Information Technology General Controls Audit - Foods Fantastic Company

CIS 401 - Section #32303

Group 104

Siddhant Chaurasia - ASURITE #: 1214887791

Varun Shourie - ASURITE #: 1214512793

Omar Tamimu - ASURITE #: 1212442047

Exhibit 4

IT General Controls Risk Assessment Report
Foods Fantastic Company
Dated April 14, 2020

Background and Purpose

Foods Fantastic Company (FFC) is a regional grocery store chain with 50 stores in the mid-Atlantic area. Owing to its integrated suites of application programs like merchandise replenishment and sales forecasting, FFC faces massive complexities in IT operations. With the recent implementation of its bio-coding payment system, an IT General Control review is prudent for long-term success.

Scope

To complete this audit, we performed a series of high-level tasks. Firstly, we conceptualized the organization's structure. Next, we interviewed all of the managers pertinent to IT about the organization's policies. Finally, we directed our audit team to inspect company activities/documentation for vulnerabilities. We cross-referenced our findings with best practices to complete an overall risk assessment.

Findings

IT Management: Medium Risk
FFC's organizational structure deviates from research-proven best practices. For example, the CFO leading the company departs from the norm of a CEO with more technical/operational knowledge. Also, the VP, IS reports to the CIO, another structural issue which likely leads to security garnering less importance in the organization. The VP, Applications assuming the role of the VP, Database Administration, and the VP, HR's relative inaction in hiring a new VP leaves a void in the segregation of duties. FFC's IT Steering Committee is a positive, but the steering committee is not involved in systems development, acquisition, and delivery, a significant weakness.

Systems Development: Medium Risk
Strengths of systems development include how FFC adopted and follows the Structured Systems Analysis and Design Methodology and has internal audit perform post-implementation reviews in projects. Areas for improvement include how instead of the VP of Applications/CIO overseeing project management, budgeting, time, and other specifics, the Steering Committee as a whole should be involved in systems development issues.

Data Security: High Risk
Initially alarming is how FFC has failed to update its security policy since 2010. Despite FFC limiting physical access to the computer room with escorts, no accountability exists for reviewing security tapes

when unauthorized access occurs. Similarly, the VP, IS fails to conduct the necessary audit procedures for keycard access, logical access and maintains the list of user authorization lists (which should be assigned to security administrators to maintain segregation of duties). The password policy uses only a single type of preventive control in the form of password authentication, lacking the much secure multi-factor or multimodal authentication to access information systems. Moreover, the password lacks a sufficient length, with the security software used for passwords not leaving behind an audit trail of statistics about users. Though user workstations are limited by role-based access and location, the VP, IS's negligent authorization to use any terminal with multiple log-ins, and users having multiple IDs opens up vulnerabilities.

Change Management: Low Risk

FFC wholly followed a formal change management procedure with its bio-coding payment system incorporating systems documentation, changelogs, and approvals from the end-user. All documentation is stored in the VP, Applications' fireproof vault. Sufficient testing/quality control occurs with two programmers in a development environment utilizing test data. Segregation of duties exists with how IT operations implement changes after the final approval of the VP of Operations and the end-users. Areas for improvement include instituting a Change Advisory Board & including contingencies for conversion controls, emergency changes, and monitoring user rights/privileges.

Business Continuity Planning: High Risk

Owing to the lack of a Business Continuity Plan, FFC is uncertain of its disaster recovery capabilities. Since backups aren't tested, the organization may not know if tapes stop functioning. Lastly, tapes being sent off-site only once a week signifies a Recovery Point Objective of up to one week in the worst-case disaster.

Conclusion

We set FFC's level of ITGC risk as **high** as FFC fails to enforce comprehensive data security controls such as internal auditing policies and confidentiality controls with passwords. Such actions place FFC in danger of not falling in compliance with Sarbanes Oxley and other financial reporting requirements. Furthermore, the lack of a BCP handicaps FFC's disaster recovery. The deficiencies in IT Management, Systems Development, and Change Management pose more operational concerns in comparison to Data Security and Business Continuity Planning.

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 which aligns with business objectives.	Strength
IT Management	FFC has an IT steering committee which focuses on security policy.	Strength
IT Management	FFC's steering committee fails to oversee project management, systems acquisition, development, and delivery.	Weakness
IT Management	The steering committee excludes the VP of Information Security and VP of Internal Audit in favor of the vacant VP of Database Administration (less optimal use of human resources).	Weakness
IT Management	The VP of Applications assumes the role of the VP of Database Administration, violating segregation of duties.	Weakness
IT Management	The CFO may not have the technical expertise to lead both business and IT functions.	Weakness
IT Management	VP of Information Security reports to the CIO instead of the chief executive of the organization.	Weakness
IT Management	VP of HR fails to prioritize the hiring of the VP of Database Administration (6-8 month hiring period).	Weakness
Systems Development	VP of Applications oversees project management budget, time, and other specifics instead of Steering Committee members.	Weakness
Systems Development	New bio-coding payment system was over its time budget and initial dollar budget.	Weakness
Systems Development	FFC adopted and actually follows the Structured Systems Analysis and Design Methodology.	Strength
Systems Development	CIO periodically reviews and reconciles the budget of each and every project.	Weakness
Systems Development	Internal audit performs post-implementation reviews on projects over $2 million.	Strength
Change Management	Lack of a centralized Change Advisory/Control Board deviates from industry practice for change management procedures.	Weakness

