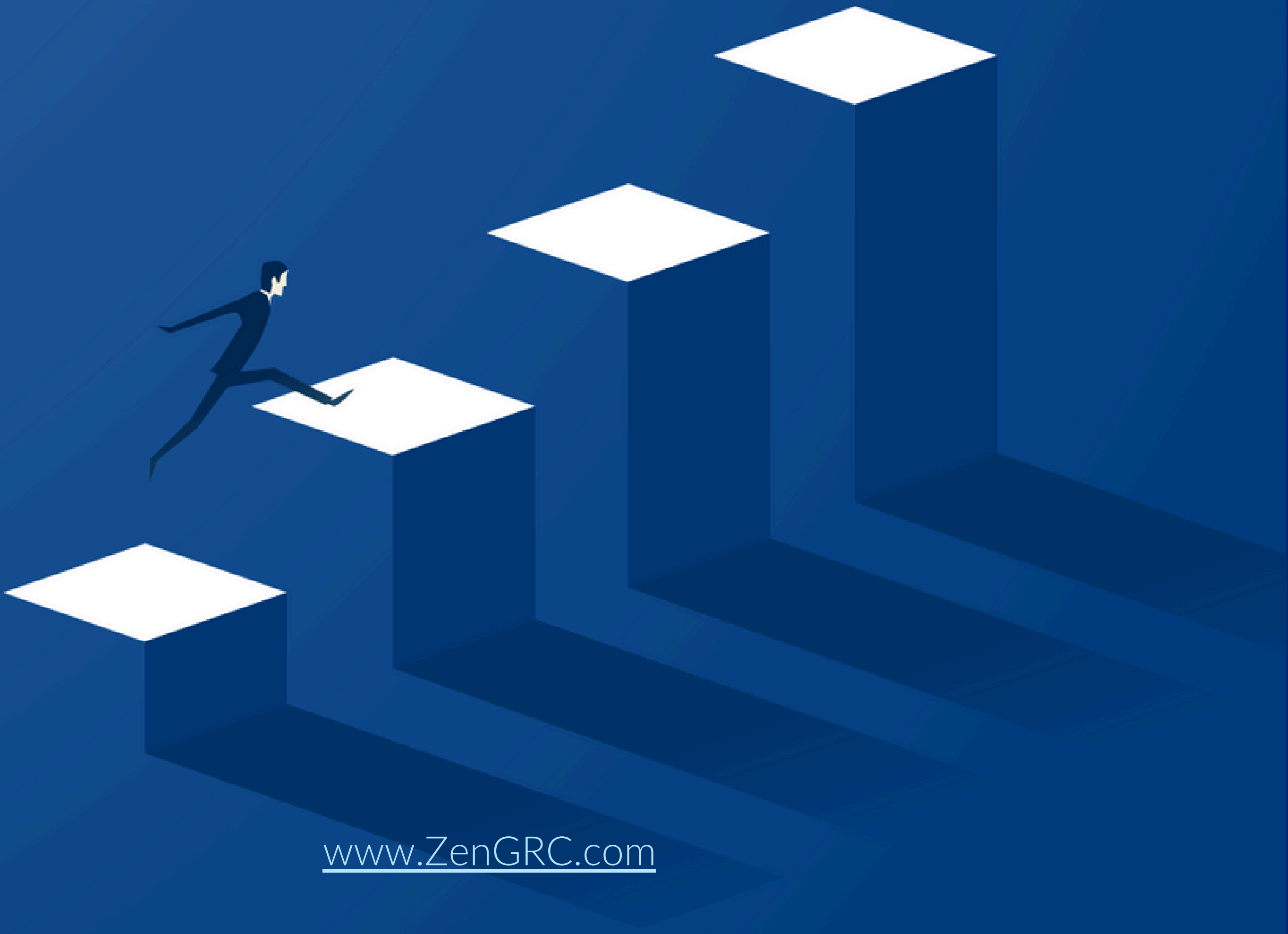
ZenGRC

Preparing for a COBIT Audit

PART ONE: ALIGN, PLAN, AND ORGANIZE

A Step-by-Step Guide



www.ZenGRC.com

In today's enterprises, information technology goals and business goals go hand-in-hand—or at least, they ought to.

