**COBIT**

How do we get Information Technology under control such that it delivers the information the organisation needs? How do we manage the risks and secure the infrastructure we are so dependent on? As with many issues facing management, these broad strategic questions generate the following traditional questions to which we will provide answers:

• What is the issue/problem?

• What is the solution?

• What does it consist of?

• Will it work?

• How do I do it?

An approach to addressing these issues has been provided by the COBIT Framework. COBIT stands for Control Objectives for Information and related Technology and is an open standard for control over information technology, developed and promoted by the IT Governance Institute. This framework identifies 34 information technology (IT) processes, a high-level approach to control over these processes, as well as 318 detailed control objectives and audit guidelines to assess the 34 IT processes. It provides a generally applicable and accepted standard for good IT security and control practices to support management’s needs in determining and monitoring the appropriate level of IT security and control for their organisations.

The IT Governance Institute has further built on this with leading-edge research, in cooperation with world-wide industry experts, analysts and academics. This has resulted in the definition of Management Guidelines for COBIT, which consist of Maturity Models, Critical Success Factors (CSFs), Key Goal Indicators (KGIs) and Key Performance Indicators (KPIs). This delivers a significantly improved framework responding to management’s need for control and measurability of IT by providing management with tools to assess and measure their organisation’s IT environment against the 34 IT processes COBIT identifies.

**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.

**MATURITY MODELS** for control over IT processes consist of developing a method of scoring so that an organisation can grade itself from non-existent to optimised (from 0 to 5). This approach has been derived from the Maturity Model that the Software Engineering Institute defined for the maturity of the software development capability2. Against these levels, developed for each of COBIT’s 34 IT processes, management can map:

• The current status of the organisation — where the organisation is today

• The current status of (best-in-class in) the industry — the comparison

• The current status of international standards — additional comparison

• The organisation’s strategy for improvement — where the organisation wants to be

|  |  |
| --- | --- |
| **Generic Maturity Model** | |
| 0 | **Non-Existent**. Complete lack of any recognisable processes. The organisation has not even recognised that there is an issue to be addressed. |
| 1 | **Initial**. There is evidence that the organisation has recognised that the issues exist and need to be addressed. There are however no standardised processes but instead there are ad hoc approaches that tend to be applied on an individual or case by case basis. The overall approach to management is disorganised. |
| 2 | **Repeatable.** Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and therefore errors are likely. |
| 3 | **Defined.** Procedures have been standardised and documented, and communicated through training. It is however left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices. |
| 4 | **Managed**. It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way. |
| 5 | **Optimised**. Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other organisations. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt. |

The Maturity Models are built up starting from the generic qualitative model (see above) to which practices and principles from the following domains are added in increasing manner through the levels:

• Understanding and awareness of risks and control issues

• Training and communication applied on the issues

• Process and practices that are implemented

• Techniques and automation to make processes more effective and efficient

• Degree of compliance to internal policy, laws and regulations

• Type and extent of expertise employed.

In summary, Maturity Models:

◆ Refer to business requirements and the enabling aspects at the different maturity levels

◆Are a scale that lends itself to pragmatic comparison

◆Are a scale where the difference can be made measurable in an easy manner

◆Are recognisable as a “profile” of the enterprise relative to IT governance, security and control

◆ Help setting “As-Is” and “To-Be” positions relative to IT governance, security and control maturity

◆ Lend themselves to do gap analysis to determine what needs to be done to achieve a chosen level

◆Avoid, where possible, discrete levels that create thresholds that are difficult to cross

◆ Increasingly apply critical success factors

◆Are not industry specific nor always applicable, the type of business defines what is appropriate.

**CRITICAL SUCCESS FACTORS (CSF)** define the most important issues or actions for management to achieve control over and within its IT processes. They must be management oriented implementation guidelines and identify the most important things to do, strategically, technically, organisationally or procedurally.

