Internal Control Act and Information Technology

Since the inception of New York State's Internal Control Act (formal name Government Accountability, Audit and Internal Control Act), each state agency has been required to review its major programs and administrative functions on a periodic basis, to arrive at a ***"reasonable assurance"*** that such programs or functions were operating efficiently and effectively, with sufficient controls in place to protect assets, ensure compliance with applicable laws, rules or regulations, and to produce financial/ management reports in an accurate/timely and relevant manner.

The Office of the State Comptroller and the Division of the Budget are the two control agencies most involved in oversight of the Internal Control Act – OSC by audits of state operations, DOB by an annual reporting and certification process.

For many years, the Information Systems Audit and Control Association (ISACA) has been promoting COBIT – Control Objectives for Information Technology as a more structured and detailed audit tool. COBIT takes into consideration those issues most relevant to the information technology environment, including:

- Computer Systems Security
- Data Integrity and Reliability
- Cost-Effectiveness of Data Processing Operations
- Timeliness/Relevance/Availability of Information to serve management and program needs
- Increasing Dependence on IT for program and management
- Increasing Vulnerability to organized and individual attacks on computing systems.

Like COSO's Control Self-Assessment and OCFS's Internal Control Review process, COBIT's – Control Objectives are goal-oriented. "The policies, procedures, practices and organizational structures are designed to provide *'reasonable assurance'* that business objectives will be achieved and that undesired events will be precented or detected and corrected."

As might be expected, COBIT depends on:

- Systemization
- Documentation
- Standards & Defined Expectations
- Measurement
- Appropriate Risk Assessment

A full-fledged COBIT review of OCFS IT operations would be beneficial, but would also be very costly and time-consuming. Following the principle of "walk before you run", it is suggested that your agency develop a modified COBIT approach, incorporating some of the basic elements of COSO Control Self-Assessment and Division of the Budget guidance on the Internal Control Act. The survey instrument for OCFS IT operations will need be more detailed than that instrument used for other agency operations, but far less complex than the COBIT instrument.

As Division of the Budget has instructed, it all starts with the **plan of organization** of the agency or operation. Accountability depends on human beings in place, planning, implementing and monitoring program performance. First step in the IT Internal Control Review will be a description of the staffing, consultants/ contractors and system (hardware/software) resources. This will also entail a description of the division of labor and responsibilities of the major bureaus within your agency, and cost estimates of the annual expenditures in each category, plus an estimate of the cumulative assets (e.g. file servers, network/transmission lines, desktop computers, etc.). The old adage "If you can't measure it, you can't manage it." holds true.

COBIT audits look (at varying levels of detail) at 34 items, detailed below. All such issues need to be examined on a global IT basis, but some of these issues may only affect one or two bureaus within IT. They include the following **Control Objectives**:

PLANNING AND ORGANIZATION		
PO-1	Define a strategic IT Plan	Long and short-range plans relevant to agency mission and information needs
PO-2	Define the information architecture	e.g. data dictionary & classification framework; security levels
PO-3	Determine technological direction	Monitor future trends; plan future acquisitions
PO-4	Define organization and relationships	Ownership of system; segregation of duties
PO-5	Manage the investment	Annual operating budget; cost-benefit analysis
PO-6	Communicate management aims & direction	Including security awareness, commitment to quality, management responsibilities
PO-7	Manage human resources	Employees and SUNY contractors; recruitment, retention, cross-training, succession planning
PO-8	Ensure compliance with external requirements	e.g. Social Service Law & Family Court confidentiality requirements; site safety, ergonomics
PO-9	Assess risk	Define acceptable level of risk
PO-10	Manage projects	Request/approval process; phased-in implementation; testing and training; link to strategic plan
PO-11	Manage quality	Quality assurance, coordination and communication; adherence to IT standards & procedures

ACQUISITION AND IMPLEMENTATION		
AI-1	Identify automated solutions	Define information requirements; third-party services; procurement control; acquisition and acceptance
AI-2	Acquire & maintain application software	e.g. CITRIX Solutions, Cognos; design approval and documentation; liabilities of proprietary software; availability and integrity ofdata
AI-3	Acquire & maintain technology architecture	e.g. Windows 2000 Server; assess new hardware/software; system security software; software maintenance; preventative maintenance
AI-4	Develop & maintain procedures	Operations manual, user guides, training materials
AI-5	Install & accredit system	Training, system and data conversion, testing and final acceptance and production
AI-6	Manage changes	Change request process; software release policy; distribution of software; system compatibility

