Governing Information Technology Through COBIT

Erik Guldentops CISA
Advisor, IT Governance Institute Board
Brussels, Belgium
erik.guldentops@pandora.be

Abstract: This paper[1] covers the following questions: - what is IT governance and why is it important; - whom does it concern; - what can they do about it; - what does it cover; - what questions should be asked; - how is it accomplished; - how does your organisation compare. After an introduction to COBIT, the COBIT Framework is explained and specific attention is given to the COBIT management guidelines.

Key words: IT Governance, COBIT, corporate governance, control objectives, risk assessment, management guidelines, benchmarking, performance indicators, critical success factors

1. WHAT IS IT GOVERNANCE AND WHY IS IT IMPORTANT?

As information technology has become a critical driver of business success, boards of directors have not kept pace. IT demands thorough and thoughtful board governance, yet such oversight has often been lacking

[1] This presentation is based on *Board Briefing on IT Governance*, published in 2001 by the IT Governance Institute™. It is available for complimentary download, as an open standard, from www.ITgovernance.org/resources.htm. The presentation is also based on *Control jectives for Information and related Technology (COBIT®) 3rd Edition©*, published in 1998 by the IT Governance Institute and distributed through the Information Systems Audit and Control Association® (ISACA™). All portions of COBIT, with the exception of the Audit Guidelines, are an open standard and are available for complimentary download at *www.isaca.org/cobit.htm*

M. Gertz et al. (eds.), *Integrity, Internal Control and Security in Information Systems*

because IT has been seen as an operations matter best left to management, and board members lacked interest or expertise in technology issues.

While boards have always scrutinized business strategy and strategic risks, IT has tended to be overlooked, despite the fact that it involves large investments and huge risks. Reasons include:

- The technical insight required to understand how IT enables the enterprise — and creates risks and opportunities;
- The tradition of treating IT as an entity separate to the business;
- The complexity of IT, even more apparent in the extended enterprise operating in a networked economy.

Closing the IT governance gap has become imperative as it becomes more difficult to separate an organisation's overall strategic mission from the underlying IT strategy that enables that mission to be fulfilled.

IT governance is ultimately important because expectations and reality often do not match. Boards expect management to juggle a myriad of responsibilities: deliver quality IT solutions on time and on budget, harness and exploit IT to return business value and leverage IT to increase efficiency and productivity while managing IT risks. However, boards frequently see business losses, damaged reputations or weakened competitive positions, unmet deadlines, higher-than-expected costs, lower-than-expected quality and failures of IT initiatives to deliver promised benefits.

IT governance extends the board's mission of defining strategic direction and ensuring that objectives are met, risks are managed and resources are used responsibly. Pervasive use of technology has created a critical dependency on IT that calls for a specific focus on IT governance. Such governance should ensure that an organization's IT sustains and extends its strategies and objectives.

Effective IT governance:

- Protects shareholder value;
- Makes clear that IT risks are quantified and understood;
- Directs and controls IT investment, opportunity, benefits and risks;
- Aligns IT with the business while accepting IT is a critical input to and component of the strategic plan, influencing strategic opportunities;
- Sustains current operations and prepares for the future;
- Is an integral part of a global governance structure.

2. WHOM DOES IT CONCERN?

Like most other governance activities, IT governance intensively engages both board and executive management in a cooperative manner. However, due to complexity and specialisation, this governance layer must rely heavily on the lower layers in the enterprise to provide the information needed in its decision-making and evaluation activities. To have effective IT governance in the enterprise, the lower layers need to apply the same principles of setting objectives, providing and getting direction, and providing and evaluating performance measures. As a result, good practices in IT governance need to be applied throughout the enterprise.

3. WHAT CAN THEY DO ABOUT IT?

Among the board's responsibilities are reviewing and guiding corporate strategy, setting and monitoring achievement of management's performance objectives, and ensuring the integrity of the organisation's systems.

3.1 How Should the Board Address the Challenges?

The board should drive enterprise alignment by:

- Ascertaining that IT strategy is aligned with enterprise strategy;
- Ascertaining that IT delivers against the strategy through clear expectations and measurement;
- Directing IT strategy to balance investments between supporting and growing the enterprise;
- Making considered decisions about where IT resources should be focused.

The board should direct management to *deliver measurable value* through IT by:

- Delivering on time and on budget;
- Enhancing reputation, product leadership and cost-efficiency;
- Providing customer trust and competitive time-to-market.

The board should also *measure performance* by:

- Defining and monitoring measures together with management to verify that objectives are achieved and to measure performance to eliminate surprises;

- Leveraging a system of balanced business scorecards maintained by management that form the basis for executive management compensation.

The board should *manage enterprise risk* by:

- Ascertaining that there is transparency about the significant risks to the organisation;
- Being aware that the final responsibility for risk management rests with the board;
- Being conscious that risk mitigation can generate cost-efficiencies;
- Considering that a proactive risk management approach can create competitive advantage;
- Insisting that risk management be embedded in the operation of the enterprise;
- Ascertaining that management has put processes, technology and assurance in place for information security to ensure that:
  - Business transactions can be trusted;
  - IT services are usable, can appropriately resist attacks and recover from failures;
  - Critical information is withheld from those who should not have access to it.

3.2 How Should Executive Management Address the Expectations?

The executive's focus is generally on cost-efficiency, revenue enhancement and building capabilities, all of which are enabled by information, knowledge and the IT infrastructure. Because IT is an integral part of the enterprise, and as its solutions become more and more complex (outsourcing, third-party contracts, networking, etc.), adequate governance becomes a critical factor for success. To this end, management should:

- *Embed clear accountabilities* for risk management and control over IT into the organisation;
- *Cascade strategy*, *policies* and *goals* down into the enterprise and *align the IT organisation* with the enterprise goals;
- *Provide organisational structures* to support the implementation of IT strategies and an *IT infrastructure* to facilitate the creation and sharing of business information;
- *Measure performance* by having outcome measures[3] for business value and competitive advantage that IT delivers and performance drivers to show how well IT performs;

- *Focus on core business competencies IT must support*, i.e. those that add customer value, differentiate the enterprise's products and services in the marketplace, and add value across multiple products and services over time;
- *Focus on important IT processes* that improve business value, such as change, applications and problem management. Management must become aggressive in defining these processes and their associated responsibilities;
- *Focus on core IT competencies* that usually relate to planning and overseeing the management of IT assets, risks, projects, customers and vendors;
- *Have clear external sourcing strategies*, focussing on the management of third-party contracts and associated service level and on building trust between organisations, enabling interconnectivity and information sharing.

3.3 What Does It Cover?

Fundamentally, IT governance is concerned about two things: that IT delivers value to the business and that IT risks are mitigated. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise. Both need measurement, for example, by a balanced scorecard. This leads to the four main focus areas for IT governance, all driven by stakeholder value. Two of them are outcomes: value delivery and risk mitigation. Two of them are drivers: strategic alignment and performance measurement.

3.3.1 IT Strategic Alignment — "IT alignment is a journey, not a destination."

The key question is whether a firm's investment in IT is in harmony with its strategic objectives (intent, current strategy and enterprise goals) and thus building the capabilities necessary to deliver business value. This state of harmony is referred to as "alignment." It is complex, multifaceted and never completely achieved. It is about continuing to move in the right direction and being better aligned than competitors. This may not be attainable for many enterprises because enterprise goals change too quickly, but is nevertheless a worthwhile ambition because there is real concern about the value of IT investment.

Alignment of IT has been synonymous with IT strategy, i.e., does the IT strategy support the enterprise strategy? For IT governance, alignment

encompasses more than strategic integration between the (future) IT organisation and the (future) enterprise organisation. It is also about whether IT operations are aligned with the current enterprise operations. Of course, it is difficult to achieve IT alignment when enterprise units are misaligned.

3.3.2 IT Value Delivery—"IT value is in the eye of the beholder."

The basic principles of IT value are delivery on time, within budget and with the benefits that were promised. In business terms, this is often translated into: competitive advantage, elapsed time for order/service fulfillment, customer satisfaction, customer wait time, employee productivity and profitability. Several of these elements are either subjective or difficult to measure, something all stakeholders need to be aware of.

The value that IT adds to the business is a function of the degree to which the IT organisation is aligned with the business and meets the expectations of the business. The business has expectations relative to the contents of the IT deliverable:

- Fit for purpose, meeting business requirements;
- Flexibility to adopt future requirements;
- Throughput and response times;
- Ease of use, resiliency and security;
- Integrity, accuracy and currency of information.

The business also has expectations regarding the method of working:

- Time-to-market;
- Cost and time management;
- Partnering success;
- Skill set of IT staff.

To manage these expectations, IT and the business should use a common language for value which translates business and IT terminology and is based wholly on fact.

3.3.3 Performance Measurement — "In IT, if you're playing the game and not keeping score, you're just practising."

Strategy has taken on a new urgency as enterprises mobilise intangible and hidden assets to compete in an information-based global economy. Balanced scorecards translate strategy into action to achieve goals with a performance measurement system that goes beyond conventional

accounting, measuring those relationships and knowledge-based assets necessary to compete in the information age: *customer* focus, *process* efficiency and the ability to *learn* and grow. At the heart of these scorecards is management information supplied by the IT infrastructure. IT also enables and sustains solutions for the actual goals set in the financial (enterprise resource management), customer (customer relationship management), process (intranet and workflow tools) and learning (knowledge management) dimensions of the scorecard.

