

Combining ITIL with COBIT and 17799

By John Wallhoff (CISA, CISM, CISSP)

What ITIL is for IT Management, COBIT is for IT-audit and ISO 17799 is for security management. As different frameworks and standards emerge they cause a great deal of confusion, especially on when you use or not use either one of them. When you take a closer look it is obvious that they successfully can be combined. In this article we have chosen to describe core issues in Service Delivery and Service Support in the ITIL framework against COBIT and ISO 17799.

Three different ways to approach IT

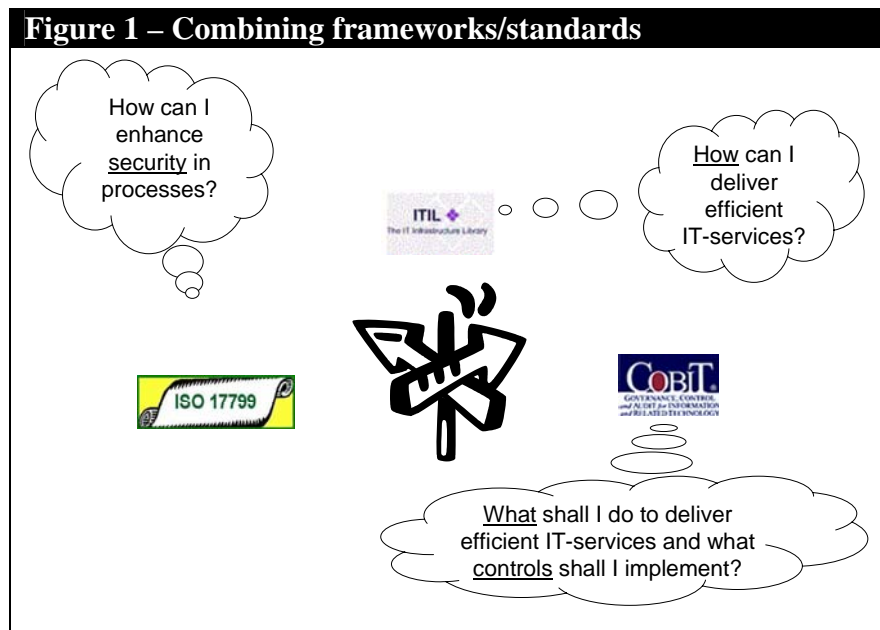
ITIL, COBIT and ISO 17799 has been available for several years now and gained recognition within different communities. Even in some countries they have been implemented in the legislation, as a reference and/or baseline.

ITIL (IT Infrastructure Library) was published by the British Office of Government Commerce (OCG). The goal was to develop a vendor-independent approach for service management. The ethos behind the development was the recognition of increased independence on IT, which has to be managed by high quality IT services. ITIL provides IT processes, but is not strong in security. It is often used as the delivery mechanism, where it describes how.

COBIT (Control Objectives for Information and related Technology) is issued by the IT Governance Institute. The mission for COBIT 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 use by business managers, IT professionals and assurance profession. COBIT provides IT controls and IT metrics, but is not strong in security. It is often used as the delivery mechanism, where it describes what.

Finally ISO/IEC 17799:2000 (The Code of Practice for Information Security Management) is an ISO standard, based on the British standard BS 7799-1. The goal of ISO/IEC 17799:2000 has been to provide information to parties responsible for implementing information security within an organization. It can be seen as a basis for developing security standards and management practices within an organization to improve reliability on information security in inter-organizational relationships. ISO/IEC 17799:2000 provides security controls, but does not define how to implement and manage them. It is to be used for improvements of security processes and controls.

When you look at these standards and framework at this level it is obvious that they serve different needs within an organization. In some essence you can use one of them and gain something another also covers. It could be the implementation of a formal change management process, with clearly defined responsibilities and procedures. That would enable controls when you need to change the IT environment and also the possibility to address security issues that are related to the change.



Combining frameworks and standard

Now if you want to go one step further and really want to get what is best within ITIL, COBIT and ISO 17799, you have to look at the different issues they cover. When we made this benchmark, we decided to start with the core publications of ITIL: Service Support and Service Delivery. In this benchmark we also used two levels for how well they correspond with each other:

- Primary: Sub-processes or sections correspond to a high extent.
- Secondary: Sub-processes or sections correspond to some extent.

ITIL related to COBIT

The strength within ITIL is the way processes are described with different activities and flowcharts to use for your own implementation. Cost/Benefit and implementation issues are also described. There are also guidelines for reviews and Critical Success Factors, but those issues are better described in COBIT. First of all COBIT was defined by IT-audit community with a strong skill within audit, where its “Audit Guidelines” is thorough set of advice for an audit or review. COBIT is also stronger when it comes down to management issues where “Management Guidelines” provides you with a reference where Critical Success Factors are described together with Key Goal Indicators, Key Performance Indicators and Capability Maturity Models (CMM).

When we benchmarked ITIL with COBIT we identified that they correspond with each other to a high degree. It is though obvious that different words are used for the same issue and they cover the same problem. It is only for Incident Management that we haven’t been able to identify any relation in COBIT. This doesn’t mean that it is not covered at all, instead it may be covered within other parts of the framework or with a different approach.