The COBIT (Control Objectives for Information and Related Technologies) framework is designed to help your organization maximize its governance in all areas while minimizing risk, especially IT-related risk.

Developed by the Information Systems Audit and Control Association (ISACA), COBIT is a complex framework with 37 principles.

Compliance is a lengthy and complicated journey, requiring a dynamic approach to enterprise governance and a recognition that, in the digital age, IT is a central component of business from end to end.

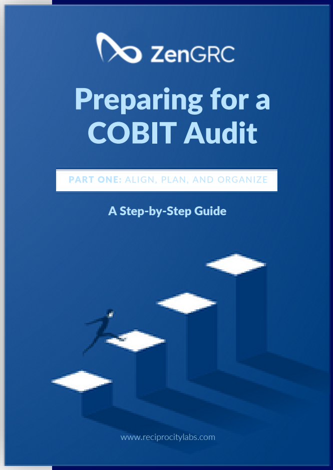
Your business's success at obtaining the coveted COBIT certification will depend in large part on how well it has adopted the "digital" mindset.

To make the task easier, we've compiled this step-by-step checklist with the help of our expert COBIT audit team. We are presenting it in three parts, each aligned with a COBIT area:

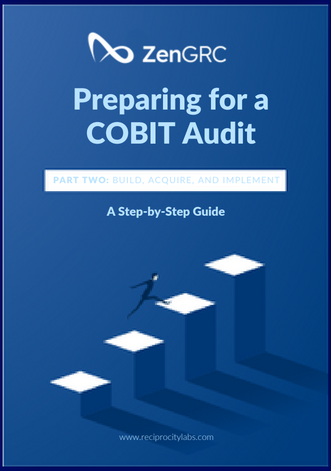
13 "ALIGN, PLAN, AND ORGANIZE" PRINCIPLES

10 "BUILD, ACQUIRE, AND IMPLEMENT" PRINCIPLES

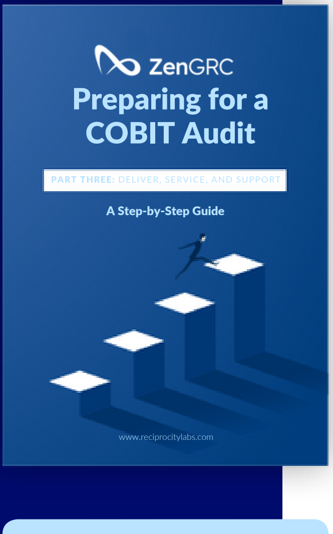
6 "DELIVER, SERVICE, AND SUPPORT" PRINCIPLES


ZenGRC
Preparing for a COBIT Audit
PART ONE: ALIGN, PLAN, AND ORGANIZE
A Step-by-Step Guide
www.reciprocitylabs.com

PART 1


ZenGRC
Preparing for a COBIT Audit
PART TWO: BUILD, ACQUIRE, AND IMPLEMENT
A Step-by-Step Guide
www.reciprocitylabs.com

GET PART 2


ZenGRC
Preparing for a COBIT Audit
PART THREE: DELIVER, SERVICE, AND SUPPORT
A Step-by-Step Guide
www.reciprocitylabs.com

GET PART 3

Work your way through these requirements using our detailed explanations, questions to consider, and suggested documents to have on hand, and you should be well prepared at audit time.

COBIT:
An Overview

EVERY ENTERPRISE STRIVES TO MEET THE NEEDS OF ITS STAKEHOLDERS AND GENERATE VALUE. THESE GOALS ARE ALSO THE DRIVERS FOR COBIT, AS REFLECTED IN ITS SIX OVERARCHING PRINCIPLES:

1. **Provide stakeholder value.**

2. **Take a holistic approach.**

3. **Develop a dynamic IT governance system.** This means that each time your organization changes a design factor—whether it's how you select computer systems, manage projects, or manage change in your organization—it also considers the impact on governance and updates its governance program accordingly.

4. **Distinguish governance from management.** Essentially, governance is strategic and long-term, and concerns your business's structure. Management concerns day-to-day operations.

