December 1999

# Adoption and Usage Patterns of an IT Audit and Control Framework,

Jane Fedorowicz
*Bentley College*

Ulric Gelinas
*Bentley College*

# Adoption and Usage Patterns of an IT Audit and Control Framework

Jane Fedorowicz, Ph.D., Bentley College, jfedorowicz@ bentley.edu

Ulric J. Gelinas, Jr., Ph.D., Bentley College, ugelinas@ bentley.edu

## Introduction

In 1996, the Information Systems Audit and Control Foundation (ISACF) published *Control Objectives for Information and Related Technology* (*COBIT*)[i]. COBIT provides a framework of generally applicable and accepted IT security and control practices[ii] that can be used to evaluate an organization's current and planned IT environment. The COBIT framework is intended to be useful to management and users (business process owners), in addition to auditors. For management, users, and auditors COBIT provides a framework to evaluate IT investments and risks and to provide assurance that IT-related business objectives are achieved. COBIT strengthens the understanding, design, exercise and evaluation of internal controls. It also helps to focus management's responsibilities to ensure that systems have integrity and that appropriate controls are in effect. COBIT outlines internal or external audit's responsibility to provide assurance with respect to those objectives.

As of August 1997 over 5,000 copies of COBIT had been sold and many organizations had begun to adopt it. In August of 1997 a survey was sent to COBIT purchasers to determine their characteristics and how they intended to use COBIT. For those who had gone forward and had begun to use COBIT, the survey was intended to determine if their actions were consistent with their intentions. The survey also captures the characteristics of those who had not adopted COBIT and their reasons for not adopting it. This article reports initial results of that survey.

## Survey Administration

A draft of the instrument was administered to 20 students in a graduate financial auditing course and the course instructor, a professional auditor. A pilot test was then administered to five IT auditors. The authors obtained similar feedback from the COBIT Steering Committee. The Information Systems Audit and Control Association provided financial support for survey administration. The survey was mailed to 5,315 individuals who had purchased COBIT. Responses were received from 439 individuals of which 429 were deemed usable (an 8.1% response rate).

## Purchase Patterns

Initial analysis of the ISACA survey of COBIT purchasers provides an in-depth look into the purchase and adoption patterns of the COBIT framework. This analysis was performed about one year after COBIT was first published. Surveys were first analyzed to identify expectations of COBIT purchasers. Results were then examined to distinguish adopters of COBIT from non-adopters.

Initial questions on the survey were formulated to gain an understanding of why respondents purchased COBIT and how they planned to use it. As a comprehensive framework for IT control, individuals would be expected to purchase COBIT primarily for guidance on IT control and secondarily for assistance in developing audit programs. Table 1 indicates the reasons selected most frequently by all respondents in support of their initial purchase decision and shows that reasons for purchasing COBIT were not always consist with the COBIT developers' expectations.

| Statement | % of Respondents |
|---|---|
| To improve our audit approach/programs | 68.3 |
| To improve the IS/IT controls in our company/organization | 48.3 |
| We viewed COBIT as a valuable benchmark for IS/IT control | 46.0 |
| COBIT provides detailed audit guidelines | 41.0 |

Table 1: Reasons for COBIT Purchase

## User Perceptions

Respondents were categorized as "users" or "non-users" based on self report. Two hundred and fifty-five respondents (59%) responded as users. Demographically, Chi-square testing shows that the distribution of users is statistically similar to the population of respondent

purchasers. Users and non-users of the framework possess many similar demographic characteristics, although users are more likely to hold a CISA certification, and report larger internal and IT audit staffs at the adopting location.

Several questions were asked to assess respondents' perceptions about several general and company-specific risk and control issues. As expected, users perceive risk analysis to be critical to an organization's success. They are also more likely than non-users to feel that internal control is an important issue for management. Users do not view internal control as an impediment to getting things done in an organization. In general, then, users have a more positive attitude toward risk and control than non-users.

User perceptions toward audit and control in their own organization are also more positive than non-COBIT adopters. COBIT users believe their IS/IT audit reports address the organization's objectives more than do non-users. They also see their IS/IT audit reports as more useful, timely, accurate and complete than their non-adopting counterparts. There is more frequent collaboration between IS/IT auditors and their clients on security, audit and control issues at users' sites.

User organizations are highly diversified and house complex IT functions, which may provide the impetus for implementing a formalized control framework. Users believe that their organization's IT operations are better controlled than other organizations in the same industry. They are more likely than non-users to agree that COBIT is the best published set of control guidelines for IT, which verifies one of the top reasons COBIT has been adopted by this group.

In summary, users tend to hail from larger, more diversified organizations with complex, well controlled IT organizations. They believe in the importance of internal control and risk assessment. They perceive their organizations' audit reports in a positive light.

## Usage Patterns

Almost four out of five adopters noted that COBIT was being used with little or no modification in their organization. Very few found it necessary to make extensive changes to the framework. This suggests that the COBIT framework is meeting the expectations of its drafters and adopters.