IT needs its own scorecard. Defining clear goals and good measures that unequivocally reflect the business impact of the IT goals is a challenge and needs to be resolved in co-operation among the different governance layers within the enterprise. The linkage between the business balanced scorecard and the IT balanced scorecard is a strong method of alignment.

3.3.4 Risk Management — "It's the IT alligators you don't see that will get you."

Enterprise risk comes in many varieties, not only financial risk. Regulators are specifically concerned about operational and systemic risk, within which technology risk and information security issues are prominent. Infrastructure protection initiatives in the US and the UK point to the utter dependence of all enterprises on IT infrastructures and the vulnerability to new technology risks. The first recommendation these initiatives make is for risk awareness of senior corporate officers.

Therefore, the board should manage enterprise risk by:

- Ascertaining that there is *transparency* about the significant risks to the organisation and clarifying the risk-taking or risk-avoidance policies of the enterprise;
- Being aware that the final *responsibility* for risk management rests with the board so, when delegating to executive management, making sure the constraints of that delegation are communicated and clearly understood;
- Being conscious that the system of internal control put in place to manage risks often has the capacity to generate *cost-efficiency;*
- Considering that a transparent and proactive risk management approach can create *competitive advantage* that can be exploited;
- Insisting that risk management is *embedded in the operation* of the enterprise, responds quickly to changing risks and reports immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).

4. WHAT QUESTIONS SHOULD BE ASKED?

While it is not the most efficient IT governance process, asking tough questions is an effective way to get started. Of course, those responsible for governance want good answers to these questions. Then they want action. Then they need follow-up. It is essential to determine, along with the action, *who* is responsible to deliver *what* by *when*.

An extensive checklist of questions is provided in *Board Briefing on IT Governance*. The questions focus on three objectives: questions asked to discover IT issues, to find out what management is doing about them, and to self-assess the board's governance over them. For example:

To Uncover IT Issues
- How often do IT projects fail to deliver what they promised?
- Are end users satisfied with the quality of the IT service?
- Are sufficient IT resources, infrastructure and competencies available to meet strategic objectives?

To Find Out How Management Addresses the IT Issues
- How well are enterprise and IT objectives aligned?
- How is the value delivered by IT being measured?
- What strategic initiatives has executive management taken to manage IT's criticality relative to maintenance and growth of the enterprise, and are they appropriate?

To Self-assess IT Governance Practices
- Is the board regularly briefed on IT risks to which the enterprise is exposed?
- Is IT a regular item on the agenda of the board and is it addressed in a structured manner?
- Does the board articulate and communicate the business objectives for IT alignment?

5. HOW IS IT ACCOMPLISHED?

Action plans for implementing effective IT governance, from both a board and an executive management point of view, are provided in detail in *Board Briefing on IT Governance*. These plans consist of the following elements:

- *Activities* list what is done to exercise the IT governance responsibilities and the *subjects* identify those items that typically get onto an IT governance agenda.
- *Outcome measures* relate directly to the subjects of IT governance, such as the alignment of business and IT objectives, cost-efficiencies realised by IT, capabilities and competencies generated and risks and opportunities addressed.
- *Best practices* list examples of how the activities are being performed by those who have established leadership in governance of technology.
- *Critical success factors* are conditions, competencies and attitudes that are critical to being successful in the practices.
- *Performance drivers* provide indicators on *how* IT governance is achieving, as opposed to the outcome measures that measure *what* is being achieved. They often relate to the critical success factors.

The plans list IT governance activities and link a set of subjects and practices to them. Practices are classified to reflect the IT governance area(s) to which they provide the greatest contribution: value delivery, strategic alignment, risk management and/or performance (V, A, R, P). A list of critical success factors is provided in support of the practices. Finally, two sets of measures are listed: outcome measures that relate to the IT governance subjects and performance drivers that relate to how activities are performed and the associated practices and critical success factors.

6. HOW DOES YOUR ORGANISATION COMPARE?

For effective governance of IT to be implemented, organisations need to assess how well they are currently performing and be able to identify where and how improvements can be made. This applies to both the IT governance process itself and to all the processes that need to be managed within IT.

The use of maturity models greatly simplifies this task and provides a pragmatic and structured approach for measuring how well developed your processes are against a consistent and easy-to-understand scale:

0 = Non-existent. Management processes are not applied at all.
1 = Initial. Processes are ad hoc and disorganised.
2 = Repeatable. Processes follow a regular pattern.
3 = Defined. Processes are documented and communicated.
4 = Managed. Processes are monitored and measured.
5 = Optimised. Best practices are followed and automated.

(For a complete description of the various maturity levels, see *Board Briefing on IT Governance.*)

Using this technique the organisation can:

- Build a view of current practices by discussing them in workshops and comparing to example models;
- Set targets for future development by considering model descriptions higher up the scale and comparing to best practices;
- Plan projects to reach the targets by defining the specific changes required to improve management;
- Prioritise project work by identifying where the greatest impact will be made and where it is easiest to implement.

7. INTRODUCING COBIT

Control Objectives for Information and related Technology (COBIT) was initially published by the Information Systems Audit and Control Foundation™ (ISACF™) in 1996, and was followed by a second edition in 1998. The third edition, which incorporates all-new material on IT governance and Management Guidelines, was issued by the IT Governance Institute in 2000. COBIT presents an international and generally accepted IT control framework enabling organisations to implement an IT governance structure throughout the enterprise.

Since its first issuance, COBIT has been adopted in corporations and by governmental entities throughout the world.

All portions of COBIT, except the Audit Guidelines, are considered an open standard and may be downloaded on a complimentary basis from the Information Systems Audit and Control Association's web site, *www.isaca.org/cobit.htm.* The Audit Guidelines are available on a downloadable basis to ISACA members only.

8. THE COBIT FRAMEWORK

Business orientation is the main theme of COBIT. It begins from the premise that IT needs to deliver the information that the enterprise needs to achieve its objectives. It is designed to be employed as comprehensive guidance for management and business process owners. Increasingly, business practice involves the full empowerment of business process owners

so they have total responsibility for all aspects of the business process. In particular, this includes providing adequate controls. COBIT promotes a process focus and process ownership.

The COBIT Framework provides a tool for the business process owner that facilitates the discharge of this responsibility. The Framework starts from a simple and pragmatic premise:

In order to provide the information that the organisation needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

The Framework continues with a set of 34 high-level Control Objectives, one for each of the IT processes, grouped into four domains:

- **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.
- **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 lifecycle is continued for these systems.
- **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.*
- **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.

Corresponding to each of the 34 high-level control objectives is an Audit Guideline to enable the review of IT processes against COBIT's 318 recommended detailed control objectives to provide management assurance and/or advice for improvement.

The Management Guidelines further enhances and enables enterprise management to deal more effectively with the needs and requirements of IT governance. The guidelines are action-oriented and generic and provide management direction for getting the enterprise's information and related processes under control, for monitoring achievement of organisational goals, for monitoring performance within each IT process and for benchmarking organisational achievement.

COBIT also contains an Implementation Tool Set that provides lessons learned from those organisations that quickly and successfully applied COBIT in their work environments. It has two particularly useful tools—Management Awareness Diagnostic and IT Control Diagnostic—to assist in analyzing an organisation's IT control environment.

Over the next few years, the management of organisations will need to demonstrably attain increased levels of security and control. COBIT is a tool that allows managers to bridge the gap with respect to control requirements, technical issues and business risks and communicate that level of control to stakeholders. COBIT enables the development of clear policy and good practice for IT control throughout organisations, worldwide. Thus, COBIT is designed to be *the* break-through IT governance tool that helps in understanding and managing the risks and benefits associated with information and related IT.

9. THE COBIT CONTROL OBJECTIVES

For the purposes of COBIT, the following definitions are provided. "Control" is adapted from the COSO Report *(Internal Control—Integrated Framework*, Committee of Sponsoring Organisations of the Treadway Commission, 1992) and "IT Control Objective" is adapted from the SAC Report *(Systems Auditability and Control Report*, The Institute of Internal Auditors Research Foundation, 1991 and 1994).

Control is defined as the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

IT Control Objective is a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

To satisfy business objectives, information needs to conform to certain criteria, which COBIT refers to as business requirements for information. In establishing the list of requirements, COBIT combines the principles embedded in existing and known reference models:

- **Quality requirements**—Quality, Cost, Delivery;
- **Fiduciary requirements** (COSO Report)—Effectiveness and Efficiency of operations; Reliability of Information; Compliance with laws and regulations;
- **Security requirements**—Confidentiality; Integrity; Availability.

Starting the analysis from the broader Quality, Fiduciary and Security requirements, seven distinct, certainly overlapping, categories were extracted. COBIT's working definitions are as follows:

- **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.
- **Efficiency** concerns the provision of information through the optimal (most productive and economical) use of resources.
- **Confidentiality** concerns the protection of sensitive information from unauthorised disclosure.
- **Integrity** relates to accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- **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.
- **Compliance** deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria.
- **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.

The IT resources identified in COBIT can be explained/defined as follows:

- **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.