5. **Tailor your governance system to the enterprise's needs.** There is no "one size fits all" with COBIT; each organization's governance system will be unique, just as every business is different.

6. **Make sure your IT governance system covers your entire organization, end to end.** It must address not only IT functions, but also the technology processing and information systems developed by your company to achieve its goals.

What Your Governance System Should Include

COBIT 2019 OUTLINES SEVEN KEY AREAS THAT EVERY IT GOVERNANCE SYSTEM SHOULD INCLUDE

1. Processes and organization
2. Organizational structure
3. Principles, policies, and procedures
4. Information flow, type, and purpose
5. Organizational culture, ethics, and behavior
6. Employee skills and competencies
7. IT infrastructure and applications

If your organization changes anything in any of these areas, your governance system should change, as well.

What Your Auditor Will Examine

A COBIT AUDITOR WILL BEGIN THEIR REVIEW BY EXAMINING

- **The size and structure of your enterprise.**
  Size matters in governance; the larger your organization, the more complicated and time-consuming each project and process will be.

- **Your governance stakeholders.**
  Do you have a board? Does the board review IT-related spending, recommend IT projects, and align those projects with business strategies? Do they provide IT guidance or IT initiatives? Do they understand IT solutions and ensure that yours conform to your organization's governance objectives, regulatory requirements, and risk management plan?

- **Your business partners.**
  What agreements do you have with business partners and managed service providers? Do these documents stipulate what types of services they will provide? How do you ensure their regulatory compliance and data security?

- **Your enterprise's IT strategy.**
  How well does it conform to overall business goals? Do you have a technology adoption plan for internal (employee) and external (customer) use?

- **Your risk profile.**
  Do you have a risk management system? What is it? How do you identify, categorize, rate, and address risks? Who manages those risks?

- **Your IT-related issues.**
  How do you identify and overcome these challenges?

- **Your threat landscape.**
  What is your organization's threat tolerance level, and is your current vulnerability appropriate for that tolerance? What security software do you use? How do you address cyberthreats—malware, phishing, viruses, ransomware?

- **Compliance.**
  To which regulatory and compliance frameworks does your organization adhere? Whether it's PCI DSS, GDPR, ISO, or something else, your enterprise should be in conformance or at least working toward compliance.

- **Your IT sourcing model.**
  What are your procurement procedures? How do you outsource IT? Who are your vendors, and what services do they perform for you? How do you engage with them? How do you ensure that they are secure? What access do you provide them to your data and systems? If a vendor is breached, who takes responsibility? Does the vendor communicate with your exposed customers? How well do you understand each vendor's security systems and policies and procedures?

- **Your IT implementation methods.**
  How do you implement IT projects and initiatives? Do you have a project management office? Is it mature—does it use an established methodology?

SPECIFICALLY, YOUR COBIT AUDITOR WILL MEASURE YOUR ENTERPRISE'S IT GOVERNANCE AGAINST THE FRAMEWORK'S PRINCIPLES. AS MENTIONED BEFORE, WE'VE DIVIDED THE MOST SALIENT ONES INTO THREE PARTS, STARTING WITH THE "ALIGN, PLAN, AND ORGANIZE" GROUP.

Align, Plan, and Organize

APO01:

Managed I&T Management Framework

This principle concerns the framework used by your information and technology management team.

ô Is your IT framework compatible with COBIT? Do you use NIST 853 Rev 4 and ISO 27001/27002? How compliant is your organization with those frameworks?

APO02:

Managed Strategy

This principle concerns the design and integration of your IT strategy.

- ô What targets or objectives does your IT strategy define? How well does your organization meet these goals? How do you measure the results?
- ô Have the partners in your business integrated the IT strategy into their plans and goals?
- ô How does the IT strategy dovetail with your enterprise's overall business strategy? Do all IT purchases and plans help to increase revenue, enhance customer satisfaction, and so on?

APO03:

Managed Enterprise Architecture

This principle concerns management of your enterprise's IT architecture, including cloud-based solutions.

