*ISSUES IN ACCOUNTING EDUCATION*
Vol. 24, No. 1
February 2009
pp. 63–76

# Assessing Information Technology General Control Risk: An Instructional Case

**Carolyn Strand Norman, Mark D. Payne, and Valaria P. Vendrzyk**

**ABSTRACT:** Information Technology General Controls (ITGCs), a fundamental category of internal controls, provide an overall foundation for reliance on any information produced by a system. Since the relation between ITGCs and the information produced by an organization's various application programs is indirect, understanding how ITGCs interact and affect an auditor's risk assessment is often challenging for students. This case helps students assess overall ITGC risk within an organization's information systems. Students identify specific strengths and weaknesses within five ITGC areas, provide a risk assessment for each area, and then evaluate an organization's overall level of ITGC risk within the context of an integrated audit.

**Keywords:** internal controls; general control; ITGC; risk assessment.

## INTRODUCTION

The Sarbanes-Oxley Act (SOX 2002) and the Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 5 (PCAOB 2007) require that the organization's chief executive officer (CEO) and chief financial officer (CFO) include an assessment of the operating effectiveness of their internal control structure over financial reporting when issuing the annual report. External auditors must review management's internal control assessment as part of an annual integrated audit of an organization's internal controls over financial reporting. In short, accountants—external auditors, internal auditors, and management accountants at all levels—are actively involved in helping their respective organizations comply with SOX-related internal control requirements.

Because of the pervasiveness of IT in organizations, the information systems themselves contain many internal controls. As a result, both internal and external auditors must develop an understanding of the IT environment and its related processes and controls, including the IT general controls (ITGCs), by performing risk assessment procedures. Although deficiencies in ITGCs do not *directly* result in misstated financial statements or material

*Carolyn Strand Norman is an Associate Professor at Virginia Commonwealth University, Mark D. Payne is an Executive Director at Ernst & Young, and Valaria P. Vendrzyk is an Associate Professor at the University of Richmond.*

The authors thank Nancy Bagranoff, Faye Borthick, Jason Emmons, Tony Hubbard, Tanya Lee, John McLain, Richard Newmark, Brad Tuttle, Ralph Viator, Marcia Weidenmier-Watson, Chris Wolfe, participants at the 2007 American Accounting Association Annual Meeting, and our anonymous reviewers for their helpful suggestions on earlier versions of this case. We gratefully acknowledge William Sanders, Information Systems Department, Virginia Tech, for the matrix prioritization materials.

control weaknesses, they can *indirectly* cause or contribute to application control deficiencies (Center for Public Company Audit Firms 2004). Since the relation between ITGCs and the information produced by an organization's various application programs is indirect, understanding how ITGCs interact and affect an auditor's risk assessment is often challenging for students. Accordingly, our case offers accounting faculty an assignment or project that is a ''real world,'' comprehensive supplement to textbook materials on the topic of risk and ITGCs.

## THE CASE

Several months ago, you started working at a large public accounting firm as an IT staff auditor. You are currently working on your first assignment, an ITGC review of the Foods Fantastic Company (FFC). FFC is a publicly traded, regional grocery store chain, headquartered in Mason, Maryland, and includes 50 stores located in the mid-Atlantic area. The centralized data center is in Mason. FFC relies on an integrated suite of application programs that include state-of-the-art software to manage merchandise replenishment, store-level sales forecasting, and point-of-sale data. For example, FFC relies on bar code scanners and credit/debit card readers. To maintain its competitive edge in its market area, FFC recently implemented a fingerprint bio-coding payment system in all of its stores. This new systems implementation required that FFC change several of its general-ledger application programs; in particular, those related to its cash receipts processing. FFC does not use any outside service organizations to provide its IT services.

