

Risk-based Sampling Using COBIT



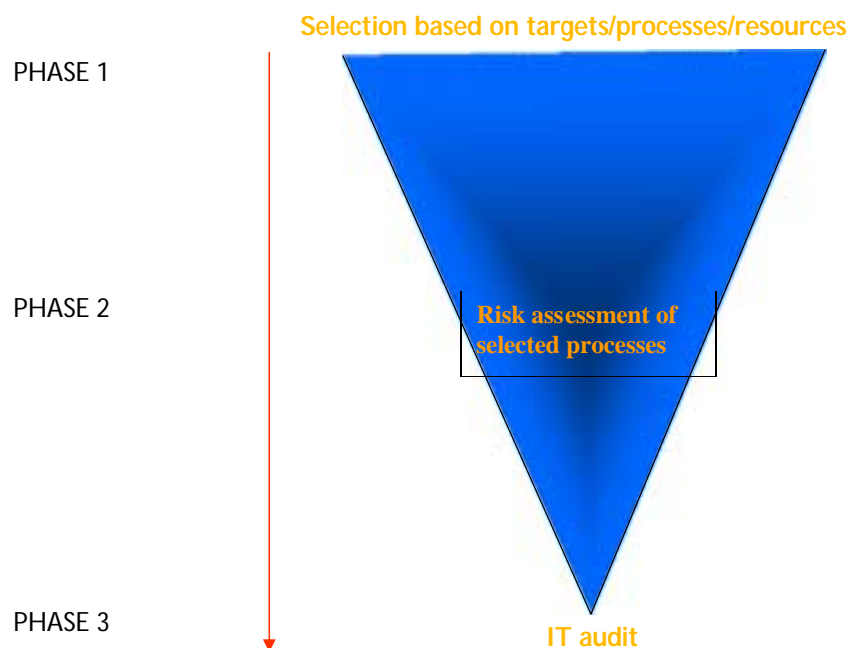
By Rune Johannessen CISA, CIA, Dip. Internal Audit

Riksrevisjonen

In this article, I would like to share some useful experiences that I have gained in my work with the COBIT (Control Objectives for Information and related Technology) tool kit. The following is not intended to be a template for the execution of risk-based audits, but rather a tentative suggestion towards a possible audit method.

Many public and private organisations now use COBIT, and I am fairly confident that anyone who has experience of the tool would confirm that it is highly comprehensive and its use quite time consuming. This is often in stark contrast to our everyday situation, where time is a critical factor of which we often have too little to carry out the tasks that have been assigned to us. It is therefore important that within our given time frames we select the areas and processes that are most important and pose the highest risk, in order that we provide our client with maximum added value.

In my opinion, COBIT does not provide clear guidelines on how to carry out an overall (or "high level") audit risk assessment; in other words how to select the most important areas and/or processes for auditing. I have therefore chosen to illustrate my solution with a general model for carrying out the auditing cycle. My method, which is based on qualitative assessments and allows considerable flexibility in relation to the audit client, can be represented in graphical form thus:



Phase 1: Selection based on targets/processes/resources

This phase consists of deciding, at a general level, what to focus on, which may be a sample of domains, processes, IT resources and/or a sample of information criteria. On the basis of the selected priorities the auditor derives a list of processes that it might be relevant to examine in more depth. In the following example I have tried to illustrate this for the domain "**Acquisitions and implementation**", where the processes "Change management" and "Acquisition and maintenance of software" are identified as highly important to the audit client and are therefore selected as relevant to the audit.

Phase 2: Risk assessment of selected processes

As a result of the selections made in Phase 1, the auditor now has a sample of processes that have been ascribed priorities. In the example above, A12 and A16 were identified as relevant within the domain "Acquisitions and implementation". As a result of restrictions on time and resources, it is often necessary to further limit the amount of work. In Phase 2 the auditor again ascribes priorities to the processes selected in phase 1, and then selects those with the highest risk. I have tried to illustrate this in the following example, where the auditor completes the following form for each of the processes that were selected in Phase 1, in this case A16:

The table lists a number of control questions linked to each process - these have been derived from the points listed under the title "and takes into consideration" on the first page of each process¹. On the basis of a sample, the auditor formulates some general control questions intended to give a 'feel' for the routines, documentation and processes in use in this area. The information required to answer the sample questions can be gathered through interviews and by observation of the routines in use. At this stage, the auditor does not make any comprehensive assessments of the content and quality of the available material.

The column for control routines should be marked as *documented*, *undocumented* or *don't know*. The following criteria may be used to answer the questions:

| Scale | Control routines |
|--------------|--|
| Documented | The audited entity has a routine, process or documentation that deals with the matter. |
| Undocumented | The audited entity does not have routines, processes or documentation that deal with the matter. |

| Importance | | | | IT process |
|----------------|-----------|--------------------|------------|---|
| Very important | Important | Not very important | Don't know | |
| | | | | ACQUISITIONS AND IMPLEMENTATION |
| | | X | | A11 Identification of solutions |
| X | | | | A12 Acquisition and maintenance of software |
| | | X | | A13 Acquisition and maintenance of technological infrastructure |
| | | X | | A14 Development and maintenance of IT procedures / routines |
| | | X | | A15 Installation and approval of systems |
| X | | | | A16 Change management |

| IT process | Control routines | | | Risk | | | Ref. | |
|---|------------------|--------------|------------|-------------|-------------|------|------|--------|
| | Documented | Undocumented | Don't know | Probability | Consequence | High | | Medium |
| A16 Change management | | | | | | | | |
| 1. Are all requests regarding change and system maintenance documented and subject to formal and structured change procedures? | | | | | | | | |
| 2. Are all change requests categorised and prioritised according to clear criteria? | | | | | | | | |
| 3. Do the organisation's routines for change management ensure that consequences as a result of the particular change are identified and assessed before it is approved / rejected? | | | | | | | | |
| 4. Have procedures been established that ensure monitoring between the system for change management and the organisation's configuration control system? | | | | | | | | |
| Etc. | | | | | | | | |

