

Implementing COBIT in Higher Education: Practices That Work Best

By Claude L. Council, Ph.D., CISM

To successfully implement an IT governance program, it is important to understand management needs. This article describes a study exploring the management aspects of implementing *Control Objectives for Information and related Technology*[®] (COBIT[®]) at South Louisiana Community College (SLCC) in Lafayette, Louisiana, USA.¹ The study was conducted using COBIT[®] 3rd Edition. Throughout the study, the investigator observed the implementation of COBIT's fifth delivery and support process (DS5) pertaining to network security. This exploration examined professional and personal needs. The investigator's objective was to answer the following research questions:

1. What managerial issues arose that affected the deployment of each of COBIT's DS5 critical success factors (CSFs) at SLCC?
2. Did SLCC's executives and leaders commit to each of COBIT's DS5 CSFs?
3. Did SLCC's faculty and staff comply with each of COBIT's DS5 CSFs?
4. What were the needs of each of the functional managers at SLCC?
5. How did these needs hinder the deployment of DS5?

Methods

To answer these questions, the investigator used COBIT's diagnostic tools to evaluate SLCC in its management of network security. COBIT's CSFs, key goal indicators (KGIs) and key performance indicators (KPIs) were used to evaluate risks, and the COBIT maturity model was used to evaluate the development and execution of the policies, procedures and controls. The leadership team members were interviewed to gain insight into their opinions of the CSFs. All of this information was provided to the chancellor at SLCC, and decisions were made on how to deploy the DS5 CSFs. The results of these decisions were used to customize the proposed security plan at SLCC.

Throughout the study, data were collected and recorded into a database. The data were then linked by the investigator to the relevant research questions. Each record in the database, sentence in the interview transcripts and item in the diagnostic worksheets were evaluated against each research question. Some items pertained to more than one research question while some did not pertain to any. The preliminary CSF deployment plan was compared to the final deployment plan to identify differences. Once this was complete, the investigator used explanation building to describe each of the items and answer the research questions.

Findings Based on the Research Questions

Overall, based on the results of this research, SLCC demonstrated that medium-sized institutions of higher learning can benefit from the implementation of an IT governance security program. In addition, the implementation of COBIT at SLCC provided answers to the research questions comprising the focus of this article. In this section, the investigator describes the information as it applies to each of the research questions.

Research Question 1: What managerial issues arose that affected the deployment of each of COBIT's DS5 CSFs at SLCC?

Several management issues, positive and negative, arose during the planning and deployment of COBIT DS5. The positive issues either enhanced the support of the CSF or facilitated enhancements to the original plan, and the negative issues resulted in the dilution of the CSFs. The dilution of the CSFs was not necessarily negative; had the dialog not occurred before the deployment, these changes would not have occurred and a loss of support would have resulted. The seven positive issues that surfaced are listed in **figure 1** with the number of CSF from which they emerged. The eight negative issues that surfaced are listed in **figure 2**.

Figure 1—Positive Management Issues

Issues	Description	Frequency
Introduction of guidelines	The provisioning of guidelines to all functional managers, providing them with guidance for directing network security efforts in their respective departments	1
Alignment	Aligning the goals of the IT department with the goals of the other functional areas within the organization	1
Leadership awareness	Communicating security concerns to the leadership of the organization	4
Employee awareness	Communicating security concerns to the employees	2
Confidentiality of sensitive data	Ensuring that the data owned by each of the functional areas remain confidential	3
Data protection	Protecting the integrity of the data owned by each of the functional areas	1
Downtime	The availability of applications for all end users	1

Figure 2—Negative Management Issues

Issues	Description	Frequency
Concerns about rigidity	Concerns that the policies are too rigid, becoming a hindrance	1
Workload of the IT staff	Concerns that the IT staff members are too busy to handle problems in the functional areas and complete the project	7
Compliance	Concerns that the institution is in compliance with all applicable regulations and laws	1
Heavy cabinet agenda	Concerns that the agenda for the cabinet meetings is too booked to add items	1
Leadership time	Concerns that the leaders of the college are too busy to devote adequate time to an issue	7
Employee time away from post	Concerns that training will take employees away from their posts for too much time to fulfill their responsibilities	3
Funding	Concerns that adequate funding is not available	2
Usability	Concerns that systems are intuitive and able to be operated by the end users	1

One management issue that surfaced related to the entire COBIT implementation was leadership time. One participant, who is traditionally a big supporter of IT, was actually replaced for the second interview because of time constraints. In addition, four of the first interviews were delayed by the participant. Interestingly, there were no postponements during the second interview.

