Your Company Name

COBIT Checklist and Review

Date

Revision History

Date	Version	Author	Change

Table of Contents

Note: Text displayed in blue italics is included to provide guidance to the author and should be deleted before publishing the document. In any table, select and delete any blue line text; then click Home→Styles and select "Table Text" to restore the cells to the default value.

1 Introduction

The Sarbanes-Oxley Act, including COBIT (Control Objectives for Information and Related Technology), provide for a standardized structure for Information Technology (IT) governance, accounting controls, and compliance.

COBIT provides management and business process owners with an Information Technology control model that helps to understand and manage the risks related with IT. COBIT helps link missing items between business risks, control needs, and technical issues.

Note: Management should review the checklists and determine those areas where information and controls are required and whether current documentation is current or must be revised or developed.

2 COBIT Control Objectives

COBIT Control Objectives focuses on specific, detailed control objectives related with each IT process. For each of the 30+ IT structure processes, there are detailed control objectives that align the overall structure with objectives from primary sources comprising standards and regulations relating to IT. It includes statements of the desired results or objectives to be achieved by implementing specific control procedures within an IT activity and, thereby, provides a clear policy and good practice for IT control throughout the industry and worldwide.

Control objectives provide a working document of specific and clear definitions of a set of controls to ensure effectiveness, efficiency, and economy of resource utilization. For each process, detailed control objectives are identified as the minimum controls needed to be in place. There are 300+ detailed control objectives that provide an overview of the domain, process, and control objective relationships.

3 COBIT Component Summary

COBIT (Control Objectives for Information and Related Technology) is a complete structure for managing Information Technology (IT) risk and control. It includes four domains, 30+ IT processes, and 300+ detailed control objectives. It includes controls that address operational and compliance objectives.

Domain	Process Topics
Plan and Organize (IT Environment)	IT Strategic Planning Information Architecture Determine Technological Direction IT Organization and Relationships Manage the IT Investment Communication of Management Aims and Direction Management of Human Resources Compliance of External Requirements Assessment of Risks Manage Projects Management of Quality
Acquire and Implement (Program Development and Program Change)	Identify Automated Solutions Acquire or Develop Application Software Acquire Technology Infrastructure Develop and Maintain Policies and Procedures Install and Test Application Software and Technology Infrastructure Manage Changes
Deliver and Support (Computer Operations and Access to Programs and Data)	Define and Manage Service Levels Manage Third-Party Services Manage Performance and Capacity Ensure Continuous Service Ensure Systems Security Identify and Allocate Costs Educate and Train Users Assist and Advise Customers Manage the Configurations Manage Problems and Incidents Manage Data Manage Facilities Manage Operations

Monitor and Evaluate (IT Environment)	Monitoring Adequacy of Internal Controls Independent Assurance Internal Audit

The following table includes COBIT domain components.

Components	Description
Control Environment	The control environment establishes the basis for internal control, creates the "direction from the top," and represents the corporate governance structure. Issues raised in the control environment component apply all through the IT organization.
Risk Assessment	Risk assessment provides for management identification and analysis of significant risks to achieve preset objectives, which form the basis for shaping control activities. Risk assessment can take place at the company level or at the activity level (e.g., for a specific process or business unit).
Control Activities	Control activities are the policies, procedures, and practices that ensure business objectives are achieved and risk mitigation strategies are completed. Control activities address control objectives to alleviate their identified risks.
Information and Communication	Organizational information is required to run the business and realize the company's control objectives. Identification, management, and communication of this information represent a challenge to IT.
Monitoring	Monitoring includes the supervision of internal control by management through continuous process review. There are two types of monitoring activities: • Continuous monitoring • Separate evaluations.

4 COBIT Processes

The following summary tables provide an indication, by IT process and domain, of the information criteria impacted by the high-level control objectives.

4.1 Planning and Organization

The Planning and Organization section includes the following topics:

- Define a Strategic IT Plan
- Define the Information Architecture
- Determine the Technological Direction
- Define the IT Organization and Relationships
- Manage the IT Investment
- Communicate Management Aims and Direction
- Manage Human Resources
- Ensure Compliance with External Requirements
- Assess Risks
- Manage Projects
- Manage Quality.

COBIT Topics	Documentation Required (Y/N)	Documentation Up-To-Date (Y/N)
Define a Strategic IT Plan • IT as Part of the Organization's Long- and Short-Range Plan • IT Long-Range Plan • IT Long-Range Planning - Approach and Structure • IT Long-Range Plan Changes • Short-Range Planning for the Information Services Function • Assessment of Existing Systems		
Define the Information Architecture • Information Architecture Model • Corporate Data Dictionary and Data Syntax Rules • Data Classification Scheme • Security Levels		
Determine the Technological Direction • Technological Infrastructure Planning • Monitor Future Trends and Regulations • Technological Infrastructure Contingency • Hardware and Software Acquisition Plans • Technology Standards		