Sophie Ewing, the audit senior who heads up your team, decided that because of FFC's complex and sophisticated IT processing, an IT General Control (ITGC) review is mandatory to meet SAS 109's risk assessment procedures and SOX Section 404 *Management Assessment of Internal Controls* requirements. You know that an ITGC review is very important because ITGCs provide the foundation for reliance on any financial information FCC's systems produce. Your evaluation will affect the financial auditor in assessing the risk of material misstatement in FFC's financials, and consequently, the audit plan. At your first team meeting, Sophie announced that your firm's network security specialists would review the technical issues related to FFC's internal controls. They will evaluate FFC's operating systems, its telecommunications software, and its network configuration and firewalls.

In preparation for the meeting, Sophie encouraged you to review the key provisions included in SAS 109, SOX Section 404, applicable sections of PCAOB Auditing Standard No. 5, and your firm's internal guidance, which groups ITGCs into the following five areas: IT management, systems development, data security, change management, and business continuity planning (BCP).

### IT Management

IT management's key concepts include IT's position within the organization, whether IT goals are aligned with the organization's strategic goals, the use of an IT steering committee, and whether the IT department's structure promotes proper segregation of duties to protect the organization's assets. Your primary concerns are:

- Does FFC have an IT strategic plan?
- To whom does the Chief Information Officer (CIO) report?
- What key responsibility areas report to the CIO?
- Does FFC have an IT steering committee? Is so, who are the members?

**Systems Development**

The key concepts within systems development include the existence of a new systems implementation methodology, project management, pre- and post-implementation reviews, quality control, adequate testing, and demonstrated compliance with the selected implementation methodology. Based on this understanding, your team's primary concerns are:

- Does FFC design, develop, and implement systems in a logical fashion?
- Does the organization consider internal controls as an integral part of systems design or does it retrofit them after implementation?
- To what extent is FFC's Internal Audit department involved in systems development activities? Is it part of the project review team? Is it a voting member of the team?
- In particular, how well did FFC manage the development and implementation of its new fingerprint bio-coding payment system?

**Data Security**

The critical concepts within data security include adherence to an established information security policy, access approval on a need-to-know basis, periodic rotation or change of access controls, monitoring, exception reporting, and incident response. Data security has both physical and logical aspects. On the physical side, data security includes physical access and environmental controls over the data center computer room. On the logical side, data security includes policies related to password configuration, change, and history restrictions. Logical security also includes prompt review, modification, or removal of access due to personnel transfers, promotions, and terminations. Your team's primary concerns are:

- How well does FFC control physical access to its data center computer room?
- Is FFC's computer room adequately protected against environmental dangers, such as fire?
- Does FFC control logical access to its information systems? In particular, how does it control the logical access of terminated or transferred employees?
- Does FFC have a current IT security policy?
- Does FFC produce access violation reports?
- Do FFC IT personnel adhere to IT policy and follow IT procedures? For example, do appropriate personnel review any access violation reports and take the prescribed action?

**Change Management**

Change Management's key concepts include documented change procedures, user authorization and approval, separation of duties in implementing changes, management review, quality control, and adequate testing. Your audit team's primary concerns are:

- Does FFC have (and follow) formal change management procedures?
- In particular, did FFC follow these procedures when making any necessary changes to its current application programs because of the new bio-coding payment system? For example: Were the changes approved? Did the programmers adequately test the changes before putting them into production? Did the application programmer(s) that made the code changes, test the changes, and/or put them into production?

**Business Continuity Planning**

Key concepts of BCP are management's expectations regarding a timely recovery of processing capabilities, the existence of a written plan, the currency of the plan, offsite

storage of both the plan and data files, and testing of the plan. Your audit team's main concerns are:

- Does FFC have a written BCP plan? Is it current?
- When is the last time FFC tested its plan?
- Does FFC back up its software and data? How often? Where do they store the backups?
- Did FFC need to recover its systems using its backups during the past fiscal year?

**Information Collected During the ITGC Review**

Under Sophie Ewing's direction, you and other members of the audit team worked very diligently reviewing FFC's policies and procedures, interviewing FFC client personnel, and observing FFC's various operations and procedures related to its ITGCs. First, your team created an organization chart to document the FFC's management structure (see Exhibit 1).

Exhibit 2 reflects the information your team collected from interviews, observations, and reviews of corroborating documentation related to FFC's ITGCs.

