RECIPROCITY

Preparing for a COBIT Audit

PART TWO: BUILD, ACQUIRE, AND IMPLEMENT

A Step-by-Step Guide

www.reciprocitylabs.com

With the lengthy “Acquire, Plan, and Organize” part of your COBIT audit preparation complete (covered in part 1 of our three-part COBIT audit guide series), you are now ready for the action phase.

> **These 10 criteria invite you to consider the function and management of IT—the linchpin of value—across your entire enterprise.**

As always, be prepared to provide evidence to support your efforts and results for each principle.

Build, Acquire, and Implement

BAI01:

Managed Programs

This principle concerns your management of IT programs, including how you define your requirements, manage solutions to build or buy, and determine what you need to know when implementing a new program.

CONSIDER THESE GENERAL PROJECT MANAGEMENT CONCEPTS:

- Organizational change
- The abilities and capacity of the systems you're implementing
- Change management
- Quality assurance and acceptance
- Configuration of the system you are purchasing

Your auditor will likely examine the investments in your portfolio to make sure they align with the enterprise's strategy. They will consider whether you implement programs and projects in phases: initiation, planning, control, execution, and monitoring or operationalization(sustainment)—the program lifecycle. After implementation, you push each project into production, followed by maintenance—covered in Part 3 of our COBIT Audit ebook series.

FOR THIS CATEGORY, YOUR AUDITOR MIGHT ASK:

○ What is the process for program approval?

○ Are all enterprise projects and programs included in your portfolio?

○ What products and services does your organization offer to clients?

○ What is your budget for IT programs and projects?

○ Do you have a charter or plan for each project? What's the scope of that plan?

○ Who is involved in your projects or programs? Are your stakeholders involved? Do you have adequate sponsors for each?

○ Does each project have a business justification? Is there a schedule for each? Is each project interdependent with other ongoing projects or programs?

○ If the scope of a program or project changes, do you update the associated business case, program schedule, and budget?

○ How does your organization benefit from its programs and projects? Have you defined the benefits from existing ones? How do you do this?

○ How do you report on your programs? Reports should include

- ○ Schedules
- ○ Funding
- ○ Costs
- ○ Functionality
- ○ User satisfaction
- ○ Internal controls
- ○ Compliance
- ○ Security
- ○ Roles and responsibilities

○ Does each project have monitoring and controlling? The project management office needs to know early on if a project is not performing as expected.

○ Do you have "stage gates" or some other mechanism for reviewing projects at each stage before transitioning to the next?

○ Have you identified the risks associated with each project or program, and determined a response to each?

○ How do you ensure that project closure occurs in an orderly and documented fashion? If closure brings changes to the organization, do you train employees in those changes? Your auditor will want to see supporting documentation to ensure that projects are closed out appropriately.

BAI02:

Defining Requirements

This principle concerns the process of identifying solutions and analyzing requirements before acquiring or creating a product or service, or before implementing a new program. You will be asked to consider applications, processes, information, data, infrastructure, and services, and the requirements for developing any of these items.

- ○ Have you identified the stakeholders in the programs for which you are developing requirements?
- ○ Do you have a charter or requirements document? It should address:
  - ○ How information is prioritized
  - ○ Technical requirements
  - ○ Business and functional design requirements
  - ○ Policies, procedures, and standards
  - ○ Architecture
  - ○ Technical information and technology plans to support the requirements
  - ○ Security
  - ○ Regulations
  - ○ Compliance
  - ○ Competencies of individuals supporting the project, program, or deliverable
  - ○ Information controls
  - ○ Business continuity
  - ○ Operationality and usability
  - ○ Safety
  - ○ Confidentiality and data protection
  - ○ Auditability—do you have an audit trail associated with your requirements?
- ○ Are any automated processes associated with the program/product/service? Those processes may have their own requirements.
- ○ Will the program/product/service affect compliance, regulations, or commercial contracts, including with vendors or partners?
- ○ Does your industry or enterprise stipulate process requirements?
- ○ Can you track and control the scope of your requirements?
- ○ Have you documented changes in your requirements, and are those changes readily visible?
- ○ What is your software policy? Are patching, protocols, encryption, and software security defined in your requirements?

BAI03:

Managed Solutions: Identification and Building

This principle concerns the establishment and maintenance of your products and services—your technology, business processes, and workflows—in alignment with enterprise requirements.

