COBIT : Mission, Framework, Governance and Controls

Introduction

Information Technology Governance is the structure of relationships and processes within an enterprise which add value to a corporation's goals while balancing risk with return-on-investment.

The management of existing information technology and the implementation of new information technology resources require increased consideration for both **security** and **control** in the management of these resources.

COBIT is the product of the *Information Systems Audit and Control Association* which may be reached via their telephone at 847 253-1545 or their internet sites: www.ITgovernance.org and www.isaca.org .

CobIT is an acronym which stands for "**C**ontrol **Ob**jectives for **I**nformation and related **T**echnology"

COBIT Mission

To research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.

COBIT Governance Tools include:

Management Guidelines ... define critical success factors, goal indicators, and performance indicators which detail how different control activities support operation processes, information requirements and IT resources.

Framework ... explains how IT processes deliver the information that a business requires to meet its objectives. There are three key areas: first: 34 high-level control objectives which collate into four separate domains; second: 7 criteria for information that supports the business objective (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability); third: IT resources (people, applications, technology, facilities and data).

Control Objectives ... provide tools which integrate the 34 high-level control objectives with 318 specific/detailed control objectives for the development of clear policy, good practice/procedure and defined responsibility.

Implementation Tool Set ... facilitates the implementation of governance tools with case studies, lessons learned, and FAQ. Included is an implementation guide, management awareness section and diagnostic standards for IT control

Audit Guidelines ... provide an outline for audit control corresponding to 34 high-level control objectives integrated with 318 specific/detailed control objectives. Audit structure: analyze, assess, interpret, react and implement

COBIT is designed to make a clear and distinct link between information technology and business goals, via:

- classification of high-level control objectives for business domains
- definition of information requirements for each business domain
- list of IT resources impacted by information requirements

The COBIT framework identifies 34 high-level control objectives in four business domains. There are 318 detailed control objectives contained within this classification which address information requirements and resources.

- quality control components - address quality, cost and delivery
- fiduciary control components - address effectiveness, efficiency, reliability of information, compliance
- security control components - address confidentiality, integrity and availability

COBIT design is based on the perception that there are three levels of management for information technology resources .. domains, processes and activities/tasks - the intent is that the grouping of activities/tasks to processes and processes to domains has a logical organization which permits the clear definition of goals for tasks and measurable results which permit "life-cycle" management for information technology resources.

The four COBIT domains for Information Technology Management are:

- Planning and Organization : linkage of business strategy to IT strategy, strategic vision, etc.

- Acquisition and Implementation : change management is required to realize IT strategy

- Delivery and Support : service delivery, support mechanisms, security, education, etc.

- Monitoring : assessment of all infrastructure components over time

Controls should facilitate achievement of business objectives.

Excessive controls cost money while insufficient controls increase risk.

The goal of control theory is to identify and establish the correct balance for each system.

Controls can be classified by:

- nature
- functional area
- action or objective

Controls are classified by nature as:

- management controls
- physical controls
- technical controls

Controls are classified by functional area as:

- application controls
- network controls
- development controls
- operations controls
- security controls
- integrity controls

Controls are classified by action or objective as:

- directive controls : management actions, policies, guidelines that cause or encourage a desired event
- preventive controls : standards, methods, practices, tools, technology to ensure quality and reliability
- detective controls : give feedback regarding the effectiveness of directive and preventive controls
- corrective controls : provide information, procedures, instructions for correcting errors, omissions, etc. detected
- recovery controls : facilitate backup, restoration, recovery of a system following interruption of services

From the perspective of assessment/audit activity, control classification by action/objective is the most useful conceptualization and within that context: preventive, detective and corrective controls the most useful for analysis.

Model for Enterprise-based Internal Control

Internal control includes those mechanisms within an enterprise which have been designed to provide reasonable assurance regarding the achievement of objectives for:

- effective and efficient operations
- reliability of financial reporting
- compliance with applicable laws and regulations

Practically speaking, internal controls are usually effective by people and help the enterprise achieve its performance/profitability targets and prevent the loss of resources. Controls should help ensure reliable financial reporting and permit the corporation to comply with laws and regulations thus avoiding damage to its reputation and other consequences.

