# Comparison between COBIT, ITIL and ISO 27001





Many friend of mine keep asking me about what is should be implemented first to improve their information system management: whether taking Cobit, ITIL, or ISO27001. And the next question usually which one is the easiest to be implemented in their company.

To be able to answer this question, let me tell you the definition of this three major standard in information system, who has a little bit difference in basic concept.

## COBIT

Cobit (http://www.securityprocedure.com/control-objectives-information-and-related-technology-cobit) is stand for Control Objective over Information and Related Technology. Cobit issued by ISACA (Information System Control Standard) a non profit organization for IT Governance. The Cobit main function is to help the company, mapping their IT process to ISACA best practices standard. Cobit usually choosen by the company who performing information system audit, whether related to financial audit or general IT audit.

## ITIL

ITIL (http://www.securityprocedure.com/information-technology-infrastructure-library) is stand for Information Technology Library. ITIL issued by OGC, is a set of framework for managing IT Service Level. Although ITIL is quite similar with COBIT in many ways, but the basic difference is Cobit set the standard by seeing the process based and risk, and in the other hand ITIL set the standard from basic IT service.

**ISO27001**

ISO27001 () is much more different between COBIT and ITIL, because ISO27001 is a security standard, so it has smaller but deeper domain compare to COBIT and ITIL.

Here is the detail table of comparison between this three standard

| AREA | COBIT | ITIL | ISO27001 |
|---|---|---|---|
| Function | Mapping IT Process | Mapping IT Service Level Management | Information Security Framework |
| Area | 4 Process and 34 Domain | 9 Process | 10 Domain |
| Issuer | ISACA | OGC | ISO Board |
| Implementation | Information System Audit | Manage Service Level | Compliance to security standard |
| Consultant | Accounting Firm, IT Consulting Firm | IT Consulting firm | IT Consulting firm, Security Firm, Network Consultant |

**What should be implemented first?**

There's no exact answer about this question, but i think its really depend on your company and your requirement. Most of company start to implemented Cobit first because its cover general information system. And after that they usually choose between ITIL or ISO27001.

Another consideration is about budget and authoritive. Cobit implementation usually run from internal audit budget and ITIL or ISO27001 usually performed using IT departement budget. This consideration usually makes what kind of standard to implemented first become depend on management policy.

**What is the easiest standard?**

From the implementatation view, ITIL is the easiest standard to be implemented. Because, ITIL could be implemented partially and still not have impact on performance. Example, if IT departement lack of budget and he could choose to implement IT Service Delivery layer only, and the next year he will try to implement IT Release Management or IT Problem Management.<

However COBIT and ISO27001 is quite difficult to be implemented partially, since it should see a process in bigger view first before they could implemented partially.

**How to choose the right vendor?**

Many vendor said that he could help your company to implement these standard effectively, in fact there is no one solution for all. Usually the COBIT vendor come from Publci Accounting Firm who has an IT Audit arm, eg PWC, DTT, KPMG, EY. This type of vendor is best choice for COBIT since they also work for COBIT implementation derivative such as COBIT for Sarbanes Oxley.

The other standard ITIL and ISO27001 usually come from General IT Consulting Company, eg. IBM, Accenture. And for ISO27001 most of IT networking company also could offer this standard consultation.

Do you have any other opinion with this comparison?

Others referrence:
ISACA: Aligning COBIT, ITIL and ISO 17799 for Business Benefit (http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=22493&TEMPLATE=/ContentManagement/ContentDisplay.cfm)

**Anjar Priandoyo, CISA** (http://priandoyo.com)

*Senior Information System Auditor at Big 4 Accounting Firm with more than five years implementing COBIT, ITIL and ISO27001



Bookmark/Search this post with:

## Trackback URL for this post:

http://www.securityprocedure.com/trackback/22