**EXHIBIT 1**
**Foods Fantastic Company Organization Chart**

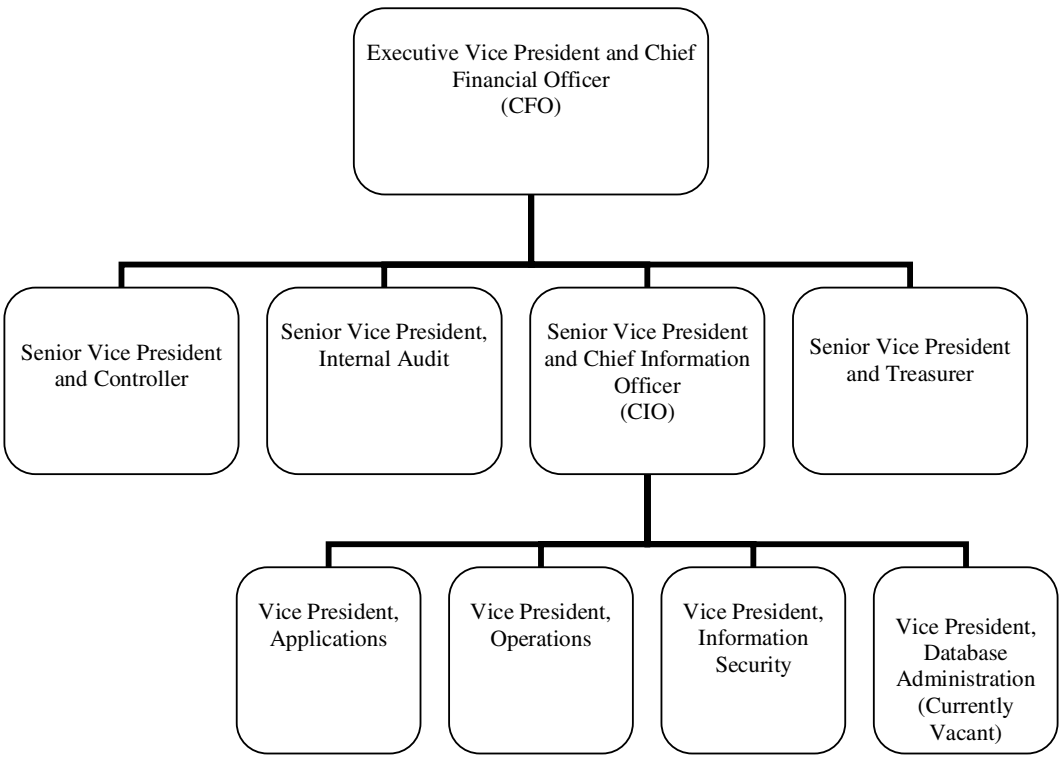

**EXHIBIT 2**
**Foods Fantastic Company**
**IT General Control (ITGC) Review Notes**

**Notes from meetings with the Chief Financial Officer (CFO):**

- Foods Fantastic Company (FFC) implemented a new bio-coding payment system in all of its stores this past fiscal year.
- FFC's IT Executive Steering Committee develops IT policies and reviews the overall operations of the IT department. The voting members of the committee are:

  1. the Senior Vice President (SrVP) and Chief Information Officer (CIO)
  2. the VP, Applications
  3. the VP, Data Base Administration (DBA)
  4. the VP, Operations
  5. the VP, Information Security (IS)
  6. the Executive Vice President and Chief Financial Officer (CFO)
  7. the SrVP, Internal Audit

- The IT Executive Steering Committee revised FFC's security policy in 2005. The policy addresses all organizational security issues including IT.
- FFC has no documented business continuity or disaster recovery plan. Management believes such a plan is cost-prohibitive for an organization of its size and FFC has never experienced any major business disruption. In case of disaster, the data center manager would retrieve the most recent backup tapes that are stored offsite. FFC would use these files to recover its systems.