SPECIFICALLY, FOR EACH PRODUCT/ SERVICE, YOU MUST MANAGE THE

- Configuration
- Test preparation
- Testing solutions
- Business processes
- Applications data and information
- Agility, scalability, and cost efficiency of solutions

Your auditor will examine how your organization's high-level design and specifications are applied to your solutions. They will also consider the requirements for adoption, such as:

○ Redesign or development of new business processes

○ Supporting services

○ Applications

○ Workflows

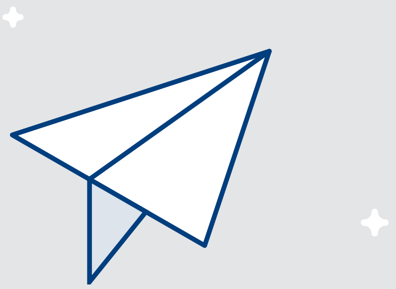
○ Infrastructure

○ Hardware

○ Additional software

○ Information repositories

○ Databases



YOUR AUDITOR MIGHT ASK:

○ What activities are associated with the workflow of your solution?

○ What is the application's design? This includes

○ Business processing rules

○ Automated controls

○ Data definitions

○ Business objects

○ Use cases

○ External interfaces

○ Design constraints

○ Licensing and legal standards

○ Internationalization

○ Are data inputs and outputs automated? Does this process use an application programming interface or batch processes? Where does the data come from?

○ Do you validate the data and ensure that it is secure and moving properly?

○ Do you use automated data exchanges? Do you test these and document the testing results? Do you have a data flow diagram?

○ What are your procedures for data storage, recovery, and retrieval?

○ Is there a special interface between the user system and the application? If so, have you documented it?

○ If design weaknesses, inconsistencies with enterprise requirements, or missing design elements were identified, did you document and explain these issues?

○ Do you audit transactions and identify causes of processing errors?

○ Do you document the design of new business processes and updates to existing processes or procedures?

○ Have you documented the roles, service level agreements, security standards, licensing, and contractual obligations for any third parties involved with solution development?

○ Can you track changes related to development, design, performance, and quality reviews?

○ Do you document customization and configuration changes?

○ Is there an approval process, perhaps with a change review board, for configuration changes that support the solution?

○ Do solutions have operation manuals and release notes?

○ Do you maintain an audit trail during configuration and integration of software?

○ Does the business verify that solutions meet specific needs and requirements, and then sign off on the solutions?

○ Do you include all new solutions in a product and service catalogue?

○ Do you test solutions? Do you have test plans, use cases, and, if using software, scripted test scripts?

○ If errors are found during testing, are they documented? Do you log the management of those errors and keep the log until the errors are fixed? Do you repeat testing until all issues are resolved?

○ Do you establish periodic reviews to ensure that patches and upgrades are applied? Do you review and identify vulnerabilities and risks, and verify that solutions continue to meet security requirements?

○ Do you have tiered service levels for solutions, such that personnel are stratified by their ability to help users if issues arise?

BAI04:

Managed availability and capacity

This principle concerns the systems' needs and availability, both current and future. It evaluates your long-term planning for the growth and scalability of your systems' capacity, availability, and performance.

○ Have you identified all your critical services and their availability and capacity?

○ Have you identified future systems that will come online? Are they applications or infrastructure? Do you have a plan for them?

○ Do you keep logs and collect data regarding use of your critical systems—how many users at once, peak use times, when systems go down, and the causes of failures?

○ Does your performance monitoring system identify the hardware or other tools necessary to sustain the current level of use of your system or network?

○ Do you have a documented escalation process in case of emergency?

○ Does a third-party vendor monitor your network traffic and maintain log files for your scrutiny? Those logs should include trend analyses and should track capacity, outages, redundancies and backups, and security incidents and events.

BAI05:

Managed organizational change

This principle concerns how your organization manages risk.

- ○ Do you have a formal change management process? ISACA, the organization administering COBIT, recommends the Prosci 3-Phase Process for change management.
- ○ Do you have a communications or change management team? How integrated and involved is that team when changes happen? Are its members mentored, trained, and coached?
- ○ How are changes communicated to those who need to know?
- ○ Do your projects end with a “lessons learned” analysis?