Define the IT Organization and Relationships • The Information Services Function Planning or Steering Committee • Organizational Placement of Information Services Function • Review of Organizational Achievements • Roles and Responsibilities • Responsibility for Quality Assurance • Responsibility for Logical and Physical Security • Ownership and Custodianship • Data and System Ownership • Supervision • Segregation of Duties • IT Staffing • Job or Position Descriptions for Information Services Function Staff • Key IT Personnel • Contracted Staff Procedures • Relationships		
Manage the IT Investment • Annual Information Services Function Operating Budget • Cost and Benefit Monitoring • Cost and Benefit Justification		
Communicate Management Aims and Direction • Positive Information Control Environment • Management's Responsibility for Policies • Communication of Organization Policies • Policy Implementation Resources • Maintenance of Policies • Compliance with Polices, Procedures, and Standards • Quality Commitment • Security and Internal Control Framework Policy • Intellectual Property Rights • Issue Specific Policies • Communication of IT Security Awareness		

Manage Human Resources • Personnel Recruitment and Promotion • Personnel Qualifications • Personnel Training • Cross-Training or Staff Back-up • Personnel Clearance Procedures • Employee Job Performance Evaluation • Job Change and Termination		
Ensure Compliance with External Requirements • External Requirements Review • Practices and Procedures for Complying with External Requirements • Safety and Ergonomic Compliance • Privacy, Intellectual Property, and Data Flow • Electronic Commerce • Compliance with Insurance Contracts		
Assess Risks • Business Risk Assessment • Risk Assessment Approach • Risk Identification • Risk Measurement • Risk Action Plan • Risk Acceptance		
Manage Projects • Project Management Framework • User Department Participation in Project Initiation • Project Team Membership and Responsibilities • Project Definition • Project Approval • Project Phase Approval • Project Master Plan • System Quality Assurance Plan • Planning of Assurance Methods • Formal Project Risk Management • Test Plan • Training Plan • Post-Implementation Review Plan		

Manage Quality • General Quality Plan • Quality Assurance Approach • Quality Assurance Planning • Quality Assurance Review of Adherence to the Information Services Function's Standards and Procedures • System Development Life Cycle Methodology • System Development Life Cycle Methodology for Major Changes to Existing Technology • Updating the System Development Life Cycle Methodology • Coordination and Communication • Acquisition and Maintenance Framework for the Technology Infrastructure • Third-Party Relationships • Program Documentation Standards • Program Testing Standards • System Testing Standards • Parallel / Pilot Testing • System Testing Documentation • Quality Assurance Evaluation of Adherence to Development Standards • Quality Assurance Review of the Achievement of Information Services • Function's Objectives • Quality Metrics • Reports of Quality Assurance Reviews		

4.2 Acquisition and Implementation

The Acquisition and Implementation section includes the following topics:

- Identify Solutions
- Acquire and Maintain Application Software
- Acquire and Maintain Technology Architecture
- Develop and Maintain IT Procedures
- Install and Accredit Systems
- Manage Changes.

COBIT Topics	Documentation Required (Y/N)	Documentation Up-To-Date (Y/N)
Identify Solutions • Definition of Information Requirements • Formulation of Alternative Courses of Action • Formulation of Acquisition Strategy • Third-Party Service Requirements • Technological Feasibility Study • Economic Feasibility Study • Information Architecture • Risk Analysis Report • Cost-Effective Security Controls • Audit Trails Design • Ergonomics • Selection of System Software • Procurement Control • Software Product Acquisition • Third-Party Software Maintenance • Contract Application Programming • Acceptance of Facilities • Acceptance of Technology		

Acquire and Maintain Application Software • Design Methods • Major Changes to Existing Systems • Design Approval • File Requirements Definition and Documentation • Program Specifications • Source Data Collection Design • Input Requirements Definition and Documentation • Definition of Interfaces • User-Machine Interface • Processing Requirements Definition and Documentation • Output Requirements Definition and Documentation • Controllability • Availability as Key Design Factor • IT Integrity Provisions in Application Program Software • Application Software Testing • User Reference and Support Materials • Re-Assessment of System Design		
Acquire and Maintain Technology Architecture • Assessment of New Hardware and Software • Preventative Maintenance for Hardware • System Software Security • System Software Installation • System Software Maintenance • System Software Change Controls		
Develop and Maintain IT Procedures • Future Operational Requirements and Service Levels • User Procedures Manual • Operations Manual • Training Materials		

Install and Accredit Systems • Training • Application Software Performance Sizing • Conversion • Testing of Changes • Parallel / Pilot Testing Criteria and Performance • Final Acceptance Test • Security Testing and Accreditation • Operational Test • Promotion to Production • Evaluation of Meeting User Requirements • Management's Post-Implementation Review		
Manage Changes • Change Request Initiation and Control • Impact Assessment • Control of Changes • Documentation and Procedures • Authorized Maintenance • Software Release Policy • Distribution of Software		

4.3 Delivery and Support

The Delivery and Support section includes the following topics:

1 Define Service Levels
2 Manage Third-Party Services
3 Manage Performance and Capacity
4 Ensure Continuous Service
5 Ensure Systems Security
6 Identify and Attribute Costs
7 Educate and Train Users
8 Assist and Advise IT Customers
9 Manage the Configuration
10 Manage Problems and Incidents
11 Manage Data
12 Manage Facilities
13 Manage Operations.