DELIVERY AND SUPPORT		
DS-1	Define service levels	Define service level agreements; monitoring and reporting
DS-2	Manage third party services	Telecommunications providers; contractor reliability/qualifications; security relationship
DS-3	Manage performance & capacity	Availability and performance requirements; workload forecasting; performance measurement; resources
DS-4	Ensure continuous service	Continuity plan, critical resources, training; back-up and off-site
DS-5	Ensure system security	Hardware & software protection; management review of user accounts, security surveillance; authentication; encryption, firewall,
DS-6	Identify & allocate costs	e.g. state vs. county, shared services; chargeable items; billing/chargeback procedures
DS-7	Educate & train users	Training organization; security awareness, training needs
DS-8	Assist & advise customers	e.g. ENTERPRISE help desk, customer query escalation (job ticket), clearances of queries

DS-9	Manage the configuration	Configuration baseline, unauthorized software, software accountability
DS-10	Manage problems & incidents	Disaster & security response teams; problem management and escalation; tracking and audit trail
DS-11	Manage data	Backup, backup, backup; data entry error handling; source document retention; authorization procedures; output distribution and retention; protection of sensitive information; authentication, media library
DS-12	Manage facilities	Physical security, visitor escort, uninterruptible power supply; environmental protections; employee health and safety; low profile of IT site
DS-13	Manage operations	24/7 operation; procedures and operations manuals; job scheduling, operations logs; remote operations;

MONITORING		
M-1	Monitor the process	Collect and assess information; user satisfaction; assess performance
M-2	Assess internal control adequacy	Timely operation of internal controls; operational security and quality assurance
M-3	Obtain independent assurance	Accreditation of IT services; proactive audit involvement; independent evaluation of effectiveness; compliance with applicable laws/rules/regulations
M-4	Provide for independent audit	Professional ethics and standards; audit charter, independence

Yes, this is a very demanding, comprehensive list. It also requires:

- Identification of the primary party responsible for each of these IT Control Objectives
- IT resources applicable
    - People
    - Applications
    - Technology
    - Facilities
    - Data
- Information criteria applicable
    - Effectiveness & Efficiency
    - Confidentiality
    - Integrity
    - Availability
    - Compliance
    - Reliability

It is interesting to note that the fourth "domain" of COBIT objectives – **Monitoring** is very similar to COSO Control Self-Assessment and OCFS Internal Control Review. ISACA has provided a 155 page document detailing these 34 COBIT objectives, but a review of the table above is informative enough for our purposes.