- ô Who is your cloud provider? How does that provider secure its systems and your enterprise's data?
- ô Do you still run mainframe systems? Are they located on or off premises? How are they managed—in-house, or by a third-party vendor? Are the duties performed in these systems segmented?
- ô What security programs or software do you use for your in-house systems? How often are they scanned or patched?
- ô How do you manage your architecture? Is there an architecture review board to determine your strategies, sign off on initiatives and changes, and monitor compliance?

APO04

Managed Innovation

This principle concerns the role of innovation in your enterprise, and how the organization manages new IT products, procedures, and services.

- What are the drivers for change in your organization? How are those drivers considered when new IT solutions are proposed? This includes software, hardware, cloud-based solutions, vendors, and changes in policies and procedures.
- When your enterprise launches a new product or service, how is it brought to market? How does your business ensure that customer support is available for that new product or service? Your customer support strategy might include new technologies such as artificial intelligence, changes in business operations, or something else.
- How does your enterprise manage changes to internal systems? What are the procedures for introducing new programs or software for internal use?

APO05:

Managed Portfolio

This principle concerns the management of your company's IT portfolio.

- How are projects and initiatives scrutinized, approved or denied, and tracked? Who oversees this process?
- Do you have a project management office? If not, you should establish one. Otherwise, you don't know where your organization's IT money is going—a fail with your auditor.

APO06:

Managed Budget and Costs

This principle concerns your enterprise's adherence to its budget for IT-related expenses.

YOUR AUDITOR WILL WANT TO SEE DOCUMENTATION OF

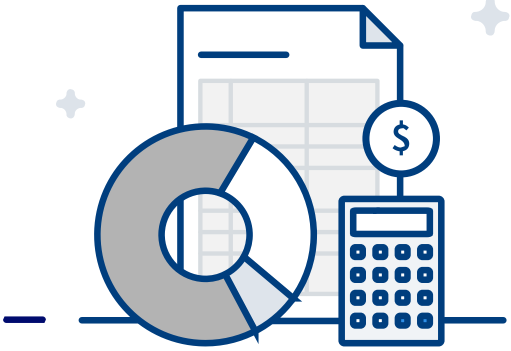
ô Your IT portfolio

ô Enterprise financial statements

ô IT budget and expenditures

ô Successes and/or failures of IT projects

ô Relationship with vendors



APO07:

Managed Human Resources

This principle concerns your organization's procedures for hiring and training personnel to support IT projects.

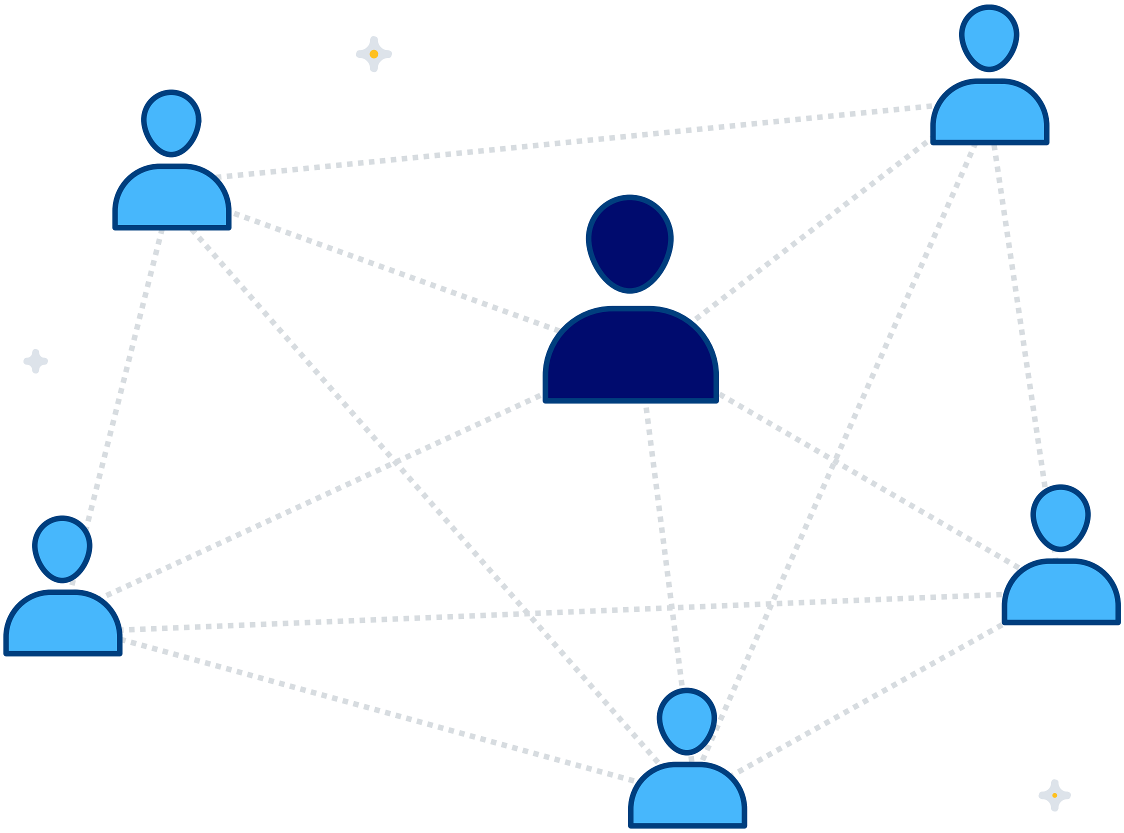
ô Do people in IT-related positions have the necessary skills for their roles?

