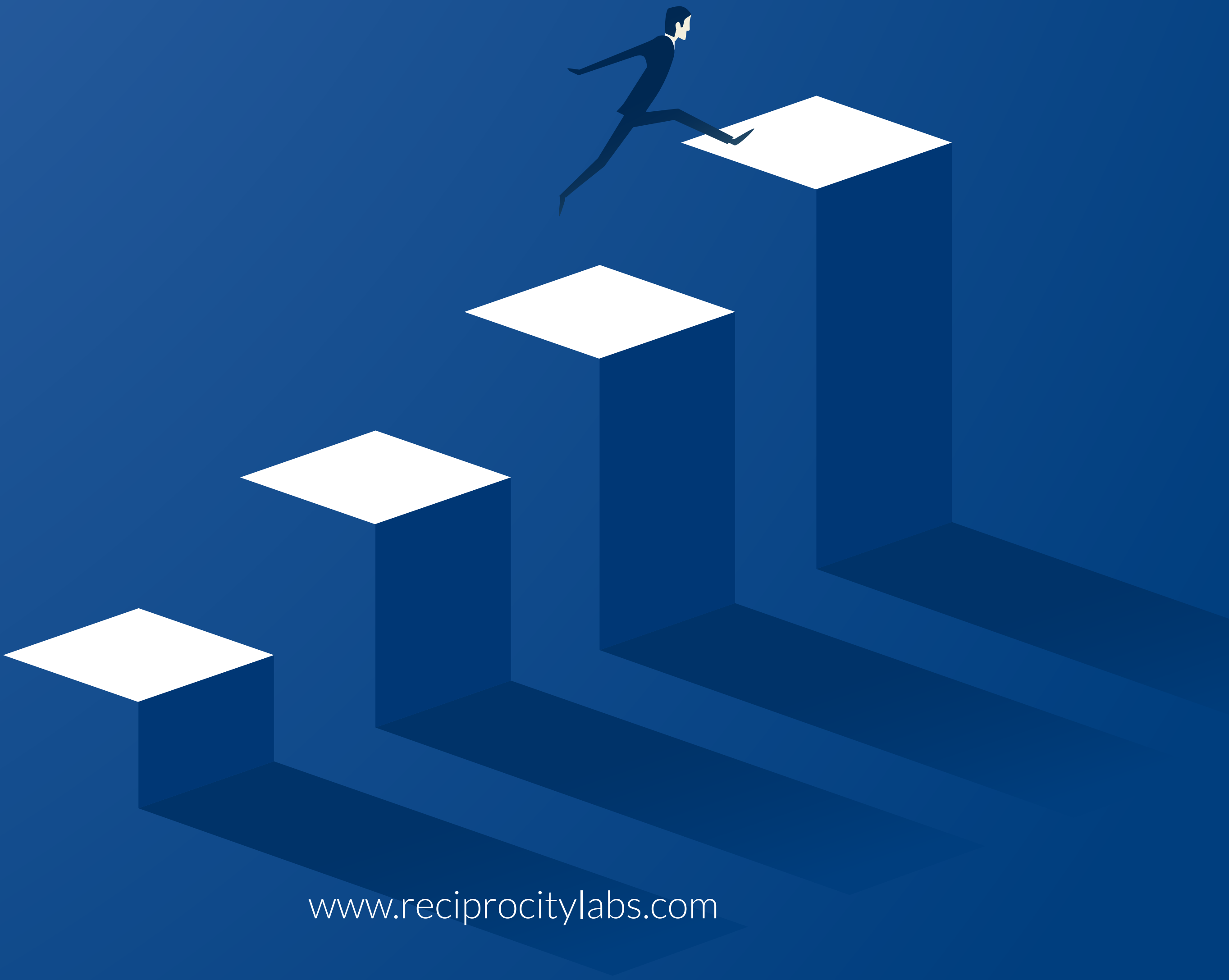
RECIPROCITY

Preparing for a COBIT Audit

PART THREE: DELIVER, SERVICE, AND SUPPORT

A Step-by-Step Guide



www.reciprocitylabs.com

How does your organization support its digital operations enterprise-wide?

Securing systems and keeping them secure is one of the greatest challenges facing businesses today—and, with privacy on the minds of everyone in the regulatory community, it is increasingly risky to neglect due diligence.

From managing your information system operations, to solving technology and security problems, to monitoring and validating transactions, COBIT's "Deliver, Service, and Support" set of principles puts the finishing touches on this comprehensive governance framework.