BAI06:

Managed IT Changes

This principle concerns management of all IT-related changes in the control environment.

YOUR AUDITOR WILL EXAMINE DOCUMENTATION RELATED TO:

- ○ Standards
- ○ Emergency outages
- ○ Maintenance windows
- ○ Systems maintenance
- ○ Business processes
- ○ Applications
- ○ Infrastructure
- ○ Changes in standard policies and procedures
- ○ Impact assessments
- ○ Prioritization of systems
- ○ Authorization of changes and of new systems
- ○ Change tracking, reporting, and documentation

BAI07:

Managed IT Changes Acceptance and Transitioning

This principle concerns your organization's acceptance and operationalization process for proposed IT changes.

YOUR AUDITOR WILL CONSIDER

- IT change implementation plans
- System data conversion plans
- Acceptance testing
- Communication plans
- Release management plans and preparation
- Segregation of duties for production changes—ensuring that developers are not pushing changes into production
- Testing results
- Implementation processes, including
  - ○ Installation
  - ○ Verification of systems and software
  - ○ Strategy for transitioning from testing into production
  - ○ Continuity plans—are yours up to date?
  - ○ Rollback strategy and recovery process in case of failure

YOUR AUDITOR MIGHT ASK:

- ○ Is everything in your implementation plan auditable?
- ○ Do data conversions undergo review?
- ○ Are procedures for maintaining data conversions subject to approval, verifying that the data has been cleaned and managed properly before it is transferred from another environment?

○ Are there clearly defined roles and responsibilities around the acceptance and transition of IT changes? Are activities reviewed periodically to ensure that access levels are correct?

○ Do you perform data retention planning and backup?

○ Does your data conversion plan address

  ○ Selection, conversion, and identification of data

  ○ Issues resolution

  ○ Data integrity

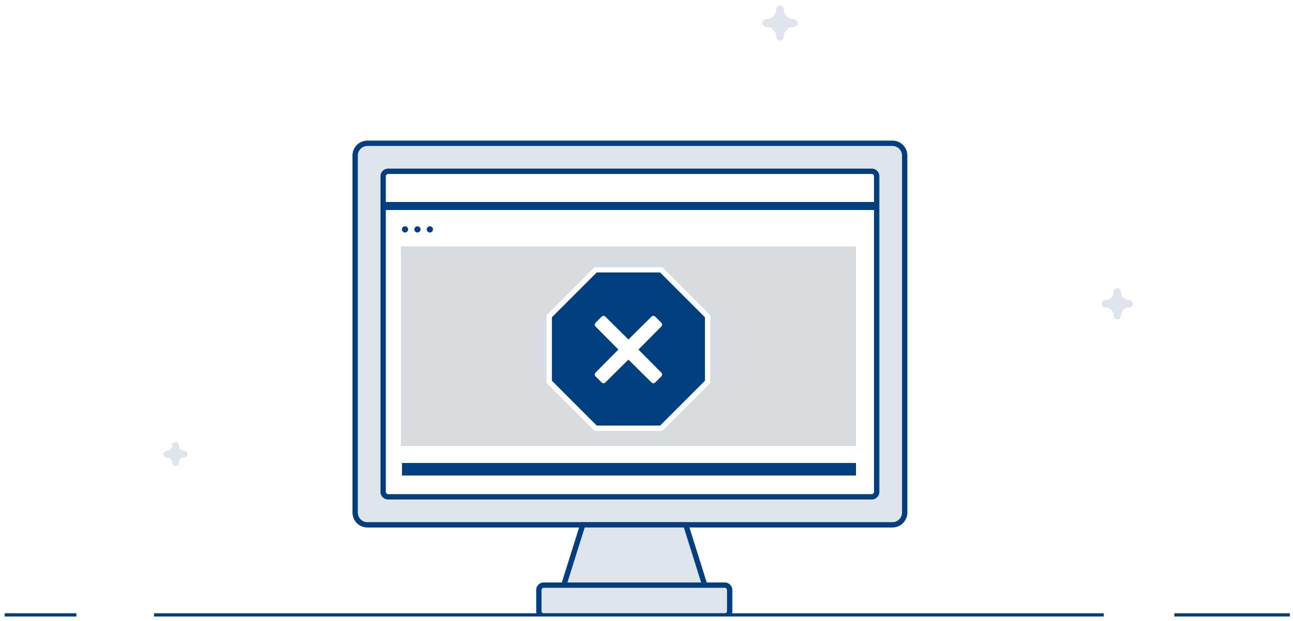
  ○ Data completeness

○ Do your test plans refer to your process requirements?