ô Does your organization pay market rates? In some states, workers have sued because they were not paid fairly for their roles.

ô Does your HR office provide security awareness training to employees?

ô Does your HR budget include development training to keep IT personnel current?

ô How does your HR office recruit for IT-related positions? What are your hiring and firing policies and procedures?



APO08:

Managed Relationships

This principle concerns your organization's management of its relationships with its business partners and vendors.

ô What types of contracts and obligations does your organization have with your vendors? When did your enterprise last review these contracts?

ô What are your vendors' obligations and responsibilities regarding the security of your information? Do they get personally identifiable information (PII) from you? If so, how do they manage and secure it?

ô How often are your business partners and vendors audited, if at all? Do you perform this function, or does someone else?

APO09:

Managed Service Agreements

This principle concerns the contracts between your enterprise and its customers, partners, and vendors—anyone doing work on your organization’s behalf.

- ô How do you review these contracts, and how often?
- ô Do you use the EU-US Privacy Shield framework? If so, do your vendors comply with it? How do you assess this, and how often?
- ô Do you re-review contracts when they are amended?
- ô Has your attorney given you an actionable checklist for contract review? If so, it might require that your contracts:

  - ô Are signed and dated
  - ô Contain the correct legal names of companies
  - ô Require indemnity or liability insurance
  - ô Require workers’ compensation insurance
  - ô Are finite, with an end date
  - ô Describe ownership, protection, and transfer of intellectual property
  - ô Require confidentiality
  - ô Reference data privacy and spell out roles and responsibilities in the event of a breach
  - ô Clearly spell out payment terms and timing of payments
  - ô Detail the process for termination of services
  - ô Specify the terms for vendor audit and risk review
  - ô Include a business continuity plan to be implemented in the event of a breach

APO10:

Managed Vendors

This principle concerns your vendor management process and vendor audits.

ô What is your vendor management process?

ô Do you audit your vendors? How? How often?

ô Do you audit your vendors in person, using online assessments, or both?

ô Do your vendor audits include the following?

> ô Contractual agreements
>
> ô Security
>
> ô Access to your systems—is it general or for a specific scope of work? Is it permanent or temporary?
>
> ô A requirement for Service Level Agreements

ô Do you track and monitor the performance of your vendors, especially those managing your systems?

APO11:

Managed Quality

This principle concerns whether your enterprise stakeholders are getting the quality they expect from your enterprise, and the degree to which quality is integrated into and across your organization.

ô What is your quality management system?

ô How do you view your risks?

ô Do you conduct quality reviews and audits?

ô Do you have an IT Infrastructure Library (ITIL) in place? If not, now is a good time to start—ITIL programs excel at quality management.

ô How does information flow through your organization?

ô Who is responsible for communicating quality issues or defects?

ô How do customers view your organization's quality? How do you measure this?

ô Do you have an ongoing quality maintenance plan?

ô Is your quality maintenance system tied to your Key Performance Indicators (KPIs)?