Figure 2 – ITIL Service Support versus COBIT

ITIL	COBIT Primary	COBIT Secondary
Service Desk	DS8 Assist and Advise Customers	AI4 Develop and Maintain Procedures DS7 Educate and Train Users
Incident Management	DS10 Manage Problems and Incidents	
Problem Management	DS10 Manage Problems and Incidents	DS8 Assist and Advise Customers
Configuration Management	DS9 Manage the Configuration	AI6 Manage Changes DS10 Manage Problems and Incidents
Change Management	AI6 Manage Changes	AI3 Acquire and Maintain Technology Infrastructure DS9 Manage the Configuration
Release Management		AI6 Manage Changes DS9 Manage the Configuration

Service Delivery follows the same results as for Service Support. It is very interesting to find that Service Level Agreement that is a key issue in ITIL is also an important issue in COBIT.

Figure 3 – ITIL Service Delivery versus COBIT		
ITIL	COBIT Primary	COBIT Secondary
Service Level Agreement	DS1 Define and Manage Service Levels	AI4 Develop and Maintain Procedures DS2 Manage Third-party Services DS4 Ensure Continuous Service DS6 Identify and Allocate Costs M3 Obtain Independent Assurance
Financial Management for IT Services	DS6 Identify and Allocate Costs	M2 Monitor the Processes
Capacity Management	DS3 Manage Performance and Capacity	
IT Service Continuity Management	DS4 Ensure Continuous Service	AI6 Manage Changes
Availability Management	DS3 Manage Performance and Capacity	AI2 Acquire and Maintain Application Software

ITIL related to ISO 17799

As already mentioned, ISO 17799 is used for information security and not just IT issues. With such broad objective we soon identified that it does not correspond with ITIL as much as COBIT did. ISO 17799 is on the other hand complimentary to a high degree when you need to specify or analyse issues that will have an impact on the overall security level within the organisation.

When we assessed ITIL Service Support we identified that Problem Management and Configuration was not possible to find as corresponding issues in ISO 17799. Especially Configuration Management surprised us because it will have a huge impact on the IT environment if it is not handled in a secure manner. You can though argue that configuration is a change management issue.

Figure 4 – ITIL Service Support versus ISO 17799		
ITIL	ISO/IEC 17799:2000 Primary	ISO/IEC 17799:2000 Secondary
Service Desk		6.3.2 Reporting security weaknesses
Incident Management	8.1.3 Incident management procedures	6.3 Responding to security incidents and malfunctions
Problem Management		
Configuration Management		
Change Management	10.5.1 Change control procedures	4.2.2 Security requirements in third party contracts 8.1.2 Operational change control 8.3.1 Controls against malicious software
Release Management		10.4.1 Control of operational software 10.5.2 Technical review of operating system changes

For ITIL Service Delivery we face another problem with the terminology. In ISO 17799 security is characterized as the preservation of Confidentiality, Integrity and Availability. In ITIL Availability is about quality aspects such as reliability, maintainability, serviceability & resilience. Another important finding in the benchmark is that financial issues are not handled at all in ISO 17799, instead it is about risk management meaning you mitigate risks to avoid costs. For ITIL it is instead about financing and cost allocation for the delivery of IT-services.

Figure 5 – ITIL Service Delivery versus ISO 17799		
ITIL	ISO/IEC 17799:2000 Primary	ISO/IEC 17799:2000 Secondary
Service Level Agreement		4.2.2 Security requirements in third party contracts
Financial Management for IT Services		
Capacity Management	8.2.1 Capacity planning	8.2.2 System planning and acceptance
IT Service Continuity Management	11 Business continuity management	
Availability Management		4.3.1 Security requirements in outsourcing contracts 8.2 System planning and acceptance 8.5.1 Network controls 8.7.4 Security of electronic mail 9.5.5 Use of system utilities 12.1.7.3 Quality and completeness of evidence

Conclusion

In every organization today we must deliver IT services in a cost efficient manner, mitigating security risks and comply with legal requirements. The equation is difficult to handle and in some cases it seems like an impossible mission. To be able to survive in this environment a combination of ITIL, COBIT and ISO 17799 can be valuable for you. You may use ITIL to define processes, use COBIT for metrics, benchmarks and audits and use ISO 17799 to address security issues to mitigate risks.

Figure 6 – Key issues to be combined		
ITIL	COBIT	ISO/IEC 17799:2000
Concept/Process	Critical Success Factors	Information Security
Activities	Metrics (CSF, KPI)	
Cost/Benefit	Benchmarking (CMM)	
Planning for implementation	Controls	
	Audit	

Another recommendation that is repeated in any article, book or presentation we have come across on this issue is that you shall not go for complete implementation of ITIL, COBIT and ISO 17799 at the same time. A big bang implementation is bound to fail. The difficult task is instead to choose issues that are important for you, from a cost/benefit, risk mitigation or regulatory compliance perspective.

John Wallhoff, CISA, CISM, CISSP

is the founder and Managing Director of Scillani Information AB. Prior to this position, he worked both as an IT-auditor, IS-consultant and with Security management practices within enterprises like Ernst & Young and AddTrust. He has over thirteen years experience in the IT field as an IT/IS consultant and in IS audit.

References

ITIL Service Delivery, OCG

ITIL Service Support, OCG

COBIT 3rd Edition Management Guidelines, ITGovernance Institute

COBIT 3rd Edition Control Objectives, ITGovernance Institute

COBIT 3rd Edition Audit Guidelines, ITGovernance Institute

Information security management – Part 1 Code of practice for information security management

ITIL Security Management, OCG

COBIT Security Baseline, ITGovernance Institute

COBIT mapping - Overview of International IT Guidance, ITGovernance Institute

BS7799 Information security management – Part 2 Specification for information security management systems

Whitepaper Combining ITIL with Cobit och 17799, By John Wallhoff, Scillani Information AB (2004), www.scillani.com