Deliver, Service, and Support

DSS01:

Managed Operations

This principle concerns the activities associated with all your organization's operational policies, procedures, and standards—for both internal and outsourced IT services.

○ What are those activities?

○ When do the activities take place? Are they scheduled?

○ Have there been any operation outages or incidents? How did you or your vendor resolve them?

○ How effective are your service level agreements (SLAs), especially with third-party hosting companies and service providers? Do those third parties meet the requirements of their SLAs?

○ How do you manage operations related to the following?

○ Critical applications and IT processes

○ Change management

○ Service requests

○ Incident management requests

○ Problem management

○ Business continuity

○ Does your organization monitor and report operational performance?

○ Are there independent audits of your operational environments, including

○ Event logs

○ Applications reporting

○ Network and system monitoring

○ Does your enterprise maintain an inventory of infrastructure assets to ensure that all are monitored? Does that inventory identify the critical assets and their relationships with integrated systems or third parties?

○ Have you established your system and availability thresholds for breaches or events?

○ What is your response plan for incidents, events, breaches, and outages? Has it been audited for effectiveness?

○ How do you protect the physical security of your mobile systems, mobile devices, and offsite equipment? Do you have a data center or some other kind of backup or redundancy?

○ How safe are your organization's buildings?

○ Are server rooms safe and secure?

○ Do your buildings have safety zones?

○ Do you monitor your principal power supplies for power outages and interruptions? Do you have backup generators?

○ Do you have a business continuity and disaster recovery plan? Does it include processes to address the following?

○ Power losses involving the supply of gas and electricity

○ Internet interruptions

○ Protection, repair, and replacement of cables, including those underground

○ Is there periodic review of conduit structures and building blueprints?

DSS02:

Managed Service Requests and Incidents

This principle concerns your organization’s approach to user requests, ability to escalate problems for fast and effective resolution, and process for resolving incidents, outages, and service changes.

○ Is your enterprise certified by the Information Technology Infrastructure Library (ITIL), or does it use the ITIL model?

○ How many service incidents have you experienced?

○ Did you resolve those incidents with permanent solutions or workarounds? What were they?

○ How long did it take you to resolve those incidents?

○ Have you documented all incidents and your responses and recovery actions? For each incident, documentation should include

○ Root-cause analysis

○ The incident report

○ Fulfillment requests

○ Configuration changes

○ Organizational changes

○ Incident escalation processes

○ Error handling procedures

○ Has stakeholder data been compromised in any incident?

○ Have any incidents recurred? How frequently, and how critical were they?

○ Have you analyzed service requests according to their category and looked for trends or patterns, SLAs, breaches, and inefficiencies?

○ Have you scheduled all repairs for remediation, completion, and implementation? Do you have a remediation plan? Has your change review board or project management office seen it?

DSS03:

Managed Problems

This principle concerns your organization's response to incidents and business disruptions.

YOUR AUDITOR WILL CONSIDER

○ The confidentiality of the losses, be it data, finances, business disruptions, reputational damage, data integrity, or something else.

○ Objectives of your

- ○ Organizational policy
- ○ Security policy
- ○ IT policy
- ○ Information security management system (ISMS) policy

○ How does your organization handle critical business disruptions? Do you conduct an impact analysis? Who performs it, and how often? Do analyses focus on strategy, technology security, and data privacy?

○ What are the plans and protocols for communicating with customers, partners, business relations, third-party vendors, and suppliers about problems within and external to the organization?

○ What are your recovery procedures and remediation or mitigation processes or plans? How do you reconcile information that might be lost as a result of a problem? How do you ensure that your Business Continuity and Disaster Recovery BC/DR plan is followed?

○ How do your response teams support employees, customers, vendors, and others affected by the problem? Your auditor may want to see any complaints and comments.

○ Do you require backups of all your systems and data, and are those backups tested and validated? How long would it take to recover and restore any lost data? What are your data recovery plans, and have they been approved? Who decides whether to restore data, what to restore, and whether to make changes, and when do they decide?

○ What is your escalation plan for a major outage? Does it delineate roles, responsibilities, and scheduling?

- ○ How often do you test your BR/DC plan? Yearly is considered the minimum, but your auditor most likely will want testing and review whenever new systems come online or major changes occur in your organization’s infrastructure or applications.
- ○ How do you train personnel to respond to problems, disasters, major incidents, or breaches? Who receives this training, and how often?
- ○ What is your backup process? What media do you use for backups? Are backups automatic? Is it possible to back up or restore your systems manually? How often do you audit backups?