**Notes from meetings with the SrVP, Internal Audit:**

- FFC's Internal Audit Department is involved as a voting member of the project teams responsible for design, development, and implementation of new projects. Internal audit performs post-implementation reviews on all projects over $2 million.
- The new bio-coding payment system was 25 percent over its initial time budget and 40 percent over its initial dollar budget.

**Notes from meetings with the CIO:**

- The VP, Applications is currently responsible for the DBA function. However, the CIO reviews the logs that show the actions of the Application VP's user ID.
- FFC has an IT strategic plan, which is consistent with its corporate strategic plan. The IT strategic plan outlines the objectives and strategies that the information systems group will implement to assist FFC in meeting its overall business objectives.
- FFC adopted Structured Systems Analysis and Design Methodology (SSADM), an industry-recognized standard for systems development and project management. All projects (buy or build) follow the applicable SSADM phases. The CIO periodically reviews each project's required budget-to-actual reconciliation.
- FFC's security policy states that the VP, IS is to conduct a user audit on a quarterly basis. The appropriate department manager reviews electronically submitted reports that list each user's profile, note changes on the reports, and return the reports to the VP, IS. The VP then makes the appropriate modifications based on the returned reports. The VP maintains the reports, and initials and dates the report after completing all modifications.

**Notes from meetings with the VP, Human Resources:**

- FFC is currently interviewing individuals to assume the DBA's responsibilities and hopes to hire someone within the next six to eight months.
- Aside from the security policy, management does not provide any formalized security awareness programs related to data security.
- Each month, the Human Resources department forwards a *Transfers and Terminations* report to the VP, IS.

(*continued on next page*)

**EXHIBIT 2 (continued)**

**Notes from meetings with the VP, Applications:**

- The VP, Applications assigns a project manager and develops an initial time and dollar budget for each new development project.
- IT personnel adequately tested the new bio-coding payment system prior to its implementation. This testing included integration testing, stress testing, and user acceptance testing. User departments corroborated their testing and acceptance of the new system.
- Application programmers do not have access to the computer room unless escorted by data center personnel (e.g., an operator).
- FFC instituted formal procedures for change management. The VP, Applications is responsible for change management and maintains all documentation in a fireproof vault in his office. A Change Request form initiates all application software changes, including required software upgrades. A user completes the form, which the user's department manager approves. The user forwards the request form to the VP, Applications, who logs each request in a Change Request Log. The VP performs an initial analysis and feasibility study and estimates the required development hours. The Change Request log is a listing of all requested changes and the status of the change request. The VP, Applications uses this log to track open items and follow up on changes not completed within the original time estimate.
- The VP, Applications assigns the change request to an applications programmer and issues the current system's documention to the programmer. The applications programmer copies the source code from the system's production region to its development region and makes the change. The programmer works in the systems development region using test data. The programmer tests the change first within the affected module and then within the entire application. Changes are never tested against production data. The programmer updates the necessary system's documentation.
- The applications programmer migrates the code to the system's test region. A second programmer performs systems integration testing, volume testing, and user acceptance testing, again using test files. The second programmer then performs a quality review of the change, including a source-compare analysis, and reviews the updated systems documentation.
- Upon completion of testing, the user who requested the change and the appropriate department manager review the test results and accept the change by signing the original request form. The VP, Applications reviews the user-approved request form on which the department manager has indicated that s/he is satisfied that the program is ready for implementation. The VP, Applications also reviews the documentation prior to implementing any new or changed program to ensure that the documentation is adequate.
- The VP, Applications approves the change, initials the change request form, and transfers the change to the VP, Operations, who officially accepts the change. The VP, Applications then updates the Change Request log and returns the revised systems documentation to the fireproof vault.