○ Do stakeholders review and sign off on your test plans? Are they involved in testing?

○ Is there documentation of the results of automated scripting or integration testing? Are those results approved before changes move into production?

○ Are error logs accessible and easy to audit?



BAI08:

Managed Knowledge

This principle concerns the maintenance of available, relevant, current, and validated knowledge of the information systems to support all the activities within the organization, including decision-making, governance, IT management, and the identification, collection, retention, use, and retirement of knowledge.

YOUR AUDITOR WILL EXAMINE THE DIVERSE SOURCES OF INFORMATION WITHIN YOUR ORGANIZATION, INCLUDING:

- Incident reports
- Strategy documents
- Configuration information
- Policies
- Procedures
- Artifacts
- Constructed and unconstructed information

This section covers many types of content, including rules, recordings, videos, digital and voice files, social media data, email, and voicemail.

○ How does that information flow through the organization?

○ Who uses the information? Who owns it?

○ How accurate is the data? How available is it?

○ Has your data been classified and tagged?

○ Do you have the tools to evaluate the impact of governance processes on the content? How often are those processes evaluated or reviewed?

○ How do you ensure that your organization's information is accurate and has few or no gaps?

○ Do you identify and monitor controls on the data to ensure that it hasn't reached its end-of-life or retirement period? Is there a retirement and archive policy for knowledge information?

○ Have you verified that your data is being used for the correct processes and purposes?

BAI09:

Managed Assets

This principle concerns the proper management of all your organization's IT assets, including systems, hardware, software, data, financial records, and configuration management processes.

BE PREPARED TO PROVIDE

○ Critical asset inventory list

○ Requirements documents

○ Service definitions

○ Service level agreements

○ Configuration management systems

○ Monitoring reports

○ Log files

○ Production schedules

○ Preventative maintenance plans

○ Hardware diagrams for all systems

○ Documented relationships with vendors (e.g., cloud providers)

○ Incident trends associated with any assets

YOUR AUDITOR MIGHT ASK:

○ Does your organization maintain an inventory of all its critical assets?

○ Have you documented the average downtime for critical assets?

○ Have you documented all system and network incidents involving your critical assets? How about their failure rate?

○ Have you documented the risks associated with the replacement, loss, or elimination of these assets?

○ If any of your critical assets were to fail or suffer unexpected downtime, how would it affect business processes?

○ How are new assets sourced, scoped, tested, and documented? Are physical assets properly labeled? What is the process for curing them?

○ What is your process for decommissioning and disposing of critical assets? Do you delete all asset-related data before retiring it, or if the asset is damaged?

○ Do you document and maintain your software and associated licenses for annual review?

BAI10:

Managed Configuration

This principle concerns the relationship between your configuration management resources and capabilities, including the collection of configuration information, establishment of configuration baselines, and ability to verify and audit your configuration information and repository.

○ Do you maintain a configuration repository?

○ Is there an approved baseline or rules regarding the configuration of your organization’s applications or IT infrastructure?

○ Does your configuration repository keep track of changes, including who made changes and when?

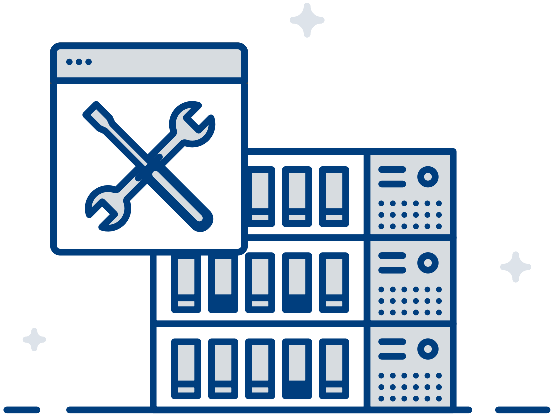
○ Who reviews the repository and logs? These should form a complete audit trail.

○ What is the approval process for configuration changes?

○ Can changes be reverted or amended? How?

○ How are configuration or system modifications reported? How often are they reviewed?