DSS04:

Managed Continuity

This principle concerns your business continuity plan (BCP) and related items. Its aim is to ensure that your organization can respond effectively and recover quickly from a disruption or incident.

- ○ Have you conducted a risk assessment? A business impact analysis? Do you review these documents periodically to verify that they adequately address the risks to your organization?
- ○ Have you identified potential threats or disruptors, and planned a response to each?
- ○ Do your documents state a recovery time objective, i.e., the time required to resume business operations after an incident or event?
- ○ What are your business continuity requirements? Does your BCP list your business and technical options as well as the components that are essential for continuity?
- ○ What role should your suppliers play in ensuring the effectiveness of your BCP? Have you sent assessments to each and audited their responses?
- ○ What are your business recovery processes and procedures?
- ○ What happens if a vendor has an outage or disruption—would you be affected? Contracts should include provisions to protect your organization.
- ○ Do you have supporting documentation that identifies the decision-making person or teams? Examples include your executive team, test team, technology professionals, and administrative teams. Have you allocated responsibility for responding to specific kinds of situations, and have you named the key resources that support your critical systems?

DSS05:

Managed Security Systems

This principle concerns security from the standpoint of risk, in accordance with your security policy.

AUDITORS WILL EXAMINE YOUR SECURITY

- Roles and responsibilities
- Access monitoring
- Incident management
- Risk assessment
- Infrastructure, hardware, and software
- Privacy protection

QUESTIONS INCLUDE:

○ Are your servers up to date? Have they been patched?

○ Have you protected your systems against malware, spyware, and ransomware? What tools do you use for this? How effective are they?

○ How many security incidents or events has your organization experienced? Have you documented the incidents and your response to each?

○ Do you patch your systems and perform configuration and change management using a central process?

○ Does your organization provide security training? How often? Who receives it?

○ Are your networks and applications monitored?

○ Are your networks protected by filtering mechanisms, such as firewalls and intrusion detection systems?

- ○ What is the process for setting up network hardware? How do you harden your systems, servers, and infrastructure before connecting to your network? Do you conduct penetration testing on new applications and systems?
- ○ How often do you test your security software? Have you installed it on your endpoints as well as your server?
- ○ Do you keep a log of incidents involving your endpoint devices and unauthorized devices?
- ○ What is the configuration of your operating systems? Have you consulted with a security professional to ensure that the configuration is secure?
- ○ How are remote access requests vetted and authenticated?
- ○ Do you monitor network traffic for anomalies and suspicious patterns?
- ○ How do you physically secure your endpoint devices?
- ○ What are the policies and procedures for hardware disposal?
- ○ How do you manage access to your buildings and grounds? Do you require badges? Are visitors escorted?
- ○ How do you protect sensitive data, such as personally identifiable information (PII)? Do you encrypt it? How?
- ○ Has your organization undergone a third-party security assessment?

DSS06:

Managed Business and Process Controls

This principle concerns the controls on your organization's in-house and outsourced business processes. Your auditor will want to see that the controls function properly, that all processes are approved, that the controls minimize disruptions to the business and customers, and that the key owners are involved in processing activities.

○ Do you have records of your organization's transactions? Are they valid, verified, and complete?

○ How do you ensure the integrity and validity of transacted data?

○ Has your organization defined the roles, responsibilities, and segregation of duties associated with business process controls?

○ Do you conduct training to ensure that security, integrity, confidentiality, and privacy are maintained for business process controls?

○ Do you keep reports of control definitions and exceptions?

○ How do you control and authenticate privileges and access to sensitive data? Do you restrict access to those who need it to do their job?

○ Do terminated employees lose their access rights immediately upon termination?

○ Does your enterprise review access rights periodically? Your auditor may prefer to see monthly reviews.

So Much Work, So Little Time

Now that you've combed through the lengthy, complex COBIT framework, you know. Passing the audit is a massive undertaking.

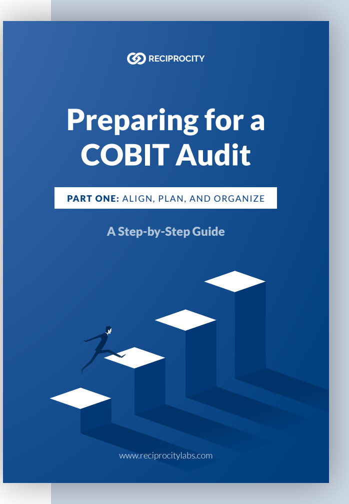
The rewards for compliance are vast, not just for your organization's reputation but also for your ability to derive maximum value from your technologies in the connected age—when all organizations will, by necessity, be not just digital, but digital-first.