**Notes from meetings with the VP, Operations:**

- FFC's computer room, within its data center, is locked at all times. All outside contractors or visitors must first contact the data center manager for entry into the computer room. Each must bring an official picture ID, sign a visitors' log, and be escorted at all times by data center personnel during the visit.
- In 2002, FFC installed video cameras on all doors entering the computer room to record activity 24/7. Building management staff, who report to the facilities manager, are responsible for maintaining these tapes. The VP, Operations has not needed to review these tapes for at least six months since no unathorized access attempts have been reported.
- Environmental controls are in place in the computer room (i.e., temperature controls, uninterrupted power supply, a backup generator, fire-extinguishing equipment, and raised floor). Appropriate maintenance staff test these controls semi-annually.
- FFC backs up all of its data each day. It stores its most recent daily backup once a week at a company-owned offsite location, along with the most recent version of its software. FFC did not test backup tapes during the past year and has no plan to test these tapes in the future.
- The VP, Operations assigns IT operations personnel the task of placing new or changed applications programs into production after the VP, Applications has approved the work.

(*continued on next page*)

**EXHIBIT 2 (continued)**

**Notes from meetings with the VP, Information Security:**

- The VP, IS grants keycard access to the computer room. The VP, IS receives a keycard access report for the computer room on a monthly basis. The VP, IS determines if an unauthorized access attempt into the computer room has occurred.
- Passwords are not displayed on terminals or reports. Password standards are enforced by security software. FFC requires a minimum password length of six alphanumeric or special characters and a maximum length of nine alphanumeric or special characters. The software prevents the same character from being used more than once in a password and prevents numbers from being used next to each other in a password. The security software forces users to change their passwords twice each year. The security software maintains a history of two previous passwords and does not permit employees to reuse their two most recent passwords. The security software does not display statistics regarding employees' sign-on information. For example, there is no information regarding a user's sign-on attempts (such as date and time of last sign-on), number of invalid sign-on attempts since last successful sign-on, or number of days prior to password expiration.
- The system allows three access attempts. If the third attempt is unsuccessful, the user ID is automatically disabled. The user must contact the VP, IS to reset the user ID. The system generates a logical access violation report on a daily basis.
- User access is limited to workstations within the corresponding responsibility area. For example, users with access to the Accounts Payable module can only log in from workstations located in the Accounts Payable area. A workstation can stand idle for up to 60 minutes before the user is logged off.
- The VP, IS is responsible for maintaining user profiles and authorization lists.
- The VP grants access to the system to new hires. The appropriate department manager completes a computerized form that specifies the proper level of access. The VP reviews the request form for proper approvals and then either approves or denies the request. If approved, the VP issues the necessary ID and initial password with the requested access via encrypted email.
- Normal users may have multiple IDs. Each user ID can log on to one sign-on session at a time. The VP, IS, who has unlimited access, can log in from any workstation and have multiple sign-on sessions.
- The VP, IS is responsible for modifying and/or disabling user IDs for personnel whose job duties change because of promotions, transfers, and/or terminations based on the *Transfers and Terminations* report. The VP, IS maintains the report, and initials and dates the report when the VP, IS has made all of the modifications.

**Notes from meeting with the facilities manager, who reports to the VP, Human Resources:**

- According to the facilities manager, no one asked to view the computer room video tapes during the past six months.

**Observations of the audit team:**

- Documentation of the systems development process for the new bio-coding payment system confirms that the VP, Applications complied with SSADM requirements when implementing this new system.
- The data center is on the first floor of FFC's building. The data center manager reports to the VP, Operations.
- Company policy requires the VP, IS to review the keycard access report at least once per quarter. During the past six months, the VP has not reviewed the report for any unauthorized access attempts.
- The team observed no instances in which application programmers were in the computer room without a proper escort.
- The team observed no instances in which visitors or outside contractors were in the computer room without a proper escort.

(*continued on next page*)

**EXHIBIT 2 (continued)**

- Documentation of the computer room environment controls test results for the last 18 months shows no irregularities. These files are in the CIO's office.
- If someone attempts to enter the computer room without authorization, company policy requires that the VP, Operations review the video tapes from the computer room cameras within 24 hours.
- The FFC security policy requires each employee to sign an acknowledgment that s/he read the current policy. A review of the personnel files of a sample of employees found no exceptions.
- A review of the selected user profiles and passwords revealed the following:

| User | Password |
|---|---|
| Vice President, Applications | 7LiAcOf# |
| Vice President, Information Systems | QSECOFR1 |

Note: The acronym QSECOFR looks familiar. Remember to review *A Beginner's Guide to Auditing the AS/400 Operating System* (Bines 2002).