ô Do you document downtime (especially unexpected downtime), maintenance issues, and security incidents? Your auditor will want to see these records.

ô Is quality integrated into your software development life cycle? Does a testing team evaluate new releases and changes? Specifically, what is the process for testing patches or changes to systems, servers, and applications before moving them into production?

ô What are your quality requirements for third-party vendors? Do you hold review meetings with them? Have you instituted a formal dispute process with your suppliers, including the process and timeline for resolution?

APO12:

Managed Risk

COBIT, like some other frameworks, is very focused on risk management*—the identification, assessment, and reduction of risk tolerance, as well as the integration of risk management across the enterprise and the ability to balance those risks against costs and benefits. The primary goal is to manage business risk, ensure that your organization uses the metrics that are necessary to manage risk well, and implement processes and procedures to manage risk by transferring, mitigating, or accepting it.*

ô How does your risk management program cover critical business objectives and services? Do you perform assessments or hold periodic risk management meetings?

ô How do you compare incidents not identified in your risk assessment against total organizational risk?

ô How often do you update your risk profile (e.g., biweekly, monthly)? What is your process?

ô Do you evaluate the costs of risk management, including hours of work lost to mitigating, reducing, or accepting risk as well as to service interruptions, planned or unplanned? Beyond lost work hours, what are the costs conferred by interruptions of business operations and reputational embarrassment?

ô How do you classify risks? Be prepared to present your risk classification system.

ô Has the organization as a whole been trained in risk management?

ô Has your enterprise conducted a survey or analysis of historical risks? Recurrent risk could indicate a quality issue.

ô Do you scrutinize agreements with vendors and partners to ensure that they actively manage their risks, and do you keep those agreements up to date?

ô Do you update your risk management processes regularly, and whenever there are specific changes or conditions? Do you know what those specific conditions are?

ô Does your risk management team evaluate potential gaps in controls, as well as control effectiveness, inconsistencies and redundancies, and remediation of risks? Are the findings reported in monthly or biweekly reviews?

APO13:

Managed Security

This principle concerns how your enterprise defines, operates, and monitors information security throughout the organization. Security management ties into your business's risk management plan and processes, applications, processing infrastructure, data security, and data privacy.

ô Do you require new vendors to undergo a security assessment? This is critical if those vendors have access to your applications and are processing data on your behalf.

ô Do your business impact analyses or business requirements include security? For instance, if you implement new systems, software, or cloud services, do you talk with the providers to ensure that their security requirements and business processes align with your security needs?

ô Have you defined the scope and boundaries of your information security management? What are the characteristics of your security frameworks? What locations, assets, and technologies do they cover? What is excluded, and why?

ô Does your security management include knowledge transfer of infrastructure and applications, and training for your IT security team?

ô Is there an approved process for communications between the information security team and business staff? This is essential any time the security team makes a change that could affect the system's ability to operate.

ô Does your enterprise have an IT security plan that describes how security risks are to be managed and handled? Does everyone know their roles and responsibilities?

ô Is there a clear separation of duties in IT development? Is the security plan "baked in" to the process, i.e., integrated into development from the very start?

ô Is security built into your enterprise's architecture? Do you know the details, and do you have a complete enterprise architecture inventory?

ô Is IT security built into the design and development of all your processes, practices, policies, and procedures?

ô Does your organization provide mandatory security training to promote awareness among all employees? How do you track and monitor conformance?

- How do you implement, design, and monitor all your organization’s information security policies and processes?
- How do you evaluate and detect security-related events, incidents, and issues?
- Is the effectiveness of your security plan one of your KPIs?
- Do you undertake regular information security reviews based on your IT security policy and objectives? Do those objectives include privacy?
- Do you conduct regular audits of your information security management system?
- Do you update your security plan when changes are made?
- How do you assess the security of your third-party vendors?
- How much has noncompliance with security requirements cost your business?
- What remediation issues have you encountered?
- How quickly does your enterprise respond to security incidents? How do you manage data and support changes to the environment in these responses?
- When and how do you apply patches and updates to your systems and applications?
- What is your process for emergency changes?
- Is your operating system up to date?
- Are new development projects assessed for information security?
- Do you have secure boundaries (firewalls, demilitarized zones) around FedRAMP-compliant systems?
- What are your policies and procedures for data security and privacy, and what is your associated governance structure? When do you review and update these?
- Do you have a sequence plan for data quality improvement?
- Do you monitor your goals and objectives for data security and privacy?
- Do you report to stakeholders on information security and data quality issues?
- Do you have processes to remedy these issues?
- Do you continuously scan your systems for security risks?
- Do you identify and rank vulnerabilities?
- What are your data cleansing policies and procedures? Do you cleanse your data history?
- Where do you keep your log files?
- Do you have server colocation and backup sites? Are they all secure?
- What security software do you use? Where is it installed?