It's not an easy task. In this ebook, we've covered just one of several essential sections of the COBIT framework that are crucial for passing an audit. We covered two more sections in the first two publications. Our complete series includes

13 "ALIGN, PLAN, AND ORGANIZE" PRINCIPLES

10 "BUILD, ACQUIRE, AND IMPLEMENT" PRINCIPLES

6 "DELIVER, SERVICE, AND SUPPORT" PRINCIPLES



RECIPROCITY

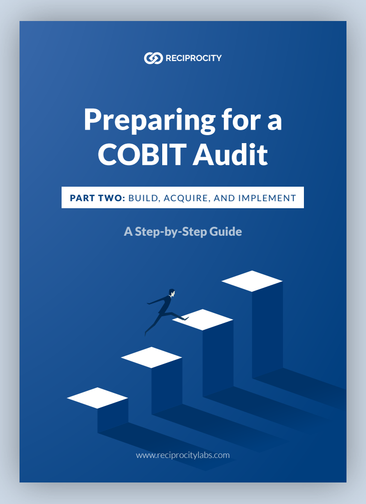
Preparing for a COBIT Audit

PART ONE: ALIGN, PLAN, AND ORGANIZE

A Step-by-Step Guide

www.reciprocitylabs.com

GET PART 1



RECIPROCITY

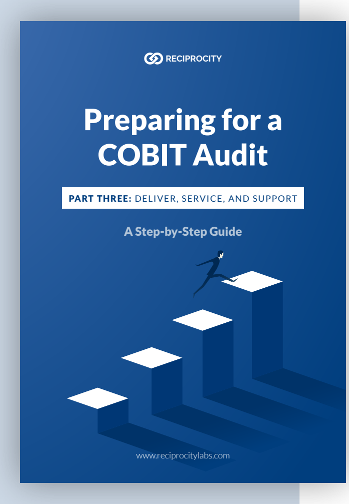
Preparing for a COBIT Audit

PART TWO: BUILD, ACQUIRE, AND IMPLEMENT

A Step-by-Step Guide

www.reciprocitylabs.com

GET PART 2



RECIPROCITY

Preparing for a COBIT Audit

PART THREE: DELIVER, SERVICE, AND SUPPORT

A Step-by-Step Guide

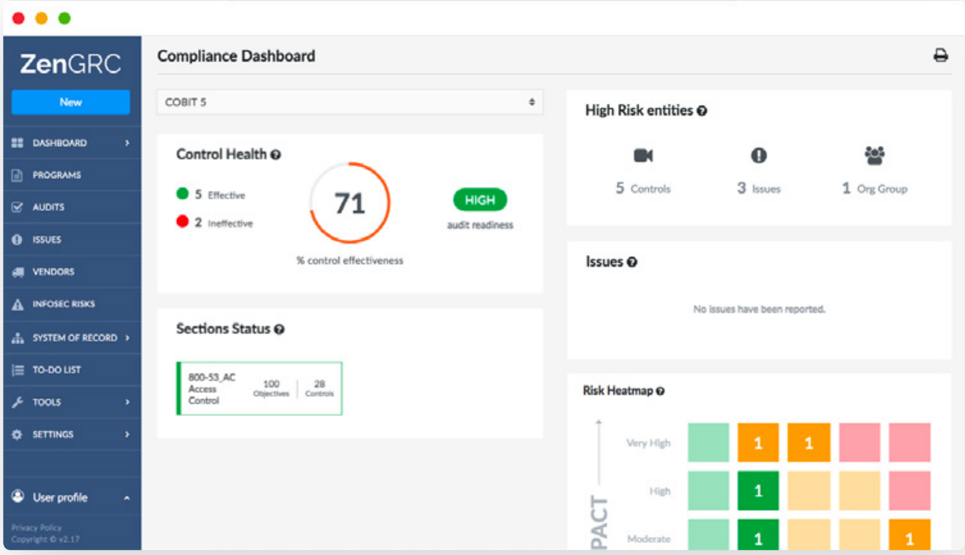
www.reciprocitylabs.com

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.

Staying on top of COBIT does require flexibility, though. These guides address COBIT 5, but the framework 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 will track your COBIT compliance for you, but can contrast and compare with other frameworks and display the results on user-friendly dashboards. 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