COBIT Control Assessment Questionnaire

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

Audit Information:

Audit / Project Name	Auditable Unit # Engagement #	Start Date End Date	Audit Team Lead	Audit Team Members
<Name Here>	<Audit Unit # > <Engagement #>	MM / DD / YYYY MM / DD / YYYY	<Name Here> <Title Here> <Phone Number Here>	• <List Name, Title, & Phone Numbers Here>
Description of Project				
<Description Here>				

Client Information:

Information For Client(s) Participating In The Joint Assessment				Responsible Officers	
Name	**Title**	**Phone**	**Location**	**Name**	**Title**
Other Information					
<This space reserved for use as necessary>					

Overall Rating Assigned For This Assessment*:

Overall Maturity Rating:	***<Rating Here>***

**** In the event that an assessment falls between two maturity ratings, the lower rating is assigned.***

<Please choose between this page and the following page, depending on whether you will use the generic rating definition or a specific rating definition to assign your overall rating.>

Legend For *Generic* COBIT Management Guidelines Maturity Ratings**:

Rating	Description
0 - Non-Existent	Management processes are not in place (Complete lack of any recognizable processes. The organization has not recognized that there is an issue to be addressed).
1 - Initial	Processes are ad hoc and disorganized (There is evidence that the organization has recognized that the issues exist and need to be addressed. However, there are no standardized processes; there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized).
2 - Repeatable	Processes follow a regular pattern (Processes have developed to a stage where different people undertaking the same task follow similar procedures. 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 errors are likely as a result).
3 - Defined	Processes are documented and communicated (Procedures have been standardized and documented and communicated through formal training. However, compliance with the procedures is left to each individual and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated, but are the formalization of existing practices).
4 - Managed	Processes are monitored and measured (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 - Optimized	Best practices are followed and automated (Processes have been refined to a level of best practice, based on the results of continuous improvement and benchmarking with other organizations and industry best practices. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt).

*****Note: Generic Ratings are applied to assessments where the overall review does not correspond specifically to a single one of COBIT's 34 High Level Control Objectives. Where an overall review corresponds to a specific IT process, the specific maturity rating definition as defined in COBIT's Management Guidelines is used.***

Client's Targeted Maturity Rating:***	***<Rating Here>***

****** Client's Targeted Maturity Rating indicates the level of maturity that the assessment owner believes is an appropriate maturity level for the assessment scope. Risks vary across IT processes; it is not desirable for every process to aspire to achieve the highest maturity rating.***

Overall Rating Assigned For This Assessment*:

Overall Maturity Rating:	***<Rating Here>***

**** In the event that an assessment falls between two maturity ratings, the lower rating is assigned.***

<Please choose between this page and the previous page, depending on whether you will use the generic rating definition or a specific rating definition to assign your overall rating. >

Legend For COBIT Management Guidelines Maturity Ratings: *DS10 Manage Problems and Incidents*:

Rating	Description
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	The organization has recognized 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	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	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 standardized, 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 centralization or analysis. Deviations from established norms or standards are likely to go undetected.
4 - Managed	The problem management process is understood at all levels within the organization. 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 analyzed 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 - Optimized	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.

Client's Targeted Maturity Rating**:	***<Rating Here>***

***** Client's Targeted Maturity Rating indicates the level of maturity that the assessment owner believes is an appropriate maturity level for the assessment scope. Risks vary across IT processes; it is not desirable for every process to aspire to achieve the highest maturity rating.***

Summary of Ratings Assigned For Specific High-level Control Objectives of This Assessment*:

**** Maturity ratings for the following specific process areas have been assigned using COBIT's Management Guideline definitions for each specific High-level Control Objective.***

POnn Name of Specific Planning & Organization process area		**<Rating Here>**
n.n	Name of first control objective reviewed	<Rating Here>
n.n	Name of first control objective reviewed	<Rating Here>
AInn Name of Specific Acquisition and Implementation process area		**<Rating Here>**
n.n	Name of first control objective reviewed	<Rating Here>
n.n	Name of first control objective reviewed	<Rating Here>
DSnn Name of Specific Delivery and Support process area		**<Rating Here>**
n.n	Name of first control objective reviewed	<Rating Here>
n.n	Name of first control objective reviewed	<Rating Here>
DSnn Name of Specific Delivery and Support process area		**<Rating Here>**
n.n	Name of first control objective reviewed	<Rating Here>
n.n	Name of first control objective reviewed	<Rating Here>
Mn Name of Specific Monitoring process area		**<Rating Here>**
n.n	Name of first control objective reviewed	<Rating Here>
n.n	Name of first control objective reviewed	<Rating Here>

Assessment Questionnaire Organized By COBIT Objective:

High-level Control Objective: *<High-level Objective 1 (follow CobiT order: PO first, then AI, DS, M)>*	**Overall Maturity Rating:** ***<Insert Rating Here>***

Definition: <COBIT Management Definition of High Level Objective taken from the page in the Management Guidelines booklet with the rating definitions – begins with "Control over the IT process … with the business goal of …>