COBIT consists of high-level control objectives for each process which identify which information criteria are most important in that IT process, state which resources will usually be leveraged and provide considerations on what is important for controlling that IT process. The underlying theory for the classification of the control objectives 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 lifecycle 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 lifecycle 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.

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 satisfies only to a lesser extent or indirectly the information criterion concerned.
- **Blank** could be applicable; however, requirements are more appropriately satisfied by another criterion in this process and/or by another process.

Similarly, all control measures will not 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 a rigorous process of input from researchers, experts and reviewers, using the strict definitions previously indicated.

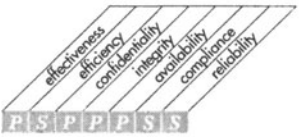
Each high-level control objective is accompanied by detailed control objectives, 318 in all, providing additional detail on how control should be exercised over that particular process. In addition, extensive audit guidelines are included for building on the objectives.

Sample high-level control objectives, with their related detailed control objectives, follow for PO9, the Assess Risks process in the Planning and Organisation domain, and DS5, the Ensure System Security process in the Delivery and Support domain.

PO9 Planning & Organisation
Assess Risks

COBIT

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assessing risks

that satisfies the business requirement

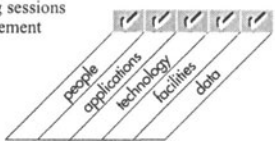
of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors

is enabled by

the organisation engaging itself in IT risk-identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks

and takes into consideration

- risk management ownership and accountability
- different kinds of IT risks (technology, security, continuity, regulatory, etc.)
- defined and communicated risk tolerance profile
- root cause analyses and risk brainstorming sessions
- quantitative and/or qualitative risk measurement
- risk assessment methodology
- risk action plan
- timely reassessment



CONTROL OBJECTIVES PO9

DETAILED CONTROL OBJECTIVES

9 ASSESS RISKS

9.1 Business Risk Assessment
CONTROL OBJECTIVE
Management should establish a systematic risk assessment framework. Such a framework should incorporate a regular assessment of the relevant information risks to the achievement of the business objectives, forming a basis for determining how the risks should be managed to an acceptable level. The process should provide for risk assessments at both the global level and system specific level, for new projects as well as on a recurring basis, and with cross-disciplinary participation. Management should ensure that reassessments occur and that risk assessment information is updated with results of audits, inspections and identified incidents.

9.2 Risk Assessment Approach
CONTROL OBJECTIVE
Management should establish a general risk assessment approach which defines the scope and boundaries, the methodology to be adopted for risk assessments, the responsibilities and the required skills. Management should lead the identification of the risk mitigation solution and be involved in identifying vulnerabilities. Security specialists should lead threat identification and IT specialists should drive the control selection. The quality of the risk assessments should be ensured by a structured method and skilled risk assessors.

9.3 Risk Identification
CONTROL OBJECTIVE
The risk assessment approach should focus on the examination of the essential elements of risk and the cause/effect relationship between them. The essential elements of risk include tangible and intangible assets, asset value, threats, vulnerabilities, safeguards, consequences and likelihood of threat. The risk identification process should include qualitative and, where appropriate, quantitative risk ranking and should obtain input from management brainstorming, strategic planning, past audits and other assessments. The risk assessment should consider business, regulatory, legal, technology, trading partner and human resources risks.

9.4 Risk Measurement
CONTROL OBJECTIVE
The risk assessment approach should ensure that the analysis of risk identification information results in a quantitative and/or qualitative measurement of risk to which the examined area is exposed. The risk acceptance capacity of the organisation should also be assessed.

9.5 Risk Action Plan
CONTROL OBJECTIVE
The risk assessment approach should provide for the definition of a risk action plan to ensure that cost-effective controls and security measures mitigate exposure to risks on a continuing basis. The risk action plan should identify the risk strategy in terms of risk avoidance, mitigation or acceptance.

9.6 Risk Acceptance
CONTROL OBJECTIVE
The risk assessment approach should ensure the formal acceptance of the residual risk, depending on risk identification and measurement, organisational policy, uncertainty incorporated in the risk assessment approach itself and the cost effectiveness of implementing safeguards and controls. The residual risk should be offset with adequate insurance coverage, contractually negotiated liabilities and self-insurance.

continued on next page

DETAILED CONTROL OBJECTIVES *continued*

9.7 **Safeguard Selection**
CONTROL OBJECTIVE
While aiming for a reasonable, appropriate and proportional system of controls and safeguards, controls with the highest return on investment (ROI) and those that provide quick wins should receive first priority. The control system also needs to balance prevention, detection, correction and recovery measures. Furthermore, management needs to communicate the purpose of the control measures, manage conflicting measures and monitor the continuing effectiveness of all control measures.

9.8 **Risk Assessment Commitment**
CONTROL OBJECTIVE
Management should encourage risk assessment as an important tool in providing information in the design and implementation of internal controls, in the definition of the IT strategic plan and in the monitoring and evaluation mechanisms.

DS5 Delivery & Support
Ensure Systems Security

COBIT

HIGH-LEVEL CONTROL OBJECTIVE

Control over the IT process of

ensuring systems security

that satisfies the business requirement

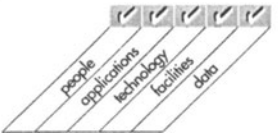
to safeguard information against unauthorised use, disclosure or modification, damage or loss

is enabled by

logical access controls which ensure that access to systems, data and programmes is restricted to authorised users

and takes into consideration

- confidentiality and privacy requirements
- authorisation, authentication and access control
- user identification and authorisation profiles
- need-to-have and need-to-know
- cryptographic key management
- incident handling, reporting and follow-up
- virus prevention and detection
- firewalls
- centralised security administration
- user training
- tools for monitoring compliance, intrusion testing and reporting



CONTROL OBJECTIVES DS5

DETAILED CONTROL OBJECTIVES

5 ENSURE SYSTEMS SECURITY

5.1 Manage Security Measures

CONTROL OBJECTIVE

IT security should be managed such that security measures are in line with business requirements. This includes:

- Translating risk assessment information to the IT security plans
- Implementing the IT security plan
- Updating the IT security plan to reflect changes in the IT configuration
- Assessing the impact of change requests on IT security
- Monitoring the implementation of the IT security plan
- Aligning IT security procedures to other policies and procedures

5.2 Identification, Authentication and Access

CONTROL OBJECTIVE

The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorisation mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorised personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimise the need for authorised users to use multiple sign-ons. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes).

5.3 Security of Online Access to Data

CONTROL OBJECTIVE

In an online IT environment, IT management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.

5.4 User Account Management

CONTROL OBJECTIVE

Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included. The security of third-party access should be defined contractually and address administration and non-disclosure requirements. Outsourcing arrangements should address the risks, security controls and procedures for information systems and networks in the contract between the parties.

5.5 Management Review of User Accounts

CONTROL OBJECTIVE

Management should have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be made to help reduce the risk of errors, fraud, misuse or unauthorised alteration.

5.6 User Control of User Accounts

CONTROL OBJECTIVE

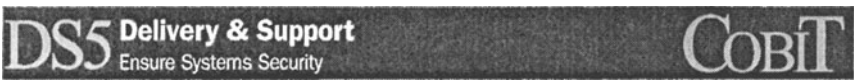
Users should systematically control the activity of their proper account(s). Also information mechanisms should be in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.

5.7 Security Surveillance

CONTROL OBJECTIVE

IT security administration should ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner.

continued on next page



DETAILED CONTROL OBJECTIVES *continued*

5.8 **Data Classification**
CONTROL OBJECTIVE
Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing "no protection" should require a formal decision to be so designated. Owners should determine disposition and sharing of data, as well as whether and when programs and files are to be maintained, archived or deleted. Evidence of owner approval and data disposition should be maintained. Policies should be defined to support reclassification of information, based on changing sensitivities. The classification scheme should include criteria for managing exchanges of information between organisations, addressing both security and compliance with relevant legislation.

5.9 **Central Identification and Access Rights Management**
CONTROL OBJECTIVE
Controls are in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.

5.10 **Violation and Security Activity Reports**
CONTROL OBJECTIVE
IT security administration should ensure that violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorised activity. The logical access to the computer resources accountability information (security and other logs) should be granted based upon the principle of least privilege, or need-to-know.

5.11 **Incident Handling**
CONTROL OBJECTIVE
Management should establish a computer security incident handling capability to address security incidents by providing a centralised platform with sufficient expertise and equipped with rapid and secure communication facilities. Incident management responsibilities and procedures should be established to ensure an appropriate, effective and timely response to security incidents.

5.12 **Reaccreditation**
CONTROL OBJECTIVE
Management should ensure that reaccreditation of security (e.g., through "tiger teams") is periodically performed to keep up-to-date the formally approved security level and the acceptance of residual risk.

5.13 **Counterparty Trust**
CONTROL OBJECTIVE
Organisational policy should ensure that control practices are implemented to verify the authenticity of the counterparty providing electronic instructions or transactions. This can be implemented through trusted exchange of passwords, tokens or cryptographic keys.

5.14 **Transaction Authorisation**
CONTROL OBJECTIVE
Organisational policy should ensure that, where appropriate, controls are implemented to provide authenticity of transactions and establish the validity of a user's claimed identity to the system. This requires use of cryptographic techniques for signing and verifying transactions.

