

COBIT

an abridged guide to
control practices
& assessment

::: If **you** are in the business world,
no doubt you have heard of **COBIT**:
Control Objectives for Information
and related Technology

2

3

6

:: table of contents

:: *introduction*

:: control practices

:: **self-assessment**

:: refresher :: COBIT is one of several popular standards for dealing with information security and data. Others include ITIL, SAS 70, & ISO 17799

:: you may have had to alter your control practices to be compliant with COBIT or hired someone to review your policies because you know why it's a big deal:

COBIT, first published in 1996, gained momentum due to events such as the Enron and Tyco International scandals and the passage of the Sarbanes-Oxley Act. Updated editions were released in 1998, 2000, and 2005.

The COBIT mission is "to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day by business managers and auditors."

::: **COBIT** has 34 high-level objectives that cover 318 control objectives, categorized under four headings:

plan & organize.

acquire & implement.

deliver & support.

monitor & evaluate.

plan & organize.

:: Planning and organizing processes help companies realize their goals and objectives by recognizing how technology will best help them succeed. It highlights an IT plan, the definition of your information architecture, the direction you would like your technology to take you - the organization - and the investment you will have to make in your IT environment.

acquire & implement.

:: After understanding your company's requirements, the next step is acquiring the technology, and implementing it into your company's business processes. This heading also refers to the maintenance plan you will need to put into place to keep your IT system, and its components, running and healthy.

delivery & support.

:: The delivery and support category covers areas such as the execution of the applications within your IT system, and the support processes involved in this. It also includes the security issues and training involved in keeping your environment live and running. Support staff dealing with the following issues will be controlled by the delivery and support section: performance and capacity, systems security, educate and train users, service desk and incidents, manage data, manage the physical environment, and manage operations.

monitor & evaluate.

:: Monitoring and evaluation are necessary to assess whether your current policies are still meeting the objectives originally set forth, and they still comply with regulatory requirements. In some cases, you may want to bring in an independent assessment to test the effectiveness of your IT system, and its ability to meet business objectives.

am i compliant?

:: while COBIT does not have a certification process in place, they have suggested a specific maturity model for self-assessment, or for an independent audit.

:: each of the 34 control objectives should be evaluated, and rated based on the following scale:

0

non-existent :: management processes are not applied at all

1

initial :: processes are ad hoc and disorganized

2

repeatable :: processes follow a regular pattern

3

defined :: processes are documented and communicated

4

managed :: processes are monitored and measured

5

optimized :: best practices are followed and automated

:: the evaluation

should be done individually for each of the 34 objectives, and should be mapped out according to the following goals:

the current status of your company ::

the current status of (best-in-class in)
the industry ::
comparison

the current status of international
standard guidelines ::
further comparison

the company's strategy for improvement ::
where do you want to be?

where do i find the self-assessment
guide?

ISACA, which is the governing company of COBIT, has the complete model available for purchase online. While you are evaluating your own processes internally, consider outsourcing your IT environment to a hosting company that is aware of your needs.



Secure-24

:: how can Secure-24 help you?

When dealing with an auditor, you will not only have to show them the practices, processes, and controls inside your offices, but also for anyone else who may help you with your information technology. We offer detailed information about Secure-24's controls, and an independent assessment of whether the controls are operating effectively. You can then present this to any auditors requiring further information.

Secure-24 recognizes the needs of its customers in many different industries. That is why we are compliant with many different standards, such as COBIT, ITIL, SAS 70, ISO 17799, and Sarbanes-Oxley. We are independently audited on a bi-yearly basis, to ensure that our processes are up to date, and accurate.

Call us now for a commitment-free review of your environment, and its requirements. Instead of spending money to review, and alter, all of your processes, we may be able to offer you a more economical solution.

for more information :: 248.784.1021