Research Question 2: Did SLCC’s executives and leaders commit to each of COBIT’s DS5 CSFs?

For the purposes of this study, commitment was established by a leader’s willingness to assist with the deployment of COBIT. The data were gathered during the second interview. Overall, the leaders were willing to commit to the program, but many were not sure how they could help. There were 70 opportunities to demonstrate commitment by offering assistance (seven participants multiplied by 10 CSFs). Of these opportunities, 61 percent (43) were taken. All participants demonstrated commitment in more than one opportunity.

The type of commitment the leadership at SLCC demonstrated was arbitrarily broken down into 10 categories. These are listed in **figure 3** with the number of times the type of commitment was offered.

The negative management issues were not a lack of willingness to commit. There was no dialog prior to the study describing how they could demonstrate commitment. The reasons for not committing were that they were not sure how (17 instances), the CSF was already in place (four instances) and the support was out of their control (one instance).

The dynamics of a community college prompted an interesting comment from one of the participants that demonstrates the willingness of employees to commit to an IT governance initiative. During the second interview one of the participants said, “I would support a plan and that may help, but it may also backfire. At a large retail chain, executive

Figure 3—Leadership Commitment Categories

Commitment	Description	Frequency
Promote executive support	Helping to sell a security program and its components to senior management	3
Ensure compliance	Helping to ensure that employees are following policies and procedures	6
Attend training	Taking the time to attend training	3
Direct the execution of the CSF	Taking ownership over the deployment of a CSF	8
Perform a task or tasks	Performing individual project tasks	8
Attend meetings	Taking the time to attend security meetings	1
Provide information to auditors	Speaking with internal and external auditors during IT audits	1
Review deliverables	Reviewing deliverables from the deployment of a security program, providing input and staying aware	1
Promote to employees	Helping to market the security program to employees	8
Support funding	Providing support during budget meetings for funding for network security projects	4

support is helpful, but in an education institution things are different. These things should be supported at several layers of management, not just the top.” This and all of the reasons for commitment and lack of commitment must be candidly discussed with the leadership team at the beginning of an initiative so that it is provided with an understanding of just how important its role is in the process.

Research Question 3: Did SLCC’s faculty and staff comply with each of COBIT’s DS5 CSFs?

A good measure of a program and its executive support is the faculty and staff’s compliance with the program. During the deployment of the CSFs, all events, comments and circumstances indicating faculty and staff compliance were recorded. Since compliance issues are predicted to surface well beyond the end of this study, SLCC’s strategies to ensure compliance were documented.

SLCC used several strategies to ensure compliance. A further developed list of these strategies will undoubtedly contribute to a healthy dialog prior to an IT governance project. **Figure 4** contains a list of six strategies used by SLCC during the deployment of DS5 and the number of times they were used.

SLCC also encountered some compliance issues. Recognition of these issues prior to an IT governance initiative provides leadership with the opportunity to plan. It also facilitates a constructive dialog that allows the organization to confront these issues with a problem-solving mindset. The four compliance issues encountered at SLCC are listed in **figure 5** with the number of times they surfaced.