Guidance can be obtained from the standard Control Model below. It follows the principles we all know when setting the room temperature (standard) for the heating system (process) which will constantly check (compare) ambient room temperature (control information) and will signal (act) the heating system to provide more heat. This model and its principles identify a number of Critical Success Factors that usually apply to all processes as they deal with what is the standard, who sets it, who controls or needs to act, etc.:

• Defined and documented processes

• Defined and documented policies

• Clear accountabilities

• Strong support/commitment of management

• Appropriate communication to concerned internal and external persons

• Consistent measurement practices.

Further guidance in developing critical success factors can be obtained by examining the objectives and monitoring guidelines of the IT Governance Framework. IT governance is the responsibility of executives and shareholders. It is a system of control that ensures that the business objectives are achieved. This usually consists of directing the organisation’s IT endeavours after reviewing its reported performance against some simple norms that call for:

• IT to be aligned with the business

• IT to enable the business and maximise its benefits

• IT resources to be used responsibly

• IT related risks to be managed appropriately.

In summary, Critical Success Factors are:

◆ Essential enablers focused on the process or supporting environment

◆A thing or a condition that is required for optimal success or an activity recommended for optimal success

◆ The most important things to do to increase the probability of success of the process

◆ Observable — usually measurable — characteristics of the organisation and process

◆ Either strategic, technological, organisational or procedural in nature

◆ Focused on obtaining, maintaining and leveraging capability and skills

◆ Expressed in terms of the process, not necessarily the business.

**KEY GOAL INDICATORS (KGI)** define measures that tell management — after the fact — whether an IT process has achieved its business requirements, usually expressed in terms of information criteria:

• Availability of information needed to support the business needs

• Absence of integrity and confidentiality risks

• Cost-efficiency of processes and operations

• Confirmation of reliability, effectiveness and compliance.

Key Goal Indicators should not be vague, but measurable as a number or percentage. These measures should show that information and technology are contributing to the mission and strategy of the organisation. Because goals and targets are specific to the enterprise and its environment, many Key Goal Indicators have been expressed with a direction, e.g., increased availability, decreased cost. In practice, management will have to set specific targets which need to be met, taking into account past performance and future goals.

To illustrate the previous points, a set of generic Key Goal Indicators is listed below that is usually applicable to all IT processes:

• Achieving targeted return on investment or business value benefits

• Enhanced performance management

• Reduced IT risks

• Productivity improvements

• Integrated supply chains

• Standardised processes

• Boost of service delivery (sales)

• Reaching new and satisfying existing customers

• Creation of new service delivery channels

• Availability of bandwidth, computing power and IT delivery mechanisms fitting the business, and their uptime and downtime

• Meeting requirements and expectations of the customer of the process on budget and on time

• Number of customers and cost per customer served

• Adherence to industry standards.

In summary, Key Goal Indicators are:

◆A representation of the process goal, i.e., a measure of “what,” or a target to achieve

◆ The description of the outcome of the process and therefore ‘LAG’indicators, i.e., measurable after the fact

◆ Immediate indicators of the successful completion of the process or indirect indicators of the value the process delivered to the business

◆ Possibly descriptions of a measure of the impact of not reaching the process goal

◆ Focused on the customer and financial dimensions of the Balanced Business Scorecard

◆ IT oriented but business driven

◆ Expressed in precise, measurable terms wherever possible

◆ Focused on those information criteria that have been identified as most importance for this process.

**KEY PERFORMANCE INDICATORS (KPI)** define measures to determine how well the IT process is performing in enabling the goal to be reached; are lead indicators of whether a goal will likely be reached or not; and are good indicators of capabilities, practices and skills.

Key Performance Indicators are short, focused and measurable indicators of performance of the enabling factors of the IT processes, indicating how well the process enables the goal to be reached. While Key Goal Indicatorss focus on «what», the Key Performance Indicators are concerned with «how». They will often be a measure of a Critical Success Factor and, when monitored and acted upon, will identify opportunities for the improvement of the process. These improvements should positively influence the outcome and, as such, Key Performance Indicators have a cause-effect relationship with the Key Goal Indicators of the process.