There were statistically significant differences noted between users and non-users in reasons for purchasing COBIT. Table 2 indicates those differences. In all cases, users had a higher response rate for each reason than did non-users, which translates into higher expectations on these dimensions on the part of those who use COBIT than those who do not.

| Statement | % of Users | % of Non Users |
|---|---|---|
| To improve our audit approach/programs | 77.3 | 55.2 |
| To improve the IS/IT controls in our company/organization | 53.3 | 40.8 |
| We viewed COBIT as a valuable benchmark for IS/IT control | 50.6 | 38.5 |
| COBIT is an update of ISACA's Control Objectives which we already use | 44.3 | 24.1 |
| To incorporate the COBIT control philosophy within our organization | 43.9 | 21.8 |
| To standardize our audit approach/programs | 41.6 | 26.4 |
| COBIT is an integrated framework | 37.3 | 25.9 |
| We thought that COBIT would facilitate communication among ***(check all that apply):*** | 36.0 | 19.0 |
| • Senior management and IS/IT | 14.9 | 8.6 |
| • IS/IT management and audit | 33.7 | 18.4 |
| It fit with our existing IS/IT control philosophy | 16.1 | 6.3 |

Table 2: Reasons Reported for Purchasing COBIT

Users were asked to select all of the ways that they were using COBIT. Table 3 indicates those uses chosen most frequently:

| Statement | % of Users |
|---|---|
| For audit planning and audit program development | 80.8 |
| To evaluate our IT risks | 51.2 |
| To validate our current IT controls | 44.6 |
| To validate our IT control objectives | 44.6 |

Table 3: Reported Uses of COBIT

As with the planned uses of COBIT, audit program development received the highest percentage of responses. Uses such as communication among key organization players and assessment of business risks did not appear to be as important to COBIT users. So, while the COBIT developers had intended COBIT to be useful to management and business process owners and as a vehicle for IT governance, the survey results do not indicate that users perceived communications improvement as a primary driver of COBIT adoption. Rather, purchases, users and non-users alike, perceive COBIT as more as an audit tool and less as an IT governance and control framework.

Non-users were then asked to indicate the reasons why they were not using COBIT. Table 4 depicts those reasons chosen most frequently.

| Statement | % of Non-users |
|---|---|
| Current workload is taking priority | 51.7 |
| We haven't had time to read it | 29.8 |
| We will go forward in the next 12 months | 25.3 |

Table 4: Reasons for Not Adopting COBIT

None of the top-cited reasons concerned content or technical problems with the framework. Indeed, COBIT adopters report that a successful COBIT implementation requires a substantial time commitment [per author interviews with adopters]. The responses of the non-users would seem to support that conclusion.

## Future Research

COBIT was purchased primarily to improve audit approaches and programs, and secondarily to improve IS/IT controls. Use of the framework is consistent with these planned reasons. However, framework designers anticipated that COBIT would enable increased communication among management, business process owners, and auditors, which was not well documented by the survey results. COBIT information and materials are not being shared with others as expected.

Continuing analysis of the data will permit further description of the use of COBIT, and increase our understanding of perceptions concerning the benefits, costs and enabling organizational characteristics of successful COBIT use. A follow-on study addressing differences between auditor and non-auditor adoption patterns is also in progress.

Finally, additional research needs to be conducted to determine how a framework such as COBIT comes to be perceived as "generally accepted." Such research would help developers of such frameworks, as well as adopters of the frameworks, to position the framework for optimal adoption and effectiveness.

---

[i] (*COBIT*) *Control Objectives for Information and Related Technology,* 2nd ed., Rolling Meadows, IL: Information Systems Audit and Control Foundation, 1998.

[ii] COBIT's control objectives were derived from a review of the following reference materials: COSO, OECD Guidelines, DTI Code of Practice for Information Security Management, ISO 9000-3, NIST Security Handbook, ITIL IT Management Practices, IBAG Framework, NSW Premiers Office Statements of Best Practices and Planning Information Management and Techniques, Memorandum Dutch Central Bank , EDPAF Monograph #7, EDI: An Audit Approach, PCIE (President's Council on Integrity and Efficiency) Model Framework, Japan Information Systems Auditing Standards, CONTROL OBJECTIVES Controls in an Information Systems Environment: Control Guidelines and Audit Procedures, CISA Job Analysis, CICA Computer Control Guidelines, IFAC International Guidelines for managing Security of Information and Communications, IFAC International Guidelines on Information Technology Management -- Managing Information Technology Planning for Business Impact, Standards for Internal Control in the U.S. Federal Government, Guide for Auditing for Controls and Security- A Systems Development Life Cycle Approach, Government Auditing Standards, Denmark Generally Accepted IT Management Practices, SPICE, DRI International Professional Practices for Business Continuity Planners, IIA, SAC Systems Auditability and Control, IIA Professional Practices Pamphlet 97-1 on Electronic Commerce, E & Y Technical Reference Series, C & L Audit Guide SAP R/3, ISO JEC JTC1/SC27 Information Technology -- Security, ISO IEC JTC1/SC27 Software Engineering, ISO TC68/SC2/WG4, Information Security Guidelines for Banking and Related Financial Services, CCEB 96/011, Common Criteria for Information Technology Security Evaluation, Recommended Practices for EDI, TickIT, ESF Baseline Control -- Communications, ESF Baseline Control -- Microcomputers, and the Computerized Information Systems (CIS) Audit Manual.