Figure 4—Strategies to Ensure Compliance

Compliance Strategies	Description	Frequency
Inclusion in unit planning process	Including security tasks such as training, policy review and risk assessment projects in the unit planning process so that functional managers are held accountable for completing these projects during the annual institutional effectiveness review	2
Policy creation	Creating and communicating policies to document expectations	3
Procedure creation	Creating and communicating procedures to provide guidance for following the policies	1
Combining events	Combining events to reduce time commitments, thus increasing support	2
Making compliance easier	Evaluating controls and making compliance as easy as possible for the users	2
Using technology	Using security tools to force compliance (e.g., a program that blocks instant messaging programs)	1

Figure 5—Compliance Issues

Compliance Issues	Description	Frequency
No control	A manager felt that he/she did not have the authority to make an impact.	4
Inappropriate responsibility assignments	A manager is held accountable for a task in a security project that he/she does not have the authority to complete.	1
Lack of consistency	A control is not applied consistently, causing a perception of favoritism and confusing the users.	1
Lack of communication	An individual felt that he/she was being singled out because a new security control was not communicated to the entire staff prior to implementation.	1

Research Question 4: What were the needs of each of the functional managers at SLCC?

To answer this question completely, the investigator was required to extend the leaders’ individual needs beyond the business requirements listed in the COBIT management guidelines.² More specifically, although the individual managers’ needs overlapped, to some degree, with the quality, fiduciary and security requirements, this inquiry explored needs at a more personal level. Rather than focusing on fulfilling business requirements, the goal was to uncover needs that can be used to enhance the support of an IT governance program from the individual leaders.

Therefore, when promoting an IT governance program, it is important to know and understand the needs of the individual functional managers. In this section, the investigator describes the needs of the functional managers within the context of each COBIT DS5 CSF. The study database was reviewed for clues about the needs of the functional managers, and these needs were arbitrarily grouped into 23 categories.

Figure 6 summarizes the 23 categories of needs. The first column contains a name for the need. The second column contains the number of times the need was identified during the study. The third column provides a definition of each of the categories.

Figure 6—DS5 Management Needs Summary

Management Needs	Frequency	Explanation
Accessibility	1	Relates to the ability of the staff members to access accurate data when they need them
Accountability	2	Ensures that the various tasks are defined and assigned to an individual who has the ability, authority and responsibility for completing them
Availability of IT	6	Ensures that the IT function is available to fulfill its service level agreement and provide services that are satisfactory to the organization
Communication	1	Provides a dialog among members of the organization to enhance their ability to successfully fulfill their mission
Compliance	4	Ensures that all governmental, accreditation and organizational rules are being followed
Confidentiality	19	Ensures that sensitive data are protected from unauthorized access
Control	1	Empowers the functional managers to fulfill their mission free of obstacles created by constraints, such as controls that are too stringent, overly aggressive centralization or misplaced responsibilities
Convenience	2	Allows all employees to perform their job functions free from frustration and poor human factors
Cost containment	4	Allows the organization to function within budget constraints
Direction for functional managers	2	Provides information that the managers need to adequately direct their staff and make informed decisions
Employee awareness	8	Empowers employees to follow guidelines and improves their morale because they understand the reasoning behind controls
Employee morale	3	Creates a more pleasant work environment, improves productivity and enhances cooperation with administration
Flexibility	1	Eliminates constraints that would prevent the organization from making decisions and performing actions that fulfill the mission of the organization
Image	1	When managed properly, allows the organization and individuals to present a positive image internally and to the public
IT alignment	1	Ensures that the IT department is managed in a way that enhances the mission of the entire college
IT department effectiveness	1	Ensures that IT resources are being used responsibly and are available to fulfill the needs of the users

Figure 6—DS5 Management Needs Summary, *cont.*

Management Needs	Frequency	Explanation
Leadership awareness	12	Provides information that the functional managers need to make good decisions and empowers them to promote good practices to their employees.
Management improvements	1	Management improvements ensure that continual quality improvements occur, increasing the efficiency and effectiveness of the functional areas
Productivity	1	Ensures that the functional managers are getting the most from their employees
Risk mitigation	2	Provides controls to lower the risk to a level that is acceptable to the organization
Second	1	Provide assurance that opinions all facets of a study have been reviewed and that information provided to management is not tainted with bias
Time	23	Increases the ability of the functional managers to fulfill their obligations to the institution
Uptime	5	Ensures that the information technology is available when needed, allowing all users to enjoy the intended benefits

Research Question 5: How did these needs hinder the deployment of DS5?

A review of the study database and interview transcripts revealed many needs of functional managers at SLCC, including those summarized in **figure 6**. Some of these needs contributed to the support of the COBIT initiative, some hindered the initiative, and others both supported and hindered the initiative.