The next step involves making an overall assessment of the probability of there being errors, weaknesses or loopholes in a process. This assessment will have as its starting point a preliminary review of the process and, as appropriate, the auditors' own opinions. The auditor should include internal and external factors that can adversely affect the process. The results are presented in a matrix with the following scale:

| Scale | Probability |
|-------|---|
| H | It is regarded as highly probable that this process will be negatively affected by internal or external events. |
| M | It is regarded as possible that this process will be negatively affected by internal or external events. |
| L | It is not regarded as very probable that this process will be negatively affected by internal or external events. |

¹ See full COBIT documentation set. This can be downloaded from... <http://www.isaca.org/>

The next step is to assess the consequences of a negative incident. In addition to any monetary losses, factors such as reputation and working environment should also be taken into consideration.

| Scale | Consequence |
|-------|---|
| H | Negative internal or external incidents are expected to have major consequences for the process. |
| M | Negative internal or external incidents are expected to have medium consequences for the process. |
| L | Negative internal or external incidents are expected to have minor consequences for the process. |

In this way, each process is subject to a risk assessment through probability and consequences being considered together. On the basis of how the process is rated in terms of risk (H high, M medium, L low), a sample is selected to be used in the following IT audit phase.

Phase 3: IT audit

An IT audit is then carried out on the processes that have been identified as having the highest risk, using the COBIT "Audit Guidelines":

| IT process and audit questions | | Results of evaluation and testing | Recommendation | Ref. |
|--------------------------------|---|---|-----------------|------|
| AI6 | Change management | | | |
| | <p>Has a method been established for prioritisation of change recommendations from users, and if so, is it being used?</p> <p>Have procedures been compiled for sudden changes, and if so, are they being used?</p> <p>Is there a formal procedure for monitoring changes, and if so, is it being used?</p> <p>Are changes logged in a way that shows whether they have been carried out in a satisfactory way?</p> <p>Etc.</p> | <p>Observation:</p> <p>Method for changes... There is no procedure for sudden changes ... Etc.</p> <p>Assessments:</p> <p>The methodology is incomplete in terms of sudden changes...</p> <p>Conclusion:</p> <p>The methodology is inadequate...</p> | We recommend... | |

I hope that these observations and suggestions will contribute to development of a practical approach to how a risk-based audit can be carried

out using COBIT. I also hope that this article will inspire others to share their experiences and describe their routines when using this tool.

About the author

Rune Johannessen is a Senior Audit Adviser at the Office of the Auditor General of Norway, where he is involved in both IT auditing and the development of methodology. Rune has 7 years experience in the field of internal auditing, financial auditing, IT auditing and quality assurance in IT projects. Before joining the Auditor General of Norway, he worked as a senior adviser for PricewaterhouseCoopers on quality assurance in system development projects and in IT security.

Rune holds a bachelor of management degree from the Norwegian School of Management and a higher degree from the University of Oslo, and is certified CISA and CIA.

COBIT

COBIT, developed by ISACA, is a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners.

COBIT comprises the following main products:

Framework: a successful organisation is built on a solid framework of data and information. The *Framework* explains how IT processes deliver the information that the business needs to achieve its objectives. This delivery is controlled through 34 high-level control objectives, one for each IT process, contained in the four domains. The *Framework* identifies which of the seven information criteria (effectiveness, efficiency, confidentiality, integrity, avail-

ability, compliance and reliability), as well as which IT resources (people, applications, technology, facilities and data) are important for the IT processes to fully support the business objective.

Management Guidelines: to ensure a successful enterprise, you must effectively manage the union between business processes and information systems. The new *Management Guidelines* is composed of Maturity Models, Critical Success Factors, Key Goal Indicators and Key Performance Indicators. These *Management Guidelines* will help answer the questions of immediate concern to all those who have a stake in enterprise success.

Detailed Control Objectives: the key to maintaining profitability in a technologically changing environment is how well you maintain control. COBIT's *Control Objectives* provides the critical insight needed to delineate a clear policy and good practice for IT controls. Included are the statements of desired results or purposes to be achieved by implementing the 318 specific, detailed control objectives throughout the 34 high-level control objectives.

Audit Guidelines: analyse, assess, interpret, react, implement. To achieve your desired goals and objectives you must constantly and consistently audit your procedures. *Audit Guidelines* outlines and suggests actual activities to be performed corresponding to each of the 34 high-level IT control objectives, while substantiating the risk of control objectives not being met.

Implementation Tool Set: an Implementation Tool Set, which contains Management Awareness and IT Control Diagnostics, Implementation Guide, frequently asked questions, case studies from organizations currently using COBIT and slide presentations that can be used to introduce COBIT into organizations. The tool set is designed to facilitate the implementation of COBIT, relate lessons learned from organizations that quickly and successfully applied COBIT in their work environments and assist management in choosing implementation options.

COBIT can be downloaded from... <http://www.isaca.org>

COBIT FAMILY OF PRODUCTS