CONTROL OBJECTIVES DS5

5.15 **Non-Repudiation**
CONTROL OBJECTIVE
Organisational policy should ensure that, where appropriate, transactions cannot be denied by either party, and controls are implemented to provide non-repudiation of origin or receipt, proof of submission, and receipt of transactions. This can be implemented through digital signatures, time stamping and trusted third-parties, with appropriate policies that take into account relevant regulatory requirements.

5.16 **Trusted Path**
CONTROL OBJECTIVE
Organisational policy should ensure that sensitive transaction data is only exchanged over a trusted path. Sensitive information includes security management information, sensitive transaction data, passwords and cryptographic keys. To achieve this, trusted channels may need to be established using encryption between users, between users and systems, and between systems.

5.17 **Protection of Security Functions**
CONTROL OBJECTIVE
All security related hardware and software should at all times be protected against tampering to maintain their integrity and against disclosure of secret keys. In addition, organisations should keep a low profile about their security design, but should not base their security on the design being secret.

5.18 **Cryptographic Key Management**
CONTROL OBJECTIVE
Management should define and implement procedures and protocols to be used for generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure. If a key is compromised, management should ensure this information is propagated to any interested party through the use of Certificate Revocation Lists or similar mechanisms.

5.19 **Malicious Software Prevention, Detection and Correction**
CONTROL OBJECTIVE
Regarding malicious software, such as computer viruses or trojan horses, management should establish a framework of adequate preventative, detective and corrective control measures, and occurrence response and reporting. Business and IT management should ensure that procedures are established across the organisation to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response and reporting.

5.20 **Firewall Architectures and Connections with Public Networks**
CONTROL OBJECTIVE
If connection to the Internet or other public networks exists, adequate firewalls should be operative to protect against denial of services and any unauthorised access to the internal resources; should control any application and infrastructure management flows in both directions; and should protect against denial of service attacks.

5.21 **Protection of Electronic Value**
CONTROL OBJECTIVE
Management should protect the continued integrity of all cards or similar physical mechanisms used for authentication or storage of financial or other sensitive information, taking into consideration the related facilities, devices, employees and validation methods used.

10. COBIT'S MANAGEMENT GUIDELINES

COBIT's Management Guidelines consist of maturity models, critical success factors (CSFs), key goal indicators (KGIs) and key performance indicators (KPIs). This structure 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 COBIT's 34 IT processes.

COBIT's Management Guidelines are generic and action-oriented for the purpose of addressing the following types of management concerns:

- Performance measurement — What are the indicators of good performance?
- IT control profiling — What's important? What are the critical success factors for control?
- Awareness — What are the risks of not achieving our objectives?
- Benchmarking — What do others do? How do we measure and compare?

An answer to these requirements of determining and monitoring the appropriate IT security and control level is the definition of specific:

- **Benchmarking** of IT control practices (expressed as maturity models);
- **Performance indicators** of the IT processes—for their outcome and their performance;
- **Critical success factors** for getting these processes under control.

The Management Guidelines are consistent with and build upon the principles of the balanced business scorecard.[4] In "simple terms," these measures will assist management in monitoring their IT organisation by answering the following questions:

1. *What is the management concern?* Make sure that the enterprise needs are fulfilled.
2. *Where is it measured?* On the balanced business scorecard as a key goal indicator, representing an outcome of the business process.
3. *What is the IT concern?* That the IT processes deliver on a timely basis the right information to the enterprise, enabling the business needs to be fulfilled. This is a critical success factor for the enterprise.
4. *Where is that measured?* On the IT balanced scorecard, as a key goal indicator representing the outcome for IT, which is that information is delivered with the right criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability).

5. *What else needs to be measured?* Whether the outcome is positively influenced by a number of critical success factors that need to be measured as key performance indicators of how well IT is doing.

Each element of the Management Guidelines will be examined in further detail.

10.1 Maturity Models

IT management is constantly on the lookout for benchmarking and self-assessment tools in response to the need to know what to do in an efficient manner. Starting from COBIT's processes and high-level control objectives, the process owner should be able to incrementally benchmark against that control objective. This creates three needs:

- A relative measure of where the organisation is;
- A manner to decide efficiently where to go;
- A tool for measuring progress against the goal.

The approach to maturity models for control over IT processes consists of developing a method of scoring so that an organisation can grade itself from non-existent to optimised (from 0 to 5). This approach is based on the maturity model that the Software Engineering Institute defined for the maturity of the software development capability.[5] Whatever the model, the scales should not be too granular, as that would render the system difficult to use and suggest a precision that is not justifiable.

In contrast, one should concentrate on maturity levels based on a set of conditions that can be unambiguously met. Against 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 standard guidelines — additional comparison;
- The organisation's strategy for improvement — where the organisation wants to be.

For each of the 34 IT processes, there is an incremental measurement scale, based on a rating of 0 through 5. The scale is associated with generic qualitative maturity model descriptions ranging from Non-existent to Optimised as follows:

- **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 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 model scales help professionals explain to managers where IT management shortcomings exist and set targets for where they need to be by comparing their organisation's control practices to the best practice examples. The right maturity level will be influenced by the enterprise's business objectives and operating environment. Specifically, the level of control maturity depends on the enterprise's dependence on IT, its technology sophistication and, most importantly, the value of its information.

A strategic reference point for an organisation to improve security and control could also consist of looking at emerging international standards and best-in-class practices. The emerging practices of today may become the expected level of performance of tomorrow and is therefore useful for planning where an organisation wants to be over time.

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, where differences can be made measurable in an easy manner;
- Help setting "as-is" and "to-be" positions relative to IT governance, security and control maturity;
- Lend themselves to 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.

10.2 Critical Success Factors

Critical success factors provide management with guidance for implementing control over IT and its processes. They are the most important things to do that contribute to the IT process achieving its goals. They are activities that can be of a strategic, technical, organisational, process or procedural nature. They are usually dealing with capabilities and skills and have to be short, focused and action-oriented, leveraging the resources that are of primary importance in the process under consideration.

A number of critical success factors can be deduced that apply to most IT processes.

Applying to IT in general

- IT processes are defined and aligned with the IT strategy and the business goals.
- The customers of the process and their expectations are known.
- Processes are scalable and their resources are appropriately managed and leveraged.
- The required quality of staff (training, transfer of information, morale, etc.) and availability of skills (recruit, retain, retrain) exist.
- IT performance is measured in financial terms, in relation to customer satisfaction, for process effectiveness and for future capability. IT management is rewarded based on these measures.
- A continuous quality improvement effort is applied.

Applying to most IT processes

- All process stakeholders (users, management, etc.) are aware of the risks, of the importance of IT and the opportunities it can offer, and provide strong commitment and support.
- Goals and objectives are communicated across all disciplines and understood; it is known how processes implement and monitor objectives, and who is accountable for process performance.
- People are goal-focused and have the right information on customers, on internal processes and on the consequences of their decisions.
- A business culture is established, encouraging cross-divisional co-operation, teamwork and continuous process improvement.
- There is integration and alignment of major processes, e.g., change, problem and configuration management.
- Control practices are applied to increase efficient and optimal use of resources and improve the effectiveness of processes.

Applying to IT governance

- Control practices are applied to increase transparency, reduce complexity, promote learning, provide flexibility and scalability, and avoid breakdowns in internal control and oversight.
- Practices that enable sound oversight are applied: a control environment and culture; a code of conduct; risk assessment as a standard practice; self-assessments; formal compliance on adherence to established standards; monitoring and follow-up of control deficiencies and risk.
- IT governance is recognised and defined, and its activities are integrated into the enterprise governance process, giving clear direction for IT strategy, a risk management framework, a system of controls and a security policy.
- IT governance focuses on major IT projects, change initiatives and quality efforts, with awareness of major IT processes, the responsibilities and the required resources and capabilities.
- An audit committee is established to appoint and oversee an independent auditor, drive the IT audit plan and review the results of audits and third party opinions.

In summary, critical success factors are:

- Essential enablers focused on the process or supporting environment;
- A thing or a condition that is required 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.

10.3 Key Goal Indicators

A key goal indicator, representing the process goal, is a measure of *what* has to be accomplished. It is a measurable indicator of the process achieving its goals, often defined as a target to achieve. By comparison, a key performance indicator is a measure of *how well* the process is performing.

How are business and IT goals and measures linked? The COBIT Framework expresses the objectives for IT in terms of the information criteria that the business needs in order to achieve the business objectives, which will usually be expressed in terms of:

- Availability of systems and services;
- Absence of integrity and confidentiality risks;
- Cost-efficiency of processes and operations;
- Confirmation of reliability, effectiveness and compliance.

The goal for IT can then be expressed as delivering the information that the business needs in line with these criteria. These information criteria are provided in the Management Guidelines with an indication whether they have primary or secondary importance for the process under review. In practice, the information criteria profile of an enterprise would be more specific. The degree of importance of each of the information criteria is a function of the business and the environment in which the enterprise operates.

Key goal indicators are *lag* indicators, as they can be measured only after the fact, as opposed to key performance indicators, which are *lead* indicators, giving an indication of success before the fact. They also can be expressed negatively, i.e., in terms of the impact of not reaching the goal.