Internal controls in and of themselves cannot:

- ensure the corporation's success or survival
- ensure the reliability of financial reporting
- ensure compliance with laws and regulations

Internal controls, during an audit, should represent a defined series of actions built into the infrastructure of the business, which are included in the inherent management of business processes. No two corporations should have the same internal control systems. Variation occurs based on the industry segment, corporation size, work place culture and management philosophy. Internal control systems are not a panacea - internal control systems operate at different levels of the enterprise with respect to different objectives ... internal controls in and of themselves cannot provide reasonable assurance due to differences in judgment, breakdowns in controls, management overrides, collusion, and problems in cost/benefit measurement.

Internal control systems have 5 components

- Control Environment ..... human resource controls ... competence levels and cost ... etc.

- Risk Assessment ..... objective setting & risk assessment integrated throughout operations

- Control Activities ..... policies and procedures which define business processes

- Information/Communication ... internal and external information and reporting ... financial ... customers ... etc.

- Monitoring ..... look for emphasis of "building in" rather than "adding on" of controls

Controls for Information Technology

Preventive Controls

- policies, procedures, standards
- mission/vision statements
- TQM programs
- short-range planning
- long-range planning
- portfolio management approach to computer investments
- establishment of benchmarks and best practice standards
- establishment of self-management teams
- establishment of electronic commerce guidelines

Detective Controls

- project management tools
- control parameter definitions
- review of operating and capital budgets
- establishment of tolerance limits
- establishment of sampling techniques

Corrective Controls

- exception reports
- progress reports
- control reports

- error reports
- statistical reports
- special reports

Controls for the Planning, Organization and Management of Information Systems

Preventive Controls

- mission/vision statement
- TQM program
- integrate business strategic planning with IS strategic planning
- establish IS steering committee
- install CIO position
- establish benchmark studies
- implement charge back system
- conduct software license audits and enforce software license requirements
- establish service level agreements
- issue acquisition policies and procedures
- establish data classification scheme and ownership rules
- issue job descriptions
- develop system access rules
- establish software QA function
- establish separation of duties
- establish and enforce policies, procedures and standards
- practice portfolio management approaches to IS investments
- issue internet use policy

Detective Controls

- perform security monitoring
- conduct security audits
- issue security checklists for self-assessment by management
- use automated tools for security function
- conduct penetration testing
- review system logs
- establish configuration management
- perform account reconciliation
- require employees to take vacations
- rotate key employees

Corrective Controls

- issue statistical reports

- issue exception reports
- develop security violation reports
- issue data file maintenance reports
- issue computer security incidence reports

Controls for Hardware and Software Platforms

Preventive Controls

- issue preventive maintenance guidelines for host computers and PCs
- establish a problem, change and configuration management function
- install and empower help-desk staff to support system users
- implement privacy and electronic mail policy
- conduct benchmark studies
- establish a PC or microcomputer support function
- issue and enforce policies, procedures, and standards
- issue service level reporting
- require documentation for end-user developed and maintained systems
- install computer capacity management function

Detective Controls

- protect configuration parameters
- require system logging of transactions
- require periodic audits of computer centre
- acquire system diagnostic tools
- implement hardware and software monitors
- test end-user developed software
- practice "desk check reviews" and peer reviews for end user developed systems

Corrective Controls

- review activity logs
- update change documentation
- ensure running of correct version of production programs

Controls for Networks and Telecommunications

Preventive Controls

- issue and enforce policies, procedures and standards
- use encryption and digital signature techniques
- comply with trans-border data transmission laws

- implement training and education plans
- establish problem and change management system
- implement fault-tolerance network design practices
- implement resilient network design principles: redundancy, alternate paths, parallel processing, etc.
- develop contingency plans
- implement network management tools
- install quality cables for LAN network
- use call-back system for dial-up telephones/modems
- implement smart tokens, password generators, etc.
- establish a separate and centralized network control function