APO14:

Managed Data

As data privacy laws become more common, managing data becomes increasingly important.

Every enterprise needs formal, sustainable management of all data assets and the ability to provide data to its owner upon request.

ô Do you have a data privacy officer or someone designated for data management?

ô Does your IT security policy include data management?

ô Do you have a data management policy? It should spell out roles and responsibilities for employees in data management, describe the structure of data governance and communications, and mandate compliance with applicable regulatory frameworks such as GDPR, HIPAA, NIST, or PCI DSS.

ô If you don’t have a data management policy, do you have a strategy?

ô What is the management process for data changes? What technologies and metrics do you use to evaluate the effectiveness of your data management program? How often do you review those metrics?

ô Does your enterprise have a data privacy taxonomy—a documented process to build, maintain, and manage a data management business glossary? Is it integrated with data requirements and definitions for a consistent shared language across the organization?

ô Is your data encrypted at the user, file, application, and/or network level? How do you handle metadata? Do you document metadata requirements? Do you have a process for categorizing metadata properties and standards?

ô Do you conduct data privacy impact analyses? Is there a repository for metadata? Who has access to it? What are the architectural layers of that repository? How are changes made?

ô Have you deployed an integrated metadata model across the organization and all platforms? Are metadata types and definitions supported and aligned with each other? What metrics do you use to evaluate the accuracy of your metadata?

ô What are the processes for making changes to data and metadata?

ô How do you verify the accuracy of your information? How do you correct errors? Do you have a data quality review process?

ô Are policies, procedures, and governance controls anchored to data management, data quality, data mandates, metadata, and your development lifecycle? Is there a sequence plan for data quality improvement across the organization?

ô Is your data profiling process standardized with methodologies, processes, practice tools, and templates? Are these linked to your governance controls? Are all data processing activities evaluated, documented, and formalized based on historical results or activities?

ô How does your enterprise store data? How is data systematically monitored and analyzed with respect to retention timelines?

ô Is data access granted only to individuals who need it?

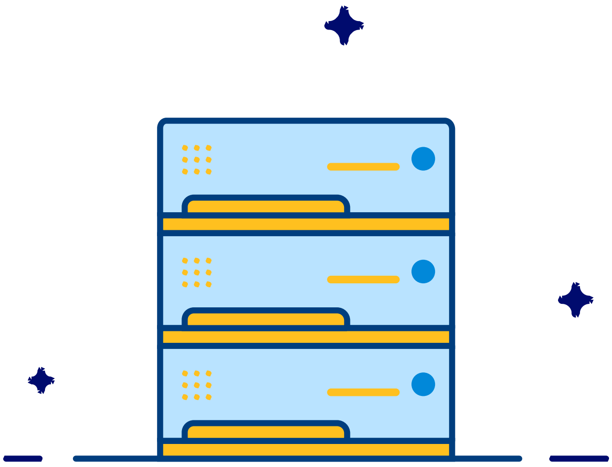
ô Do you periodically review data quality management and measurement reports to determine data volatility?

ô What's the process for changing incorrect historical data? What are your policies and procedures regarding access, controls, and governance for the transmission and modification of historical and archived data?

ô What are the data management policies in your service level agreements with third-party vendors?

ô What is your process for destroying systems containing critical data?

ô Do you collect data only for specific purposes? Is that data tied to a governance structure?



ô Do you have a data warehouse repository? How do you ensure that the data meets analytical needs or supports business processes or changes in the data set?