In summary, Key Performance Indicators:

◆Are a measure of how well the process is performing

◆ Predict the probability of success or failure in the future, i.e., are ‘LEAD’indicators

◆Are process oriented, but IT driven

◆ Focus on the process and learning dimensions of the Balanced Business Scorecard

◆Are expressed in precisely measurable terms

◆ Will help in improving the IT process when measured and acted upon

◆ Focus on those resources identified as the most important for this process.

The Management Guidelines are consistent with and build upon the existing COBIT Framework, Control Objectives and Audit Guidelines. In addition, to help focus on performance management, the principles of the Balanced Business Scorecard1 were used. They assisted in defining Key Goal Indicators to identify and measure outcomes of processes and Key Performance Indicators to assess how well processes are performing by measuring the enablers of the process. In our information services dominated environment, IT has become the major enabler of the business.

**Framework**

A successful organization 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 COBIT Framework states that IT enables the business by delivering the information the business needs. IT’s goal is therefore measured by looking at COBIT’s Information Criteria contained in the COBIT Framework.

The Framework identifies which of the seven information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability) :

1. **Effectiveness** : deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
2. **Efficiency :** concerns the provision of information through the optimal (most productive and economical) use of resources.
3. **Confidentiality :** concerns the protection of sensitive information from unauthorised disclosure.
4. **Integrity:** relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
5. **Availability:** relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
6. **Compliance:** deals with complying with those laws, regulations and contractual arrangements to which the business process is subject; i.e., externally imposed business criteria.
7. **Reliability of Information**: relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities.

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

**Data :** are objects in their widest sense (i.e., external and internal), structured and non-structured, graphics, sound, etc.

**Application Systems** : are understood to be the sum of manual and programmed procedures.

**Technology:** covers hardware, operating systems, database management systems, networking, multimedia, etc.

**Facilities:** are all the resources to house and support, information systems.

**People:** include staff skills, awareness and productivity to plan, organise, acquire, deliver, support and monitor information systems and services.

The COBIT Framework consists of high-level Control Objectives and an overall structure for their classification. The underlying theory for the classification is that there are, in essence, three levels of IT efforts when considering the management of IT resources. Starting at the bottom, there are the activities and tasks needed to achieve a measurable result. Activities have a lifecycle concept while tasks are more discrete. The life-cycle concept has typical control requirements different from discrete activities. Processes are then defined one layer up as a series of joined activities or tasks with natural (control) breaks. At the highest level, processes are naturally grouped together into domains. Their natural grouping is often confirmed as responsibility domains in an organisational structure and is in line with the management cycle or life-cycle applicable to IT processes.

Thus, the conceptual framework can be approached from three vantage points: (1) Information Criteria, (2) IT Resources and (3) IT Processes. For example, managers may want to look with a Quality, Fiduciary or Security interest (included in the Framework as seven specific information criteria). An IT manager, on the other hand, may want to consider IT resources for which he/she is accountable. Process owners, IT specialists and users may have a specific interest in particular processes or activities/tasks. Auditors may wish to approach the Framework from a control coverage point of view. These three vantage points are depicted in the COBIT Cube.

With the above as the framework, the domains are identified using wording that management would use in the day-to-day activities of the organisation—not auditor jargon. Thus, four broad domains are identified: planning and organisation, acquisition and implementation, delivery and support, and monitoring.

Definitions for the four domains identified for the high-level classification are:

1. **Planning and Organisation**

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organisation as well as technological infrastructure must be put in place.

1. **Acquisition and Implementation**

To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.

1. **Delivery and Support**

This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. In order to deliver services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls.

1. **Monitoring**

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management’s oversight of the organisation’s control process and independent assurance provided by internal and external audit or obtained from alternative sources.

It should be noted that these processes can be applied at different levels within an organisation. For example, some of these processes will be applied at the enterprise level, others at the information services function level, others at the business process owner level, etc.

It should also be noted that the effectiveness criterion of processes that plan or deliver solutions for business requirements will sometimes cover the criteria for availability, integrity and confidentiality—in practice, they have become business requirements. For example, the process of “identify solutions” has to be effective in providing the Availability, Integrity and Confidentiality requirements.