Detective Controls

- test contingency plans
- require network line utilization statistics
- implement network diagnostic tools
- provide network testing capabilities
- test cables and connectors prior to power-up for each node
- conduct periodic inventory of network equipment
- install physical security devices
- implement logical security mechanisms
- implement message sequence numbers
- use checksum techniques
- install computer virus detection tools
- log identification and authentication mechanisms
- log changes to access control information
- use hardware and software inventory tracking system

Corrective Controls

- update contingency plans
- acquire network diagnostic data collection tools with automatic corrective action
- provide network routing capability
- implement network monitoring tools
- establish recovery mechanisms such as checkpoints, roll-back and roll-forward features in the database
- establish recovery techniques from computer viruses

Controls for Operations Management

Preventive Controls

- establish and enforce computer centre policies, procedures and standards
- establish a problem, change and configuration management structure
- install and empower help-desk staff to support system users
- require periodic audits of the computer centre
- install automated job scheduling system
- discourage printing of hardcopy reports and encourage on-line viewing
- install automate tape and disk management systems
- develop partnership relationships with customers and suppliers
- install program library management software

Detective Controls

- require system logging of transactions
- reduce computer operator intervention by installing automated console management system
- review system activity logs, journals and exception reports
- rotate key employees in the computer center
- acquire or develop automated job accounting information system
- require employees to take vacations
- ensure running of correct version of production programs
- implement run-to-run program controls
- compare production resource usage statistics
- install hardware and software monitors

Corrective Controls

- automate report balancing procedures
- use comments in job execution language
- provide periodic backup of data and programs, and rotate them through off-site storage
- facilitate system recovery and restart procedures
- install automated job recovery software
- develop fall-back systems and procedures
- install fault-tolerant hardware and software for recovery from a system failure

Controls for the Protection of Information Assets

Preventive Controls

- implement advanced identification and authentication techniques using smart/memory tokens, biometrics and one-time passwords
- use encryption and digital signature techniques
- install anti-virus software

- implement reference monitor concept
- establish security tags (labels) for sensitive information
- use traffic padding or flooding techniques to confuse intruders
- install secure gateways and firewalls for internet security
- protect modems and terminal servers
- implement least privilege concept
- implement cryptographic techniques
- implement strong password management
- implement logical and physical access controls
- assign asset responsibility to employees and exact accountability from them
- distribute job descriptions with security responsibility
- generate a security awareness among employees
- encourage legal ownership of software and protection of copyrighted (intellectual) property
- provide guidelines to protect confidentiality of data and information with data ownership/custody
- establish a quality control technique for computer security function
- require periodic security audits
- issue guidelines for software development and maintenance methodology focusing on computer security design

Detective Controls

- require all employees to wear badges for checking by security guards
- provide last activity/sign-on data on computer terminals
- inform the user of any unauthorized attempts to guess his password
- install continuous area surveillance mechanisms
- review system activity logs, journals, and exception reports to detect security violations
- conduct periodic security audits
- require that employees take vacations and rotate employees
- insert dummy names and known addresses as decoys into financially related mailing lists to detect their unauthorized use
- provide dummy data files for intruders to trap which reviewing the data
- control program changes to ensure that only authorized changes are made
- implement variance detection techniques
- install audit trails
- implement checksum programs to detect changes
- install intrusion detection tools
- use real-time user verification
- install video cameras in the data centre
- install software configuration controls
- implement incident logging and reporting
- install smoke and fire detectors and a fire alarm system
- conduct "tiger team" reviews to detect security flaws and vulnerabilities
- implement cyclic redundancy check algorithm for error detection

Correction Controls

- provide checkpoints in application systems for production jobs with long run-times (> 30 minutes)
- develop fall-back systems and procedures
- establish system recovery / restart guidelines in applications and systems software
- implement vital records retention programs
- use disk repair utility programs for PCs
- install fault-tolerant hardware and software
- display system warning messages
- issue computer security incident reports

Controls for Business Continuity and Disaster Recovery

Preventive Controls

- conduct risk analysis
- establish a planning committee
- prioritize application systems
- revisit the data storage and retention practices
- install electronic vaulting
- purge data and program files periodically
- issue guidelines on how to discard/dispose of used paper records, mechanical records and electronic records
- develop disaster-awareness among employees
- establish system recovery/restart guidelines in applications and systems software