Key goal indicators should be 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 has to set specific targets which need to be met, taking into account past performance and future goals.

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 important for this process.

10.4 Key Performance Indicators

Key performance indicators are measures that tell management that an IT process is achieving its business requirements by monitoring the performance of the enablers of that IT process. Building on balanced business scorecard principles, the relationship between key performance indicators and key goal indicators is as follows: 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 indicators focus on *what*, the key performance indicators are concerned with *how*. They often are a measure of a critical success factor and, when monitored and acted upon, 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.

While key goal indicators are business-driven, key performance indicators are process-oriented and often express how well the processes and the organisation leverage and manage the needed resources. Similar to key goal indicators, they often are expressed as a number or percentage. A good test of a key performance indicator is to see whether it really does predict success or failure of the process goal and whether or not it assists management in improving the process.

Some generic key performance indicators follow that usually are applicable to all IT processes:

Applying to IT in general
- Reduced cycle times (i.e., responsiveness of IT production and development);
- Increased quality and innovation;
- Utilisation of communications bandwidth and computing power;
- Service availability and response times;
- Satisfaction of stakeholders (survey and number of complaints);
- Number of staff trained in new technology and customer service skills.

Applying to most IT processes
- Improved cost-efficiency of the process (cost vs. deliverables);
- Staff productivity (number of deliverables) and morale (survey);
- Amount of errors and rework.

Applying to IT governance
- Benchmark comparisons;
- Number of non-compliance reportings.

In summary, key performance indicators:
- Are measures 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;
- Help in improving the IT process when measured and acted upon;
- Focus on those resources identified as the most important for this process.

11. MANAGEMENT GUIDELINES FOR SELECTED COBIT PROCESSES

Although COBIT consists of 34 high-level IT control practices, through extensive testing and surveying, the 15 most important have been identified. On the following pages, COBIT's Management Guideline for seven of these 15 processes is included, outlining critical success factors, key goal indicators, key performance indicators and a maturity model for each.

PO1 Planning & Organisation
Define a Strategic Information Technology Plan

COBIT

Control over the IT process **Define a Strategic IT Plan** with the business goal of *striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment*

ensures delivery of information to the business that addresses the required Information Criteria and is measured by Key Goal Indicators

is enabled by *a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals*

considers Critical Success Factors that leverage specific IT Resources and is measured by Key Performance Indicators

Information Criteria
P effectiveness
S efficiency
confidentiality
integrity
availability
compliance
reliability

(P) primary (S) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Key Goal Indicators

- Percent of IT and business strategic plans that are aligned and cascaded into long- and short-range plans leading to individual responsibilities
- Percent of business units that have clear, understood and current IT capabilities
- Management survey determines clear link between responsibilities and the business and IT strategic goals
- Percent of business units using strategic technology covered in the IT strategic plan
- Percent of IT budget championed by business owners
- Acceptable and reasonable number of outstanding IT projects

Critical Success Factors

- The planning process provides for a prioritisation scheme for the business objectives and quantifies, where possible, the business requirements
- Management buy-in and support is enabled by a documented methodology for the IT strategy development, the support of validated data and a structured, transparent decision-making process
- The IT strategic plan clearly states a risk position, such as leading edge or road-tested, innovator or follower, and the required balance between time-to-market, cost of ownership and service quality
- All assumptions of the strategic plan have been challenged and tested
- The processes, services and functions needed for the outcome are defined, but are flexible and changeable, with a transparent change control process
- A reality check of the strategy by a third party has been conducted to increase objectivity and is repeated at appropriate times
- IT strategic planning is translated into roadmaps and migration strategies

Key Performance Indicators

- Currency of IT capabilities assessment (number of months since last update)
- Age of IT strategic plan (number of months since last update)
- Percent of participant satisfaction with the IT strategic planning process
- Time lag between change in the IT strategic plans and changes to operating plans
- Index of participants involved in strategic IT plan development, based on size of effort, ratio of involvement of business owners to IT staff and number of key participants
- Index of quality of the plan, including timelines of development effort, adherence to structured approach and completeness of plan

MANAGEMENT GUIDELINES PO1

PO1 Maturity Model

Control over the IT process **Define a Strategic IT Plan** with the business goal of *striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment*

0 Non-existent IT strategic planning is not performed. There is no management awareness that IT strategic planning is needed to support business goals.

1 Initial/Ad Hoc The need for IT strategic planning is known by IT management, but there is no structured decision process in place. IT strategic planning is performed on an as needed basis in response to a specific business requirement and results are therefore sporadic and inconsistent. IT strategic planning is occasionally discussed at IT management meetings, but not at business management meetings. The alignment of business requirements, applications and technology takes place reactively, driven by vendor offerings, rather than by an organisation-wide strategy. The strategic risk position is identified informally on a project-by-project basis.

2 Repeatable but Intuitive IT strategic planning is understood by IT management, but is not documented. IT strategic planning is performed by IT management, but only shared with business management on an as needed basis. Updating of the IT strategic plan occurs only in response to requests by management and there is no proactive process for identifying those IT and business developments that require updates to the plan. Strategic decisions are driven on a project-by-project basis, without consistency with an overall organisation strategy. The risks and user benefits of major strategic decisions are being recognised, but their definition is intuitive.

3 Defined Process A policy defines when and how to perform IT strategic planning. IT strategic planning follows a structured approach, which is documented and known to all staff. The IT planning process is reasonably sound and ensures that appropriate planning is likely to be performed. However, discretion is given to individual managers with respect to implementation of the process and there are no procedures to examine the process on a regular basis. The overall IT strategy includes a consistent definition of risks that the organisation is willing to take as an innovator or follower. The IT financial, technical and human resources strategies increasingly drive the acquisition of new products and technologies.

4 Managed and Measurable IT strategic planning is standard practice and exceptions would be noticed by management. IT strategic planning is a defined management function with senior level responsibilities. With respect to the IT strategic planning process, management is able to monitor it, make informed decisions based on it and measure its effectiveness. Both short-range and long-range IT planning occurs and is cascaded down into the organisation, with updates done as needed. The IT strategy and organisation-wide strategy are increasingly becoming more coordinated by addressing business processes and value-added capabilities and by leveraging the use of applications and technologies through business process re-engineering. There is a well-defined process for balancing the internal and external resources required in system development and operations. Benchmarking against industry norms and competitors is becoming increasingly formalised.

5 Optimised IT strategic planning is a documented, living process, is continuously considered in business goal setting and results in discernable business value through investments in IT. Risk and value added considerations are continuously updated in the IT strategic planning process. There is an IT strategic planning function that is integral to the business planning function. Realistic long-range IT plans are developed and constantly being updated to reflect changing technology and business-related developments. Short-range IT plans contain project task milestones and deliverables, which are continuously monitored and updated, as changes occur. Benchmarking against well-understood and reliable industry norms is a well-defined process and is integrated with the strategy formulation process. The IT organisation identifies and leverages new technology developments to drive the creation of new business capabilities and improve the competitive advantage of the organisation.

PO9 Planning & Organisation
Assess Risks

COBIT

Control over the IT process **Assess Risks** with the business goal of *supporting management decisions in achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors*

ensures delivery of information to the business that addresses the required Information Criteria and is measured by Key Goal Indicators

is enabled by *the organisation engaging itself in IT risk-identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks*

considers Critical Success Factors that leverage specific IT Resources and is measured by Key Performance Indicators

Information Criteria	
P	effectiveness
S	efficiency
P	confidentiality
P	integrity
P	availability
S	compliance
S	reliability

(P) primary (S) secondary

IT Resources	
✓	people
✓	applications
✓	technology
✓	facilities
✓	data

(✓) applicable to

Key Goal Indicators

- Increased degree of awareness of the need for risk assessments
- Decreased number of incidents caused by risks identified after the fact
- Increased number of identified risks that have been sufficiently mitigated
- Increased number of IT processes that have formal documented risk assessments completed
- Appropriate percent or number of cost effective risk assessment measures

Critical Success Factors

- There are clearly defined roles and responsibilities for risk management ownership and management accountability
- A policy is established to define risk limits and risk tolerance
- The risk assessment is performed by matching vulnerabilities, threats and the value of data
- Structured risk information is maintained, fed by incident reporting
- Responsibilities and procedures for defining, agreeing on and funding risk management improvements exist
- Focus of the assessment is primarily on real threats and less on theoretical ones
- Brainstorming sessions and root cause analyses leading to risk identification and mitigation are routinely performed
- A reality check of the strategy is conducted by a third party to increase objectivity and is repeated at appropriate times

Key Performance Indicators

- Number of risk management meetings and workshops
- Number of risk management improvement projects
- Number of improvements to the risk assessment process
- Level of funding allocated to risk management projects
- Number and frequency of updates to published risk limits and policies
- Number and frequency of risk monitoring reports
- Number of personnel trained in risk management methodology

MANAGEMENT GUIDELINES PO9

PO9 Maturity Model

Control over the IT process **Assess Risks** with the business goal of *supporting management decisions in achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors*

0 Non-existent Risk assessment for processes and business decisions does not occur. The organisation does not consider the business impacts associated with security vulnerabilities and with development project uncertainties. Risk management has not been identified as relevant to acquiring IT solutions and delivering IT services.