○ Does someone periodically verify physical configuration changes in your repository? Who does this, and how often?



BAI11:

Managed Projects

This section concerns project management, with projects defined as the discrete steps needed to fulfill a program. For each project:

- ○ Is there a project plan? It should include
  - ○ Approach
  - ○ Strategy
  - ○ Methodology, including
    - ○ Initiation
    - ○ Control
    - ○ Planning
    - ○ Execution
    - ○ Integration
    - ○ Implementation
    - ○ Lifecycle
    - ○ Processes
    - ○ Policies and procedures
    - ○ Scope
    - ○ Resources
    - ○ Closure
- ○ Are requirements for the project well defined?
- ○ Has due diligence been applied when choosing tech solutions, infrastructure, hardware, and software for the project?
- ○ Are costs clearly stated?
- ○ What is the standard for releasing project phases and for moving from one milestone or phase to the next?
- ○ Do stakeholders and sponsors review requirements, approve changes, define acceptance criteria, and give permission to move into each subsequent phase, including final implementation?

○ Be prepared to provide the following:

- ○ Project communication plan
- ○ Project charter
- ○ Project definition document
- ○ Requirements document
- ○ Change management document

○ Have the following been identified and documented for each project?

- ○ Interdependencies
- ○ Integration
- ○ Collaboration with other systems and vendors
- ○ Milestones
- ○ Roles and responsibilities
- ○ Key metrics and success factors
- ○ Testing and quality assurance
- ○ Owner of the system and data

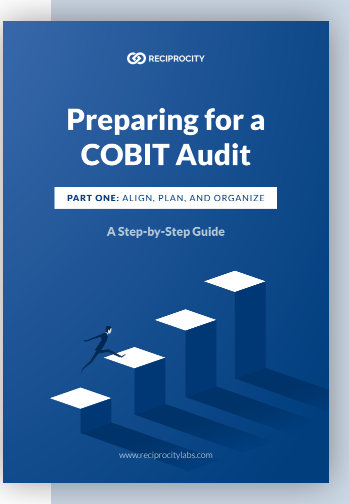
An Exhaustive, Complex Framework

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. Our complete series includes

13 "ALIGN, PLAN, AND ORGANIZE" PRINCIPLES


RECIPROCITY

Preparing for a COBIT Audit

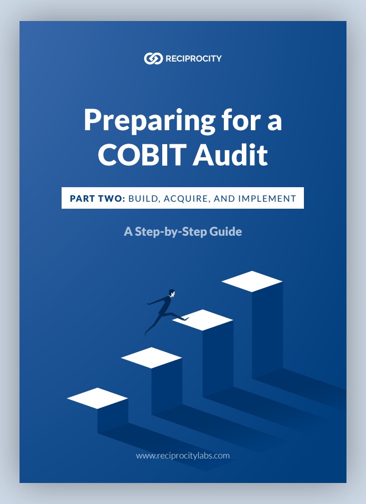
PART ONE: ALIGN, PLAN, AND ORGANIZE

A Step-by-Step Guide

www.reciprocitylabs.com

GET PART 1

10 "BUILD, ACQUIRE, AND IMPLEMENT" PRINCIPLES


RECIPROCITY

Preparing for a COBIT Audit

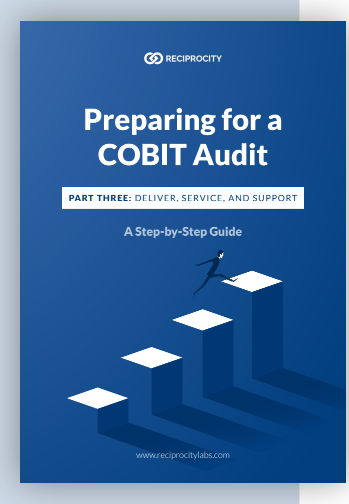
PART TWO: BUILD, ACQUIRE, AND IMPLEMENT

A Step-by-Step Guide

www.reciprocitylabs.com

PART 2

6 "DELIVER, SERVICE, AND SUPPORT" PRINCIPLES


RECIPROCITY

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.

A caveat: 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 Reciprocity

Founded in 2009, Reciprocity 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. Reciprocity has U.S. headquarters in San Francisco and global offices in Ljubljana, Slovenia; and Argentina.

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

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