Detailed Control Objectives	Maturity Rating	Assessment Questions	Client Responses & Assessment Results
EXAMPLE: **Visitor Escort** **Objectives Specific to XYZ Company Technology Area Under Review:** • Visitors should be properly identified prior to being accorded access to the site. • Visitors to critical areas of the site (those areas that house critical computer and network hardware, monitoring areas where hardware and software can be controlled, and environmental control and monitoring areas) should be escorted and monitored by an appropriate IT representative. • Logs should be kept to record activity. • Security guards and general staff should understand the requirements related to admitting visitors to the site. • Visitor access procedures should detail requirements for authorization of entry and supervision. **Applicable COBIT Objective:** • DS12.3 Visitor Escort Appropriate procedures are to be in place ensuring that individuals who are not members of the IT function's operations group are escorted by a member of that group when they must enter the computer facilities. A visitor's log should be kept and reviewed regularly.	<Rating Here>	1. Describe visitor access requirements, detailing identification, escort and monitoring of site visitors. 2. Is a log kept to record the entry and exit of each visitor to the site? 3. Are visitors provided with electronic access badges? If so, please describe any controls relevant to restricting access to appropriate areas of the facility, and terminating access. 4. Are visitor access policies and procedures documented?	
<Name of COBIT Detailed Objective> **Objectives Specific to XYZ Company Technology Area Under Review:** • <Include XYZ Company specific objectives here> **Applicable COBIT Objective:** • <Number and name of COBIT objective> <Text of the control objective as taken from COBIT>	<Rating Here>	1. Assessment Questions Here 2. <Question> 3. <Question> 4. <Question>	

High-level Control Objective: *<High-level Objective 2 (follow CobiT order: PO first, then AI, DS, M)>*	**Overall Maturity Rating: *<Insert Rating Here>***
Definition: <COBIT Management Definition of High Level Objective taken from the page in the Management Guidelines booklet with the rating definitions – begins with "Control over the IT process … with the business goal of …>	

Detailed Control Objectives	Maturity Rating	Assessment Questions	Client Responses & Assessment Results
EXAMPLE: **Visitor Escort** **Objectives Specific to XYZ Company Technology Area Under Review:** • Visitors should be properly identified prior to being accorded access to the site. • Visitors to critical areas of the site (those areas that house critical computer and network hardware, monitoring areas where hardware and software can be controlled, and environmental control and monitoring areas) should be escorted and monitored by an appropriate IT representative. • Logs should be kept to record activity. • Security guards and general staff should understand the requirements related to admitting visitors to the site. • Visitor access procedures should detail requirements for authorization of entry and supervision. **Applicable COBIT Objective:** • DS12.3 Visitor Escort Appropriate procedures are to be in place ensuring that individuals who are not members of the IT function's operations group are escorted by a member of that group when they must enter the computer facilities. A visitor's log should be kept and reviewed regularly.	<Rating Here>	5. Describe visitor access requirements, detailing identification, escort and monitoring of site visitors. 6. Is a log kept to record the entry and exit of each visitor to the site? 7. Are visitors provided with electronic access badges? If so, please describe any controls relevant to restricting access to appropriate areas of the facility, and terminating access. 8. Are visitor access policies and procedures documented?	
<Name of COBIT Detailed Objective> **Objectives Specific to XYZ Company Technology Area Under Review:** • <Include XYZ Company specific objectives here> **Applicable COBIT Objective:** • <Number and name of COBIT objective> <Text of the control objective as taken from COBIT>	<Rating Here>	5. Assessment Questions Here 6. <Question> 7. <Question> 8. <Question>	

High-level Control Objective: *<High-level Objective 3 (follow CobiT order: PO first, then AI, DS, M)>*	**Overall Maturity Rating: *<Insert Rating Here>***

Definition: <COBIT Management Definition of High Level Objective taken from the page in the Management Guidelines booklet with the rating definitions – begins with "Control over the IT process … with the business goal of …>

Detailed Control Objectives	Maturity Rating	Assessment Questions	Client Responses & Assessment Results
EXAMPLE: **Visitor Escort** **Objectives Specific to XYZ Company Technology Area Under Review:** • Visitors should be properly identified prior to being accorded access to the site. • Visitors to critical areas of the site (those areas that house critical computer and network hardware, monitoring areas where hardware and software can be controlled, and environmental control and monitoring areas) should be escorted and monitored by an appropriate IT representative. • Logs should be kept to record activity. • Security guards and general staff should understand the requirements related to admitting visitors to the site. • Visitor access procedures should detail requirements for authorization of entry and supervision. **Applicable COBIT Objective:** • DS12.3 Visitor Escort Appropriate procedures are to be in place ensuring that individuals who are not members of the IT function's operations group are escorted by a member of that group when they must enter the computer facilities. A visitor's log should be kept and reviewed regularly.	<Rating Here>	9. Describe visitor access requirements, detailing identification, escort and monitoring of site visitors. 10. Is a log kept to record the entry and exit of each visitor to the site? 11. Are visitors provided with electronic access badges? If so, please describe any controls relevant to restricting access to appropriate areas of the facility, and terminating access. 12. Are visitor access policies and procedures documented?	
<Name of COBIT Detailed Objective> **Objectives Specific to XYZ Company Technology Area Under Review:** • <Include XYZ Company specific objectives here> **Applicable COBIT Objective:** • <Number and name of COBIT objective> <Text of the control objective as taken from COBIT>	<Rating Here>	9. Assessment Questions Here 10. <Question> 11. <Question> 12. <Question>	

And so on…