Awareness of needs that may hinder a project is important because a checklist can be created by the champion to address them at the beginning of deployment. Awareness of these needs empowers the champion to identify opportunities for compromise, enhancing the overall support of the project. **Figure 7** lists needs with the potential to hinder the COBIT effort from a review of the study database.

Figure 7—Hindering Needs

Hindering Need	Frequency
Availability of IT	6
Convenience	2
Cost containment	4
Employee morale	3
Flexibility	1
Image	1
Productivity	1
Time	23

The availability of the IT staff to resolve problems and complete projects was a large concern at SLCC. The leadership at SLCC referenced concerns that some of the COBIT CSFs encumber the IT staff, preventing them from fulfilling their most basic functions. This was mentioned six times during the interviews. One participant articulated this

concern by saying, “When I need to register a student or complete a report, and if I am having problems getting on the network, I need help right then.”

Another concern stated twice was convenience. Indeed, security controls such as difficult and expiring passwords do decrease the convenience of authentication. In both statements, the leaders provided personal accounts of how these controls had inconvenienced them. Both accounts involved difficulty with remembering expiring passwords. These were recorded in the transcripts of the interviews and in the study database.

Cost containment was stated four times. Community colleges are provided with a finite budget, and these funds must be prioritized. This underscores the importance of presenting the administration with the risks quantified in potential losses so that they can make informed decisions about what expenditures are appropriate.

The leaders at SLCC stated the need for high employee morale three times. As the leaders manage their staff, unhappy employees create problems for them and are less productive. In all three references to employee morale, the participants were concerned about complaints from the staff. User awareness is one strategy for overcoming this issue.

Productivity was also described as a need by one of the participants. The aforementioned budget constraints result in reduced manpower, causing functional managers to focus on getting the most out of the people they have. When controls decrease the productivity of one’s staff, the leaders are often required to cover the unfinished tasks on their own time.

A need for flexibility was expressed by one of the participants, who said, “Plans can lead to rigidity and we can quickly outgrow the plan.” Policies and procedures that are too rigid can prevent leaders from being able to adapt to changes in their environment and lead to resentment.

Image was a need expressed by another participant within the context of third-party reviews. No organization likes to disclose its weaknesses to individuals on the outside. One strategy for addressing this might be to include a confidentiality clause in contracts with third-party reviewers.

The need expressed most frequently was time. The participants described a need for time 23 times during the interviews. Indeed, a need for time had the most potential to hinder the project at SLCC. As leaders fill several roles within the organization, time is their most valuable asset. It is imperative that an IT governance champion describe what they get in return for their time as early as possible in the project.

Summary

In this article, the investigator described the implementation of COBIT at SLCC, a medium-sized institution of higher learning, and answered the research questions pertaining to the management aspects of deploying an IT governance program. Throughout the study, the managerial issues that affect the deployment of each of COBIT’s DS5 CSFs at SLCC were documented. SLCC’s executives’ and leaders’ commitment and compliance to each of COBIT’s DS5 CSFs and needs were also recorded. Finally, the details of how these needs hindered the deployment of DS5 were explored.

References

- IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003
- IT Governance Institute, *COBIT 3rd Edition Audit Guidelines*, USA, 2000
- IT Governance Institute, *COBIT 3rd Edition Control Objectives*, USA, 2000
- IT Governance Institute, *COBIT 3rd Edition Executive Summary*, USA, 2000
- IT Governance Institute, *COBIT 3rd Edition Implementation Tool Set*, USA, 2000

Endnotes

- ¹ Council, C.; *An Investigation of a COBIT Systems Security IT Governance Initiative in Higher Education*, Doctoral Dissertation, Nova Southeastern University Graduate School of Computer and Information Sciences, 2006 (UMI Dissertation Information Service no. 3206177)
- ² IT Governance Institute, *COBIT 3rd Edition Management Guidelines*, Rolling Meadows, IL, USA, 2000

Claude L. Council, Ph.D., CISM

works in assurance at Target Corporation. Prior to joining Target, Council was the director of information technology at South Louisiana Community College, where this study was completed.