COBIT Topics	Documentation Required (Y/N)	Documentation Up-To-Date (Y/N)
Define Service Levels • Service Level Agreement Framework • Aspects of Service Level Agreements • Performance Procedures • Monitoring and Reporting • Review of Service Level Agreements and Contracts • Chargeable Items • Service Improvement Program		
Manage Third-Party Services • Supplier Interfaces • Owner Relationships • Third-Party Contracts • Third-Party Qualifications • Outsourcing Contracts		

• Continuity of Services • Security Relationships • Monitoring		
Manage Performance and Capacity • Availability and Performance Requirements • Availability Plan • Monitoring and Reporting • Modeling Tools • Proactive Performance Management • Workload Forecasting • Capacity Management of Resources • Resources Availability • Resources Schedule		
Ensure Continuous Service • IT Continuity Framework • IT Continuity Plan Strategy and Philosophy • IT Continuity Plan Contents • Minimizing IT Continuity Requirements • Maintaining the IT Continuity Plan • Testing the IT Continuity Plan • IT Continuity Plan Training • IT Continuity Plan Distribution • User Department Alternative Processing Back-up Procedures • Critical IT Resources • Back-up Site and Hardware • Wrap-up Procedures		
Ensure Systems Security • Manage Security Measures • Identification, Authentication, and Access • Security of Online Access to Data • User Account Management • Management Review of User Accounts • User Control of User Accounts • Security Surveillance • Data Classification • Central Identification and Access Rights Management		

• Violation and Security Activity Reports • Incident Handling • Re-Accreditation • Counterparty Trust • Transaction Authorization • Non-Repudiation • Trusted Path • Protection of Security Functions • Cryptographic Key Management • Malicious Software Prevention, Detection and Correction • Firewall Architectures and Connections with Public Networks • Protection of Electronic Value		
Identify and Attribute Costs • Chargeable Items • Costing Procedures • User Billing and Chargeback Procedures		
Educate and Train Users • Identification of Training Needs • Training Organization • Security Principles and Awareness Training		
Assist and Advise IT Customers • Help Desk • Registration of Customer Queries • Customer Query Escalation • Monitoring of Clearance • Trend Analysis and Reporting		
Manage the Configuration • Configuration Recording • Configuration Baseline • Status Accounting • Configuration Control • Unauthorized Software • Software Storage		
Manage Problems and Incidents • Problem Management System • Problem Escalation		

• Problem Tracking and Audit Trail		
Manage Data • Data Preparation Procedures • Source Document Authorization Procedures • Source Document Data Collection • Source Document Error Handling • Source Document Retention • Data Input Authorization Procedures • Accuracy, Completeness, and Authorization Checks • Data Input Error Handling • Data Processing Integrity • Data Processing Validation and Editing • Data Processing Error Handling • Output Handling and Retention • Output Distribution • Output Balancing and Reconciliation • Output Review and Error Handling • Security Provision for Output Reports • Protection of Sensitive Information during Transmission and Transport • Protection of Disposed Sensitive Information • Storage Management • Retention Periods and Storage Terms • Media Library Management System • Media Library Management Responsibilities • Back-up and Restoration • Back-up Jobs • Back-up Storage • Archiving • Protection of Sensitive Messages • Authentication and Integrity • Electronic Transaction Integrity • Continued Integrity of Stored Data		
Manage Facilities • Physical Security • Low Profile of the IT Site • Visitor Escort		

• Personnel Health and Safety • Protection against Environmental Factors • Uninterruptible Power Supply		
Manage Operations • Processing Operations Procedures and Instructions Manual • Startup Process and Other Operations Documentation • Job Scheduling • Departures from Standard Job Schedules • Processing Continuity • Operations Logs • Remote Operations		

4.4 Monitoring

The Monitoring section includes the following topics:

- Monitor the Processes
- Assess Internal Control Adequacy
- Obtain Independent Assurance
- Provide for Independent Audit.

COBIT Topics	Documentation Required (Y/N)	Documentation Up-To-Date (Y/N)
Monitor the Processes • Collecting Monitoring Data • Assessing Performance • Assessing Customer Satisfaction • Management Reporting		
Assess Internal Control Adequacy • Internal Control Monitoring • Timely Operation of Internal Controls • Internal Control Level Reporting • Operational Security and Internal Control Assurance		
Obtain Independent Assurance • Independent Security and Control Certification / Accreditation of IT Services • Independent Security and Control Certification / Accreditation of Third-Party Service Providers • Independent Effectiveness Evaluation of IT Services • Independent Effectiveness Evaluation of Third-Party Service Providers • Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments • Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third-Party Service Providers • Competence of Independent Assurance Function • Proactive Audit Involvement		

Provide for Independent Audit • Audit Charter • Independence • Professional Ethics and Standards • Competence • Planning • Performance of Audit Work • Reporting • Follow-up Activities		

5 Appendix