1 Initial/Ad Hoc The organisation is aware of its legal and contractual responsibilities and liabilities, but considers IT risks in an ad hoc manner, without following defined processes or policies. Informal assessments of project risk take place as determined by each project. Risk assessments are not likely to be identified specifically within a project plan or to be assigned to specific managers involved in the project. IT management does not specify responsibility for risk management in job descriptions or other informal means. Specific IT-related risks such as security, availability and integrity are occasionally considered on a project-by-project basis. IT-related risks affecting day-to-day operations are infrequently discussed at management meetings. Where risks have been considered, mitigation is inconsistent.

2 Repeatable but Intuitive There is an emerging understanding that IT risks are important and need to be considered. Some approach to risk assessment exists, but the process is still immature and developing. The assessment is usually at a high-level and is typically applied only to major projects. The assessment of on-going operations depends mainly on IT managers raising it as an agenda item, which often only happens when problems occur. IT management has not generally defined procedures or job descriptions dealing with risk management.

3 Defined Process An organisation-wide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff through training. Decisions to follow the process and to receive training are left to the individual's discretion. The methodology is convincing and sound, and ensures that key risks to the business are likely to be identified. Decisions to follow the process are left to individual IT managers and there is no procedure to ensure that all projects are covered or that the ongoing operation is examined for risk on a regular basis.

4 Managed and Measurable The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by IT management. It is likely that IT risk management is a defined management function with senior level responsibility. The process is advanced and risk is assessed at the individual project level and also regularly with regard to the overall IT operation. Management is advised on changes in the IT environment which could significantly affect the risk scenarios, such as an increased threat from the network or technical trends that affect the soundness of the IT strategy. Management is able to monitor the risk position and make informed decisions regarding the exposure it is willing to accept. Senior management and IT management have determined the levels of risk that the organisation will tolerate and have standard measures for risk/return ratios. Management budgets for operational risk management projects to reassess risks on a regular basis. A risk management database is established.

5 Optimised Risk assessment has developed to the stage where a structured, organisation-wide process is enforced, followed regularly and well managed. Risk brainstorming and root cause analysis, involving expert individuals, are applied across the entire organisation. The capturing, analysis and reporting of risk management data are highly automated. Guidance is drawn from leaders in the field and the IT organisation takes part in peer groups to exchange experiences. Risk management is truly integrated into all business and IT operations, is well accepted and extensively involves the users of IT services.

PO10 Planning & Organisation
Manage Projects

COBIT

Control over the IT process **Manage Projects** with the business goal of *setting priorities and delivering on time and within budget*

ensures delivery of information to the business that addresses the required Information Criteria and is measured by Key Goal Indicators

is enabled by *the organisation identifying and prioritising projects in line with the operational plan and the adoption and application of sound project management techniques for each project undertaken*

considers Critical Success Factors that leverage specific IT Resources and is measured by Key Performance Indicators

Information Criteria	
P	effectiveness
P	efficiency
	confidentiality
	integrity
	availability
	compliance
	reliability

(P) primary (S) secondary

IT Resources	
✓	people
✓	applications
✓	technology
✓	facilities
	data

(✓) applicable to

Key Goal Indicators

- Increased number of projects completed on time and on budget
- Availability of accurate project schedule and budget information
- Decrease in systemic and common project problems
- Improved timeliness of project risk identification
- Increased organisation satisfaction with project delivered services
- Improved timeliness of project management decisions

Critical Success Factors

- Experienced and skilled project managers are available
- An accepted and standard programme management process is in place
- There is senior management sponsorship of projects, and stakeholders and IT staff share in the definition, implementation and management of projects
- There is an understanding of the abilities and limitations of the organisation and the IT function in managing large, complex projects
- An organisation-wide project risk assessment methodology is defined and enforced
- All projects have a plan with clear traceable work breakdown structures, reasonably accurate estimates, skill requirements, issues to track, a quality plan and a transparent change process
- The transition from the implementation team to the operational team is a well-managed process
- A system development life cycle methodology has been defined and is used by the organisation

Key Performance Indicators

- Increased number of projects delivered in accordance with a defined methodology
- Percent of stakeholder participation in projects (involvement index)
- Number of project management training days per project team member
- Number of project milestone and budget reviews
- Percent of projects with post-project reviews
- Average number of years of experience of project managers

MANAGEMENT GUIDELINES PO10

PO10 Maturity Model

Control over the IT process **Manage Projects** with the business goal of *setting priorities and delivering on time and within budget*

0 Non-existent Project management techniques are not used and the organisation does not consider business impacts associated with project mismanagement and development project failures.

1 Initial/Ad Hoc The organisation is generally aware of the need for projects to be structured and is aware of the risks of poorly managed projects. The use of project management techniques and approaches within IT is a decision left to individual IT managers. Projects are generally poorly defined and do not incorporate business and technical objectives of the organisation or the business stakeholders. There is a general lack of management commitment and project ownership and critical decisions are made without user management or customer input. There is little or no customer and user involvement in defining IT projects. There is no clear organisation within IT projects and roles and responsibilities are not defined. Project schedules and milestones are poorly defined. Project staff time and expenses are not tracked and compared to budgets.

2 Repeatable but Intuitive Senior management has gained and communicated an awareness of the need for IT project management. The organisation is in the process of learning and repeating certain techniques and methods from project to project. IT projects have informally defined business and technical objectives. There is limited stakeholder involvement in IT project management. Some guidelines have been developed for most aspects of project management, but their application is left to the discretion of the individual project manager.

3 Defined Process The IT project management process and methodology have been formally established and communicated. IT projects are defined with appropriate business and technical objectives. Stakeholders are involved in the management of IT projects. The IT project organisation and some roles and responsibilities are defined. IT projects have defined and updated milestones, schedules, budget and performance measurements. IT projects have formal post system implementation procedures. Informal project management training is provided. Quality assurance procedures and post system implementation activities have been defined, but are not broadly applied by IT managers. Policies for using a balance of internal and external resources are being defined.

4 Managed and Measurable Management requires formal and standardised project metrics and "lessons learned" to be reviewed following project completion. Project management is measured and evaluated throughout the organisation and not just within IT. Enhancements to the project management process are formalised and communicated, and project team members are trained on all enhancements. Risk management is performed as part of the project management process. Stakeholders actively participate in the projects or lead them. Project milestones, as well as the criteria for evaluating success at each milestone, have been established. Value and risk are measured and managed prior to, during and after the completion of projects. Management has established a programme management function within IT. Projects are defined, staffed and managed to increasingly address organisation goals, rather than only IT specific ones.

5 Optimised A proven, full life-cycle project methodology is implemented and enforced, and is integrated into the culture of the entire organisation. An on-going programme to identify and institutionalise best practices has been implemented. There is strong and active project support from senior management sponsors as well as stakeholders. IT management has implemented a project organisation structure with documented roles, responsibilities and staff performance criteria. A long-term IT resources strategy is defined to support development and operational outsourcing decisions. An integrated programme management office is responsible for projects from inception to post implementation. The programme management office is under the management of the business units and requisitions and directs IT resources to complete projects. Organisation-wide planning of projects ensures that user and IT resources are best utilised to support strategic initiatives.

AI6 Acquisition & Implementation
Manage Changes

COBIT

Control over the IT process **Manage Changes** with the business goal of *minimising the likelihood of disruption, unauthorised alterations and errors*

ensures delivery of information to the business that addresses the required Information Criteria and is measured by Key Goal Indicators

is enabled by *a management system which provides for the analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure*

considers Critical Success Factors that leverage specific IT Resources and is measured by Key Performance Indicators

Information Criteria	IT Resources
P effectiveness	✓ people
P efficiency	✓ applications
confidentiality	✓ technology
P integrity	✓ facilities
P availability	✓ data
compliance	
S reliability	

(P) primary (S) secondary (✓) applicable to

Critical Success Factors

- Change policies are clear and known and they are rigorously and systematically implemented
- Change management is strongly integrated with release management and is an integral part of configuration management
- There is a rapid and efficient planning, approval and initiation process covering identification, categorisation, impact assessment and prioritisation of changes
- Automated process tools are available to support workflow definition, pro-forma workplans, approval templates, testing, configuration and distribution
- Expedient and comprehensive acceptance test procedures are applied prior to making the change
- A system for tracking and following individual changes, as well as change process parameters, is in place
- A formal process for hand-over from development to operations is defined
- Changes take the impact on capacity and performance requirements into account
- Complete and up-to-date application and configuration documentation is available
- A process is in place to manage co-ordination between changes, recognising interdependencies
- An independent process for verification of the success or failure of change is implemented
- There is segregation of duties between development and production

Key Goal Indicators

- Reduced number of errors introduced into systems due to changes
- Reduced number of disruptions (loss of availability) caused by poorly managed change
- Reduced impact of disruptions caused by change
- Reduced level of resources and time required as a ratio to number of changes
- Number of emergency fixes

Key Performance Indicators

- Number of different versions installed at the same time
- Number of software release and distribution methods per platform
- Number of deviations from the standard configuration
- Number of emergency fixes for which the normal change management process was not applied retroactively
- Time lag between the availability of the fix and its implementation
- Ratio of accepted to refused change implementation requests

MANAGEMENT GUIDELINES AI6

AI6 Maturity Model

Control over the IT process **Manage Changes** with the business goal of *minimising the likelihood of disruption, unauthorised alterations and errors*

0 Non-existent There is no defined change management process and changes can be made with virtually no control. There is no awareness that change can be disruptive for both IT and business operations, and no awareness of the benefits of good change management.