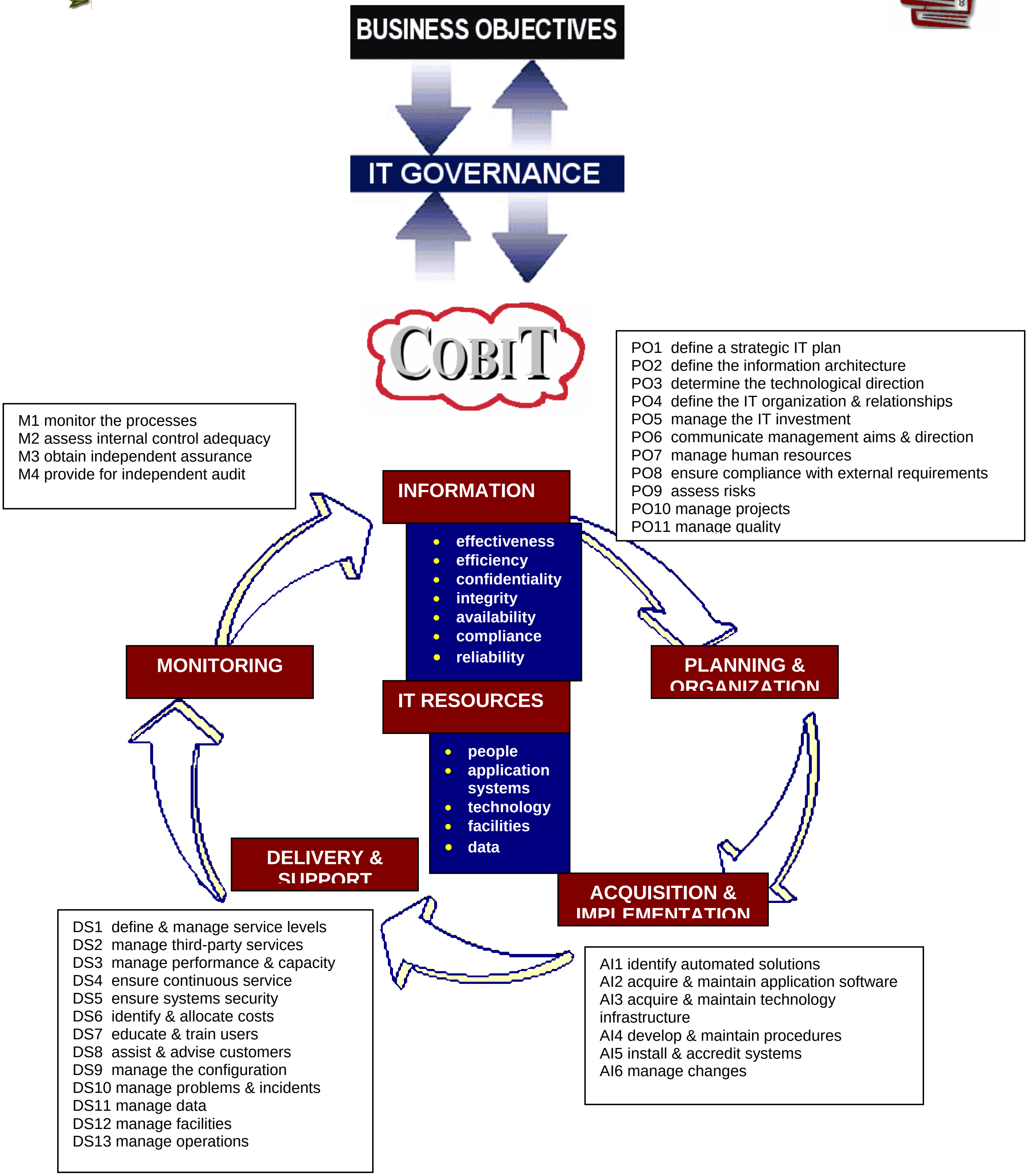
A full-fledge COBIT review would entail considerable training of both auditor and auditee. A more workable alternative is for the internal control officer to initiate a series of management consultations with IT executives and managers, following the general framework of a COBIT audit, though taking into account the incremental nature of such a review, since we are starting from the ground up.

It is also important for IT staff to take ownership of the need for such a review. As agencies become increasingly reliant on information technology there is a greater need for self-reliance in the development, maintenance and improvement of all its information systems. Where necessary, there will also need to be mutual agreement between the internal control officer and IT regarding terminology used, and degree of detail required to fulfill annual reporting/certification requirements of the Internal Control Act.

Past experience with internal control review processes in most agencies indicates that the internal control review process is of greater value to those in charge or a program or function, when they fully embrace such process, and document systems to a level of detail in excess of minimum Internal Control Act requirements.

However, the current fiscal/staffing climate may interfere with such eventuality (at least on a short-term basis).

The following chart from the COBIT manual bears an uncanny resemblance to Canada’s own internal control approach (CICA, vs. COSO), indicating it is a constant renewal process, as we learn by doing.



BUSINESS OBJECTIVES

IT GOVERNANCE

COBIT

PO1 define a strategic IT plan
PO2 define the information architecture
PO3 determine the technological direction
PO4 define the IT organization & relationships
PO5 manage the IT investment
PO6 communicate management aims & direction
PO7 manage human resources
PO8 ensure compliance with external requirements
PO9 assess risks
PO10 manage projects
PO11 manage quality

M1 monitor the processes
M2 assess internal control adequacy
M3 obtain independent assurance
M4 provide for independent audit

INFORMATION

- effectiveness
- efficiency
- confidentiality
- integrity
- availability
- compliance
- reliability

MONITORING

PLANNING & ORGANIZATION

IT RESOURCES

- people
- application systems
- technology
- facilities
- data

DELIVERY & SUPPORT

ACQUISITION & IMPLEMENTATION

DS1 define & manage service levels
DS2 manage third-party services
DS3 manage performance & capacity
DS4 ensure continuous service
DS5 ensure systems security
DS6 identify & allocate costs
DS7 educate & train users
DS8 assist & advise customers
DS9 manage the configuration
DS10 manage problems & incidents
DS11 manage data
DS12 manage facilities
DS13 manage operations

AI1 identify automated solutions
AI2 acquire & maintain application software
AI3 acquire & maintain technology infrastructure
AI4 develop & maintain procedures
AI5 install & accredit systems
AI6 manage changes