- During the past six months, the dates of the modifications were about three weeks after the VP, IS received the HR's *Transfers and Terminations* report.
- The VP, IS performed the most recent user audit eight months ago.
- Company policy requires the VP, IS to review the unauthorized system access report on a monthly basis to check for unusual activity (e.g., multiple violations, changes to the authorization lists, etc.). During the past six months, the VP, IS has not reviewed the report for any unauthorized access attempts.
- The audit team verified that FFC followed its approved change management procedures when making the bio-code payment-related changes to its cash receipts processing and other financial reporting application programs.
- In the past fiscal year, no incidents occurred that required FFC to recover its systems using its backup tapes.

## Case Requirements

Sophie Ewing assigned your team the following tasks:

1. For each ITGC area, identify the control issues and classify them as strengths or weaknesses, using Exhibit 3 to document your work. Exhibit 3 will be part of the audit team's work papers.
2. Determine the level of risk (High, Medium, or Low) that you believe is present in each particular ITGC area.
3. Assess the overall risk of the organization's ITGCs, taking into consideration the five separate risk assessments that you just made (task #2 above), and their relative importance to internal controls over FFC's financial reporting.
4. Prepare a report that documents and appropriately supports your overall IT risk assessment (task #3), using the guidance Sophie provided in Exhibit 4. You must include a statement explicitly stating your overall risk assessment in the report's concluding section and attach your completed ITGCs matrix.

**EXHIBIT 3**
**Foods Fantastic Company IT General Controls Matrix**

**Part A: Strengths and Weaknesses**

| ITGC Area | Summary of Issue | Strength or Weakness |
|---|---|---|
| IT Management | FFC has an IT strategic plan | Strength |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

**Part B: Risk Assessment for each ITGC area (Indicate Low, Medium or High)**

| ITGC Area | Risk Assessment |
|---|---|
| IT Management | |
| Systems Development | |
| Data Security | |
| Change Management | |
| Business Continuity Planning | |

**EXHIBIT 4**
**Report Guidance**

IT General Controls Risk Assessment Report
Foods Fantastic Company
Student's Name
Date

**Background:** Write a short description of Foods Fantastic Company (FFC) and why the ITGC review is necessary (2–3 sentences).

**Purpose:** Briefly describe the purpose of an ITGC review and why it is important (2–3 sentences).

**Scope:** Provide a short description of the work your team performed at Foods Fantastic to develop your risk assessment (3–4 sentences).

**Findings:** Elaborate on the key finding(s) that influenced your overall risk assessment. Discuss the key control strengths and weaknesses you identified within each of the five ITGC areas and its corresponding risk assessment. Provide enough detail to support your assessment. Include specific examples from the information your team collected (interviews, observations, and reviews of corroborating documentation). Your arguments need to be consistent with your risk assessment for the five different areas, as well as your overall risk assessment (4–5 paragraphs).

**Conclusion:** Provide a statement of your overall risk assessment. For example, I set FFC's assessed level of ITGC risk as _____ (*Low, Medium, or High)* because of _____. Summarize the primary reasons that contributed to your assessment. Keep in mind the relative importance of each of the five ITGC areas in controlling FFC's financial reporting (3–4 sentences).

## REFERENCES

Bines, J. 2002. A beginner's guide to auditing the AS/400 operating system. *Information Systems Control Journal*, Volume 2. Available at: http://www.isaca.org.

Center for Public Company Audit Firms. 2004. *A Framework for Evaluating Control Exceptions and Deficiencies*, Version No. 3. Available at: http://cpcaf.aicpa.org.

Public Company Accounting Oversight Board (PCAOB). 2007. *An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*. Auditing Standard No. 5. Washington, D.C.: PCAOB.

U.S. House of Representatives. 2002. The Sarbanes-Oxley Act of 2002. Public Law 107-204 [H. R. 3763]. Washington, D.C.: Government Printing Office. See also: http://www.sarbanes-oxley.com.