1 Initial/Ad Hoc It is recognised that changes should be managed and controlled, but there is no consistent process to follow. Practices vary and it is likely that unauthorised changes will take place. There is poor or non-existent documentation of change and configuration documentation is incomplete and unreliable. Errors are likely to occur together with interruptions to the production environment caused by poor change management.

2 Repeatable but Intuitive There is an informal change management process in place and most changes follow this approach; however, it is unstructured, rudimentary and prone to error. Configuration documentation accuracy is inconsistent and only limited planning and impact assessment takes place prior to a change. There is considerable inefficiency and rework.

3 Defined Process There is a defined formal change management process in place, including categorisation, prioritisation, emergency procedures, change authorisation and release management, but compliance is not enforced. The defined process is not always seen as suitable or practical and, as a result, workarounds take place and processes are bypassed. Errors are likely to occur and unauthorised changes will occasionally occur. The analysis of the impact of IT changes on business operations is becoming formalised, to support planned rollouts of new applications and technologies.

4 Managed and Measurable The change management process is well developed and consistently followed for all changes and management is confident that there are no exceptions. The process is efficient and effective, but relies on considerable manual procedures and controls to ensure that quality is achieved. All changes are subject to thorough planning and impact assessment to minimise the likelihood of post-production problems. An approval process for changes is in place. Change management documentation is current and correct, with changes formally tracked. Configuration documentation is generally accurate. IT change management planning and implementation is becoming more integrated with changes in the business processes, to ensure that training, organisational changes and business continuity issues are addressed. There is increased co-ordination between IT change management and business process re-design.

5 Optimised The change management process is regularly reviewed and updated to keep in line with best practices. Configuration information is computer based and provides version control. Software distribution is automated and remote monitoring capabilities are available. Configuration and release management and tracking of changes is sophisticated and includes tools to detect unauthorised and unlicensed software. IT change management is integrated with business change management to ensure that IT is an enabler in increasing productivity and creating new business opportunities for the organisation.

DS5 Delivery & Support
Ensure Systems Security

COBIT

Control over the IT process **Ensure Systems Security** with the business goal of *safeguarding information against unauthorised use, disclosure or modification, damage or loss*

ensures delivery of information to the business that addresses the required Information Criteria and is measured by Key Goal Indicators

is enabled by *logical access controls which ensure that access to the systems, data and programmes is restricted to authorised users*

considers Critical Success Factors that leverage specific IT Resources and is measured by Key Performance Indicators

Information Criteria
effectiveness
efficiency
P confidentiality
P integrity
S availability
S compliance
S reliability

(P) primary (S) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Critical Success Factors

- An overall security plan is developed that covers the building of awareness, establishes clear policies and standards, identifies a cost-effective and sustainable implementation, and defines monitoring and enforcement processes
- There is awareness that a good security plan takes time to evolve
- The corporate security function reports to senior management and is responsible for executing the security plan
- Management and staff have a common understanding of security requirements, vulnerabilities and threats, and they understand and accept their own security responsibilities
- Third-party evaluation of security policy and architecture is conducted periodically
- A "building permit" programme is defined, identifying security baselines that have to be adhered to
- A "drivers licence" programme is in place for those developing, implementing and using systems, enforcing security certification of staff
- The security function has the means and ability to detect, record, analyse significance, report and act upon security incidents when they do occur, while minimising the probability of occurrence by applying intrusion testing and active monitoring
- A centralised user management process and system provides the means to identify and assign authorisations to users in a standard and efficient manner
- A process is in place to authenticate users at reasonable cost, light to implement and easy to use

Key Goal Indicators

- No incidents causing public embarrassment
- Immediate reporting on critical incidents
- Alignment of access rights with organisational responsibilities
- Reduced number of new implementations delayed by security concerns
- Full compliance, or agreed and recorded deviations from minimum security requirements
- Reduced number of incidents involving unauthorised access, loss or corruption of information

Key Performance Indicators

- Reduced number of security-related service calls, change requests and fixes
- Amount of downtime caused by security incidents
- Reduced turnaround time for security administration requests
- Number of systems subject to an intrusion detection process
- Number of systems with active monitoring capabilities
- Reduced time to investigate security incidents
- Time lag between detection, reporting and acting upon security incidents
- Number of IT security awareness training days

MANAGEMENT GUIDELINES DS5

DS5 Maturity Model

Control over the IT process **Ensure Systems Security** with the business goal of *safeguarding information against unauthorised use, disclosure or modification, damage or loss*

0 Non-existent The organisation does not recognise the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process to IT security breaches. There is a complete lack of a recognisable system security administration process.

1 Initial/Ad Hoc The organisation recognises the need for IT security, but security awareness depends on the individual. IT security is addressed on a reactive basis and not measured. IT security breaches invoke "finger pointing" responses if detected, because responsibilities are unclear. Responses to IT security breaches are unpredictable.

2 Repeatable but Intuitive Responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator with no management authority. Security awareness is fragmented and limited. IT security information is generated, but is not analysed. Security solutions tend to respond reactively to IT security incidents and by adopting third-party offerings, without addressing the specific needs of the organisation. Security policies are being developed, but inadequate skills and tools are still being used. IT security reporting is incomplete, misleading or not pertinent.

3 Defined Process Security awareness exists and is promoted by management. Security awareness briefings have been standardised and formalised. IT security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for IT security are assigned, but not consistently enforced. An IT security plan exists, driving risk analysis and security solutions. IT security reporting is IT focused, rather than business focused. Ad hoc intrusion testing is performed.

4 Managed and Measurable Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and practices are completed with specific security baselines. Security awareness briefings have become mandatory. User identification, authentication and authorisation are being standardised. Security certification of staff is being established. Intrusion testing is a standard and formalised process leading to improvements. Cost/benefit analysis, supporting the implementation of security measures, is increasingly being utilised. IT security processes are co-ordinated with the overall organisation security function. IT security reporting is linked to business objectives.

5 Optimised IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimised and included in a verified security plan. Security functions are integrated with applications at the design stage and end users are increasingly accountable for managing security. IT security reporting provides early warning of changing and emerging risk, using automated active monitoring approaches for critical systems. Incidents are promptly addressed with formalised incident response procedures supported by automated tools. Periodic security assessments evaluate the effectiveness of implementation of the security plan. Information on new threats and vulnerabilities is systematically collected and analysed, and adequate mitigating controls are promptly communicated and implemented. Intrusion testing, root cause analysis of security incidents and pro-active identification of risk is the basis for continuous improvements. Security processes and technologies are integrated organisation wide.

DS10 Delivery & Support
Manage Problems and Incidents

COBIT

Control over the IT process **Manage Problems and Incidents** with the business goal of *ensuring that problems and incidents are resolved, and the cause investigated to prevent any recurrence*

ensures delivery of information to the business that addresses the required Information Criteria and is measured by Key Goal Indicators

is enabled by *a problem management system which records and progresses all incidents*

considers Critical Success Factors that leverage specific IT Resources and is measured by Key Performance Indicators

Information Criteria
P effectiveness
P efficiency
confidentiality
integrity
S availability
compliance
reliability

(P) primary (S) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Key Goal Indicators

- A measured reduction of the impact of problems and incidents on IT resources
- A measured reduction in the elapsed time from initial symptom report to problem resolution
- A measured reduction in unresolved problems and incidents
- A measured increase in the number of problems avoided through pre-emptive fixes
- Reduced time lag between identification and escalation of high-risk problems and incidents

Critical Success Factors

- There is clear integration of problem management with availability and change management
- Accessibility to configuration data, as well as the ability to keep track of problems for each configuration component, is provided
- An accurate means of communicating problem incidents, symptoms, diagnosis and solutions to the proper support personnel is in place
- Accurate means exist to communicate to users and IT the exceptional events and symptoms that need to be reported to problem management
- Training is provided to support personnel in problem resolution techniques
- Up-to-date roles and responsibilities charts are available to support incident management
- There is vendor involvement during problem investigation and resolution
- Post-facto analysis of problem handling procedures is applied

Key Performance Indicators

- Elapsed time from initial symptom recognition to entry in the problem management system
- Elapsed time between problem recording and resolution or escalation
- Elapsed time between evaluation and application of vendor patches
- Percent of reported problems with already known resolution approaches
- Frequency of coordination meetings with change management and availability management personnel
- Frequency of component problem analysis reporting
- Reduced number of problems not controlled through formal problem management

MANAGEMENT GUIDELINES DS10

DS10 Maturity Model

Control over the IT process **Manage Problems and Incidents** with the business goal of *ensuring that problems and incidents are resolved, and the cause investigated to prevent any recurrence*

0 Non-existent There is no awareness of the need for managing problems and incidents. The problem-solving process is informal and users and IT staff deal individually with problems on a case-by-case basis.

1 Initial/Ad Hoc The organisation has recognised that there is a need to solve problems and evaluate incidents. Key knowledgeable individuals provide some assistance with problems relating to their area of expertise and responsibility. The information is not shared with others and solutions vary from one support person to another, resulting in additional problem creation and loss of productive time, while searching for answers. Management frequently changes the focus and direction of the operations and technical support staff.