It is clear that all control measures will not necessarily satisfy the different business requirements for information to the same degree.

• **Primary** is the degree to which the defined control objective directly impacts the information criterion concerned.

**• Secondary** is the degree to which the defined control objective only satisfies to a lesser extent or indirectly the information criterion concerned.

**• Blank** could be applicable; however, requirements are more appropriately satisfied by another criteria in this process and/or by another process.

Similarly, not all control measures will necessarily impact the different IT resources to the same degree. Therefore, the COBIT Framework specifically indicates the applicability of the IT resources that are specifically managed by the process under consideration (not those that merely take part in the process). This classification is made within the COBIT Framework based on the same rigorous process of input from researchers, experts and reviewers, using the strict definitions previously indicated.

**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.

The Control Objectives have been organised by process/activity, to facilitate combined or global approaches, such as installation/implementation of a process, global management responsibilities for a process and the use of IT resources by a process.

The Control Objectives have been defined in a generic way, i.e., not depending on the technical platform, while accepting the fact that some special technology environments may need separate coverage for control objectives.

**Audit Guidelines**

Analyze, 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.

**CONCLUSION**

To get Information Technology under control such that IT is aligned with the business and enables it by delivering the information the organisation needs, a number of management tools have been provided in these Management Guidelines. The relationship between the Critical Success Factors, the Maturity Models, the Key Performance Indicators and the Key Goal Indicators can be expressed as:

“CSFs are the most important things you need to do based on the choices made in the Maturity Model, whilst monitoring through KPIs whether you will likely reach the goals set by the KGIs.”

However, it needs to be emphasised that these guidelines remain generic, generally applicable and do not provide industry specific measures. Organisations will in many cases need to customise this general set of directions to their own environment.

Starting from the COBIT Framework, the application of international standards and guidelines, and research into best practices have led to the development of the Control Objectives. Audit Guidelines have been developed to assess whether these Control Objectives are appropriately implemented. However, management needs a similar application of the Framework so it can self-assess and make choices for control implementation and improvements over its information and related technology.

That is the main purpose of the Management Guidelines, developed with the help of world-wide experts in the field of IT governance, performance management, and information security and control. They provide a set of tools to assist management in responding to the question:

|  |  |
| --- | --- |
| **PLANNING AND ORGANISATION** | **DELIVERY AND SUPPORT** |
| PO1 Define a Strategic IT Plan | DS1 Define and Manage Service Levels |
| PO2 Define the Information Architecture | DS2 Manage Third-Party Services |
| PO3 Determine Technological Direction | DS3 Manage Performance and Capacity |
| PO4 Define the IT Organisation and Relationships | DS4 Ensure Continuous Service |
| PO5 Manage the IT Investment | DS5 Ensure Systems Security |
| PO6 Communicate Management Aims and Direction | DS6 Identify and Allocate Costs |
| PO7 Manage Human Resources | DS7 Educate and Train Users |
| PO8 Ensure Compliance with External Requirements | DS8 Assist and Advise Customers |
| PO9 Assess Risks | DS9 Manage the Configuration |
| PO10 Manage Projects | DS10 Manage Problems and Incidents |
| PO11 Manage Quality | DS11 Manage Data |
|  | DS12 Manage Facilities DS13 Manage Operations |
| **ACQUISITION AND IMPLEMENTATION** |  |
| AI1 Identify Automated Solutions | **MONITORING** |
| AI2 Acquire and Maintain Application Software | M1 Monitor the Processes |
| AI3 Acquire and Maintain Technology Infrastructure | M2 Assess Internal Control Adequacy |
| AI4 Develop and Maintain Procedures | M3 Obtain Independent Assurance |
| AI5 Install and Accredit Systems | M4 Provide for Independent Audit |
| AI6 Manage Changes |  |

The following pages provide detailed Management Guidelines for each of the 34 COBIT processes and Appendix I provides guidance on how to read them.