ô What is the process for backing up and restoring critical data? Are those processes linked to your security management objectives?

ô Who manages your onsite and/or offsite data storage and backup systems?

ô How often are data volumes or data storage replenished? How long are stored and backup data files kept? Is there a testing schedule for data backups?

ô What is your process for restoring data while minimizing interruptions to the business?

ô What is your process for defining, and communicating to the business, your organization's

ô Data strategy

ô Data profiling methodologies

ô Data assessment approach

ô Data cleansing processes and procedures

ô Data archiving and retention policies

ô Data backup and restoration processes

ô Data vocabulary (using the data glossary)

ô Metadata management

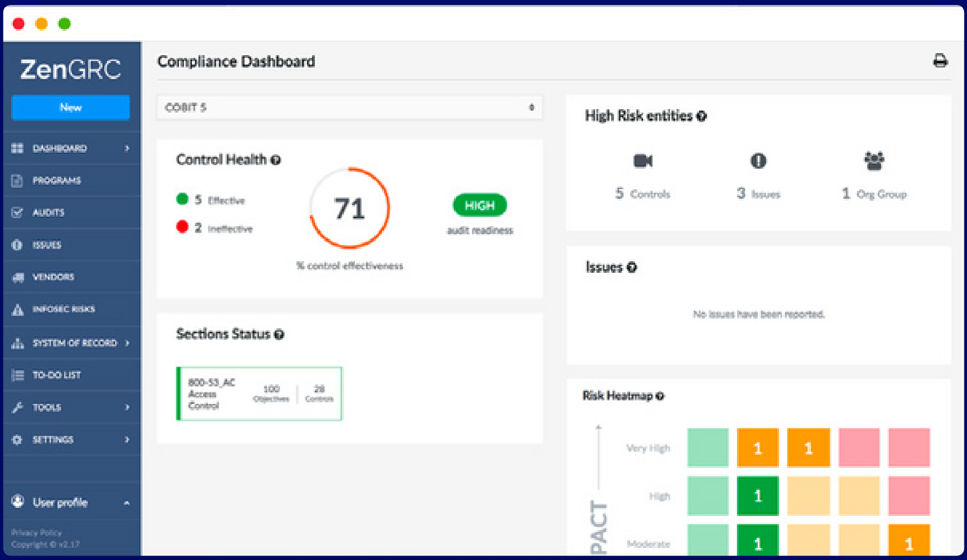
ô Overall data management strategy, roles, and responsibilities

An Exhaustive, Complex Framework

COBIT is one of the most detailed and expansive frameworks in IT governance today. Because it applies not just to the IT department but to technology planning and operations throughout the enterprise, its mandates are incredibly detailed. And because it focuses on governance (the *how* of business) rather than management (the *what*), COBIT can be confusing for those trying to implement its mandates.

But businesses go for the COBIT gold because it's worth it. A COBIT certification positions your enterprise to derive maximum value from its technologies in the impending connected age—when, by necessity, all organizations will be not just digital, but digital-first.

It’s not an easy task. In this ebook, we’ve covered just one of three essential sections of the COBIT framework that are crucial for passing an audit. We cover the remaining two sections in subsequent publications. And COBIT 5 has just undergone changes to become COBIT 2019, for which auditing guidelines will soon be released.



If you’re trying to keep track of all these moving parts using spreadsheets, you’re doing it wrong. The digital age calls for a fully digital solution

—one that not only tracks your COBIT compliance for you, but contrasts and compares those requirements with other frameworks and displays the results on user-friendly dashboards. Then, with your COBIT compliance assured, you can relax and focus on the business at hand—the Zen way.

About ZenGRC

Founded in 2009, ZenGRC has reimagined bulky legacy GRC software to meet the demands of today's dynamic data-driven ecosystem. The company is recognized for its forward-thinking cloud platform, ZenGRC, that elevates risk,compliance, and audit from a burdensome expense to a strategic advantage. ZenGRC is headquartered in San Francisco.

Contact a ZenGRC expert today to request your **free demo**, and embark on the worry-free path to regulatory compliance—the Zen way.

www.zengrc.com/resources
engage@zengrc.com
(877) 440-7971