2 Repeatable but Intuitive There is a wide awareness of the need to manage IT related problems and incidents within both the business units and information services function. The resolution process has evolved to a point where a few key individuals are responsible for managing the problems and incidents occurring. Information is shared among staff; however, the process remains unstructured, informal and mostly reactive. The service level to the user community varies and is hampered by insufficient structured knowledge available to the problem solvers. Management reporting of incidents and analysis of problem creation is limited and informal.

3 Defined Process The need for an effective problem management system is accepted and evidenced by budgets for the staffing, training and support of response teams. Problem solving, escalation and resolution processes have been standardised, but are not sophisticated. Nonetheless, users have received clear communications on where and how to report on problems and incidents. The recording and tracking of problems and their resolutions is fragmented within the response team, using the available tools without centralisation or analysis. Deviations from established norms or standards are likely to go undetected.

4 Managed and Measurable The problem management process is understood at all levels within the organisation. Responsibilities and ownership are clear and established. Methods and procedures are documented, communicated and measured for effectiveness. The majority of problems and incidents are identified, recorded, reported and analysed for continuous improvement and are reported to stakeholders. Knowledge and expertise are cultivated, maintained and developed to higher levels as the function is viewed as an asset and major contributor to the achievement of IT objectives. The incident response capability is tested periodically. Problem and incident management is well integrated with interrelated processes, such as change, availability and configuration management, and assists customers in managing data, facilities and operations.

5 Optimised The problem management process has evolved into a forward-looking and proactive one, contributing to the IT objectives. Problems are anticipated and may even be prevented. Knowledge is maintained, through regular contacts with vendors and experts, regarding patterns of past and future problems and incidents. The recording, reporting and analysis of problems and resolutions is automated and fully integrated with configuration data management. Most systems have been equipped with automatic detection and warning mechanism, which are continuously tracked and evaluated.

DS11 Delivery & Support
Manage Data

COBIT

Control over the IT process **Manage Data** with the business goal of *ensuring that data remains complete, accurate and valid during its input, update and storage*

ensures delivery of information to the business that addresses the required Information Criteria and is measured by Key Goal Indicators

is enabled by *an effective combination of application and general controls over the IT operations*

considers Critical Success Factors that leverage specific IT Resources and is measured by Key Performance Indicators

Information Criteria	
	effectiveness
	efficiency
	confidentiality
P	integrity
	availability
	compliance
P	reliability

(P) primary (S) secondary

IT Resources	
	people
	applications
	technology
	facilities
✓	data

(✓) applicable to

Critical Success Factors

- Data entry requirements are clearly stated, enforced and supported by automated techniques at all levels, including database and file interfaces
- The responsibilities for data ownership and integrity requirements are clearly stated and accepted throughout the organisation
- Data accuracy and standards are clearly communicated and incorporated into the training and personnel development processes
- Data entry standards and correction are enforced at the point of entry
- Data input, processing and output integrity standards are formalised and enforced
- Data is held in suspense until corrected
- Effective detection methods are used to enforce data accuracy and integrity standards
- Effective translation of data across platforms is implemented without loss of integrity or reliability to meet changing business demands
- There is a decreased reliance on manual data input and re-keying processes
- Efficient and flexible solutions promote effective use of data
- Data is archived and protected and is readily available when needed for recovery

Key Goal Indicators

- A measured reduction in the data preparation process and tasks
- A measured improvement in the quality, timeline and availability of data
- A measured increase in customer satisfaction and reliance upon the data
- A measured decrease in corrective activities and exposure to data corruption
- Reduced number of data defects, such as redundancy, duplication and inconsistency
- No legal or regulatory data compliance conflicts

Key Performance Indicators

- Percent of data input errors
- Percent of updates reprocessed
- Percent of automated data integrity checks incorporated into the applications
- Percent of errors prevented at the point of entry
- Number of automated data integrity checks run independently of the applications
- Time interval between error occurrence, detection and correction
- Reduced data output problems
- Reduced time for recovery of archived data

MANAGEMENT GUIDELINES DS11

DS11 Maturity Model

Control over the IT process **Manage Data** with the business goal of *ensuring that data remains complete, accurate and valid during its input, update and storage*

0 Non-existent Data is not recognised as a corporate resource and asset. There is no assigned data ownership or individual accountability for data integrity and reliability. Data quality and security is poor or non-existent.

1 Initial/Ad Hoc The organisation recognises a need for accurate data. Some methods are developed at the individual level to prevent and detect data input, processing and output errors. The process of error identification and correction is dependent upon manual activities of individuals, and rules and requirements are not passed on as staff movement and turnover occur. Management assumes that data is accurate because a computer is involved in the process. Data integrity and security are not management requirements and, if security exists, it is administered by the information services function.

2 Repeatable but Intuitive The awareness of the need for data accuracy and maintaining integrity is prevalent throughout the organisation. Data ownership begins to occur, but at a department or group level. The rules and requirements are documented by key individuals and are not consistent across the organisation and platforms. Data is in the custody of the information services function and the rules and definitions are driven by the IT requirements. Data security and integrity are primarily the information services function's responsibilities, with minor departmental involvement.

3 Defined Process The need for data integrity within and across the organisation is understood and accepted. Data input, processing and output standards have been formalised and are enforced. The process of error identification and correction is automated. Data ownership is assigned, and integrity and security are controlled by the responsible party. Automated techniques are utilised to prevent and detect errors and inconsistencies. Data definitions, rules and requirements are clearly documented and maintained by a database administration function. Data becomes consistent across platforms and throughout the organisation. The information services function takes on a custodian role, while data integrity control shifts to the data owner. Management relies on reports and analyses for decisions and future planning.

4 Managed and Measurable Data is defined as a corporate resource and asset, as management demands more decision support and profitability reporting. The responsibility for data quality is clearly defined, assigned and communicated within the organisation. Standardised methods are documented, maintained and used to control data quality, rules are enforced and data is consistent across platforms and business units. Data quality is measured and customer satisfaction with information is monitored. Management reporting takes on a strategic value in assessing customers, trends and product evaluations. Integrity of data becomes a significant factor, with data security recognised as a control requirement. A formal, organisation-wide data administration function has been established, with the resources and authority to enforce data standardisation.

5 Optimised Data management is a mature, integrated and cross-functional process that has a clearly defined and well-understood goal of delivering quality information to the user, with clearly defined integrity, availability and reliability criteria. The organisation actively manages data, information and knowledge as corporate resources and assets, with the objective of maximising business value. The corporate culture stresses the importance of high quality data that needs to be protected and treated as a key component of intellectual capital. The ownership of data is a strategic responsibility with all requirements, rules, regulations and considerations clearly documented, maintained and communicated.

12. ENDNOTES AND REFERENCES

[1] In this document, "stakeholder" is used to indicate anyone who has either a responsibility for or an expectation from the enterprise's IT, e.g., shareholders, directors, executives, business and technology management, users, employees, governments, suppliers, customers and the public.

[2] In this document, "board of directors" and "board" are used to indicate the body that is ultimately accountable to the stakeholders of the enterprise.

[3] The COBIT control framework refers to key goal indicators (KGIs) and key performance indicators (KPIs) for the balanced business scorecard concepts of outcome measures and performance drivers.

[4] "The Balanced Business Scorecard — Measurements that Drive Performance," Robert S. Kaplan and David P. Norton, *Harvard Business Review*, January-February 1992

[5] "Capability Maturity Model SM for Software," Version 1.1. Technical Report CMU/SEI-93-TR-024, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, February 1993

Control Objectives for Information and related Technology (COBIT) 3rd Edition, IT Governance Institute, 1998, *www.isaca.org/cobit.htm* (All sections of COBIT, except the Audit Guidelines, can be downloaded on a complimentary basis. Print copies of all components, including the Audit Guidelines, may be purchased from the ISACA Bookstore; contact *bookstore@isaca.org* for availability.)

Board Briefing on IT Governance, IT Governance Institute, 2001, *www.ITgovernance.org/resources.htm* (May be downloaded on a complimentary basis. Print copies may be purchased from the ISACA Bookstore; contact *bookstore@isaca.org* for availability.)

Information Security Governance: Guidance for Boards of Directors and Executive Management, IT Governance Institute, 2001, *www.ITgovernance.org/resources.htm* (May be downloaded on a complimentary basis. Print copies may be purchased from the ISACA Bookstore; contact *bookstore@isaca.org* for availability.)

About the Author

Erik Guldentops, CISA, was until recently security advisor for the Society of Worldwide Interbank Financial Telecommunication (SWIFTsc) in Brussels, Belgium, where he previously held the positions of chief inspector and director of information security. SWIFT provides secure global communication to more than 7,000 financial institutions in more than 190 countries. More than five million messages valued in trillions of dollars are sent over SWIFT's network every business day. Guldentops is advisor to the board of thIT Governance Institute and an executive professor in the management school of the University of Antwerp, Belgium, where he teaches on the subjects of IT security and control, IT governance and risk management. He initiated and has headed up the developments of Control Objectives for Information and related Technology (COBIT) since the early nineties and is currently the chair of Information Systems Audit and Control Association's COBIT Steering Committee.