Detective Controls

- establish recovery organization with clearly defined responsibilities
- establish recovery logging procedures
- conduct disaster recovery training
- conduct recovery testing
- conduct periodic fire drills
- maintain a problem log during plan testing

Corrective Controls

- provide periodic backup of data and programs and rotate through off-site storage
- test the disaster recovery plan

- install automated job recovery software
- test the emergency procedures
- obtain sufficient insurance coverage
- implement vital records retention programs
- develop fall-back systems and procedures
- update the panning document
- issue a report of lessons learned from testing

Controls for IT Development, Acquisition, Implementation and Maintenance

Preventive Controls

- establish a software development management (steering) committee
- establish a software quality assurance function
- issue software development methodology guidelines
- establish a data administration and database administration function
- encourage auditor and management participation and reviews
- require active user participation and receive sign-off letters
- issue guidelines for systems usability, maintainability, audit-ability, controllability and secure-ability criteria
- implement good project management tools and techniques to track project status and progress
- use structured techniques for analysis, design, programming and testing
- inspect and test software independently
- perform cost/benefit analysis similar to a portfolio approach to investments
- develop applications using "open systems" architecture to provide seamless integration of systems
- install data-editing and validation routines
- separate test, quality and production libraries
- install logical access control software
- install program library management software
- install problem/change management software
- use incremental approach instead of grand design approach to develop applications
- plan for continuous testing of software during its development and maintenance

Detective Controls

- practice peer reviews
- use program tracing tools and techniques
- practice structured walk-through events
- use automated documentation aids

- practice software verification and validation techniques
- use software debugging tools during testing
- design data editing and validation control routines into the software
- inspect and test software independently
- conduct code and file comparisons
- install management oversight reviews
- implement formal technical reviews
- conduct through testing of software
- practice be-bugging (error seeding) techniques to detect errors in software

Corrective Controls

- design automated error correction features into applications software
- produce before-and-after image reports for correcting errors during date file maintenance activities
- design audit trail reports, control reports, aging reports and exception reports for user and auditor review
- use pre-processors to make programs more readable
- use interactive program debugging tools
- use comments in computer programs and job execution language
- design checkpoint and recovery/restart procedures into software
- require statistical and exception reports
- arrange for fall-back provisions to handle system problems and crashes

Controls for Business Process Evaluation and Application Systems

Preventive Controls

- electronic commerce guidelines
- data dictionary
- structured techniques
- programming and documentation standards
- processing parameters
- on-line prompting
- self-help features
- default options
- good screen design
- field highlighting
- screen diagnostic messages
- pre-numbered forms
- systems assigned numbers
- pre-coded forms and screens
- turnaround documents

- data ownership / classification
- table lookups
- passwords
- transaction cancellation
- management approvals
- concurrent access controls
- two-person controls
- system or manual over-rides
- validity checks
- fail safe and fail soft systems
- TQM programs
- benchmarks and best practices
- risk assessment guidelines

Detective Controls

- batch control totals
- hash totals
- limit checks
- reasonableness checks
- check digits
- overflow checks
- format checks
- date checks
- label checks
- completeness tests
- range tests
- record counts
- sign tests
- size tests
- sequence checks (cumulative)
- duplicate checks
- cross-field checking
- cross-record checking
- system matching
- field combination tests
- validity checks
- run-to-run totals
- suspense files
- header/trailer record verifications
- balance controls
- system logs
- comparison controls
- computation controls
- ratio tests
- rounding techniques
- descriptive read-back
- structured walk-through
- data checks

- key verification
- one-for-one checking
- cross-footing

Corrective Controls

- program comments
- job control comments
- automatic error correction
- over-ride by supervisors
- audit trail reports
- control reports
- exception reports
- productivity reports
- aging reports
- error reports
- before/after image reporting
- clear and complete error messages
- error totals
- documentation
- automated back-up and recovery mechanisms
- journaling
- data retention
- checkpoint controls
- transaction back-out
- recovery logging
- fall-back procedures
- end-of-job markers
- end-of-report markers