compliance by automating governance tasks, improving visibility into security processes, and strengthening application security practices throughout the implementation of governance systems. [Request a demo](#) today.



Written by
Legit Security

Share this guide

Published on
June 04, 2025

Related ASPM Knowledge Posts

6 IT Security Frameworks for Cybersecurity

Explore common IT security frameworks to streamline compliance and strengthen your defenses. Learn how to choose one that aligns with your needs.

Read More →

What Is Governance, Risk, and Compliance (GRC) in Cybersecurity?

Explore how governance, risk, and compliance (GRC) cybersecurity fortifies organizations against threats and streamlines risk management.

Read More →



DevOps Governance: Importance and Best Practices

Strengthen your DevOps governance with the right strategies, models, and best practices. Enhance security, compliance, and efficiency in your SDLC.

[Read More](#) →

NIST AI Risk Management Framework Explained

Explore the NIST AI Risk Management Framework and learn how it helps organizations manage AI risks. Discover its core components and implementation steps.

[Read More](#) →

Understanding the NYDFS Cybersecurity Regulation

Explore the NYDFS cybersecurity regulation, who needs to comply, and its requirements. Learn how to ensure compliance with this essential framework.

[Read More](#) →

CIA Cybersecurity: The CIA Triad for Protecting Information

Explore CIA cybersecurity strategies and the CIA Triad. Deep dive into how confidentiality, integrity, and availability reduce risk.


[Read More](#) →



See More

SECURITY

ASPM

A diagram illustrating the ASPM (Automated Supply Chain Platform) architecture. It features a central network of interconnected nodes and lines. Key components include a 'Security Discovery' node, a 'Missing SAST' node, an 'AWS' logo, a 'Vulnerability Plugins' node, and a 'Google' logo. The diagram is set against a dark purple background with a grid pattern.

ASPM Platform You Can Trust

Legit is an ASPM platform that automates security issue discovery and prioritization. A trusted ASPM vendor option for your supply chain.

Read More →



S E C U R I T Y

Vulnerability Management



Vulnerability Management

Stay ahead of risks with Legit's vulnerability management. Fix issues across your SDLC with real-time visibility, prioritization, and automated remediation.

[Read More →](#)

S E C U R I T Y

Integrations



Integrations

Legit Security Integrations module highlights all the available and integrations with the Legit Security Platform.

[Read More →](#)



Blog

The graphic features the NIST Cybersecurity Framework logo on the left, with the text 'NIST' in large, bold, grey letters and 'Cybersecurity Framework' in smaller, blue letters below it. To the right is a large, stylized shield with a white keyhole in the center. The shield and background are composed of a blue hexagonal pattern, resembling a molecular or network structure. The shield is illuminated from below, creating a bright glow.

What are the Five Elements of the NIST Cybersecurity Framework?

Legit Security | This blog details the five elements of the NIST cybersecurity framework and identifies the critical aspects of protecting any org.

[Read More](#) →

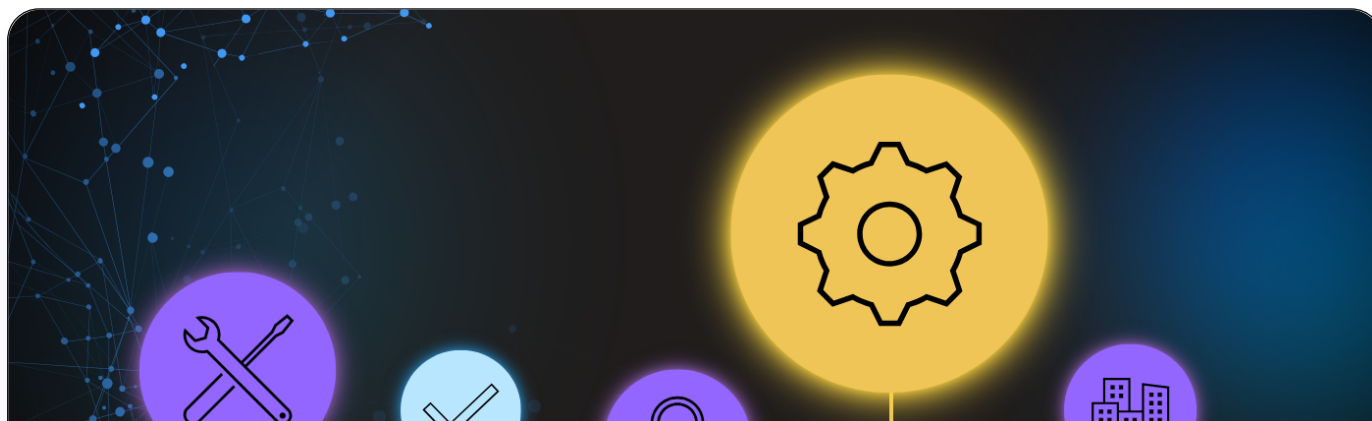




Why Legit Security Immediately Joined the New Coalition for Secure Artificial Intelligence (CoSAI)

Legit Security | Why Legit Security Immediately Joined Google's New Coalition for Secure Artificial Intelligence (CoSAI). Get details on CoSAI and why Legit chose to be a part of this forum.

[Read More](#) →



SLSA Provenance Blog Series, Part 4: Implementation Challenges for SLSA Provenance for Enterprises

This blog series covers everything from SLSA levels to real-world adoption issues. It helps enterprises confidently navigate and implement secure software.

[Read More](#) →



A Foundation You Can Trust

Get a stronger AppSec foundation you can trust and prove it's doing the job right.

[Request a Demo](#)

Platform

Unified Vulnerability Remediation

Code Scanning (SAST, SCA)

Secrets Detection & Prevention

Software Supply Chain Security

Advanced Code Change Management

Compliance

Customers

Customers



Company

[Partners](#)

[About Us](#)

[Careers](#)

[News](#)

[Events](#)

[Contact Us](#)

Resources

[Blog](#)

[Resource Library](#)

[Open Source](#)

Compare

[OX Security](#)

[ArmorCode](#)

[Apiiro](#)

[Cycode](#)

Learn

[ASPM Knowledge Base](#)

[SDLC Security](#)

[DevOps Security](#)

[GitHub Security](#)

[Secure Software](#)

[Supply Chain](#)

[Application Security Posture Management](#)



[Privacy Policy](#)

[Terms of Use](#)

© 2025 Legit Security