Change Management	Lack of evidence of conversion controls for data transfers between systems; no internal auditing of the conversion process exists.	Weakness
Change Management	Lack of contingencies in the formal change procedures for these areas: backout plans after the change, monitoring of user rights/privileges during the change, the handling and documentation of emergency changes in times of crises.	Weakness
Change Management	FFC has formal documented change procedures with approval from department managers, the VP of Applications, and end-users where necessary.	Strength
Change Management	Both programmers perform changes in a separate development/ test environment with test data, not live data.	Strength
Change Management	The second programmer functions as a quality control measure for the changes performed by the first programmer.	Strength
Change Management	Programmers perform adequate testing prior to implementation (integration, volume, user acceptance, etc. testing)	Strength
Change Management	A securely stored audit trail exists of updated systems documentation from programmers and the change request log	Strength
Change Management	IT operations implements applications changes after changes are approved by the VP of Applications in formal procedures.	Strength
Change Management	FFC actually followed formal change management procedures when changing bio-code payment systems (as per audit team).	Strength
Data Security	No applications programmers, outside contractors, or visitors are permitted access into computer rooms without an escort. Visitors/contractors must contact the data center manager, bring a picture ID, and sign a log as well.	Strength
Data Security	Environmental controls are in place for protection against fires, and tested semi-annually by employees.	Strength
Data Security	The documentation for environmental controls testing is valid and up to date.	Strength
Data Security	No formalized security awareness or training program for FFC employees besides the outdated security policy.	Weakness
Data Security	Each employee has read and is aware of the security policy.	Strength
Data Security	The VP Operations has not needed to review the video camera tapes for at least six months since no unauthorized access attempts have been reported.	Weakness

Data Security	VP of Human Resources takes one month to send *Transfers and Terminations* Report to VP of Information Security -- this should be a real-time process.	Weakness
Data Security	VP of Information Security takes 3 weeks to modify/revoke access rights for transferred and terminated employees after receiving *Transfers and Terminations* report.	Weakness.
Data Security	VP of Information Security should not be modifying/revoking access; this should be a task for the security administrator	Weakness
Data Security	VP, IS should delegate tasks of auditing user audits, unauthorized user access reports, keycard access reports, etc. to security administrators.	Weakness
Data Security	The VP, IS should perform a quarterly user audit as per company procedures, but has not done this in the past 8 months.	Weakness
Data Security	The VP, IS didn't perform monthly checks of unauthorized user access reports as per company procedures for the past 6 months.	Weakness
Data Security	The VP, IS has not performed necessary quarterly checks of keycard access reports for the past 6 months.	Weakness
Data Security	Only one form of preventative control (password authentication)	Weakness
Data Security	Passwords are not displayed on terminals or reports.	Strength
Data Security	Security 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.	Strength
Data Security	Security software for passwords does not leave an audit trail through statistics of employees' sign-on information.	Weakness
Data Security	Quality of passwords such as "QSECOFR1" suggests executives and users may utilize passwords from default user profiles.	Weakness
Data Security	Security system generates daily logical access violation reports.	Strength
Data Security	System only allows three access attempts before locking out the user from access permanently.	Weakness
Data Security	The user must contact the VP, IS to have credentials reinstated (lack of help desk - departure from industry practices)	Weakness
Data Security	VP, IS should not be responsible for maintaining user profiles and authorization lists (violation of segregation of duties).	Weakness

Data Security	Although the VP, IS authorizes new hires, they should not issue credentials to new hires (should be completed by security admins)	Weakness
Data Security	User access is limited to workstations within the corresponding responsibility area (role-based access controls)	Strength
Data Security	Workstations can sit idle for 60 minutes.	Weakness
Data Security	Normal users may have multiple IDs. Each user ID may log onto one workstation at a time, meaning a user can technically log onto multiple workstations.	Weakness
Data Security	VP, IS has unlimited access to workstations and multiple sign-on sessions (no role-based access controls).	Weakness
Data Security	Facilities manager reports to the VP of Human Resources, who lacks security expertise.	Weakness
Data Security	As no one has reviewed the tapes for 6 months, there is no verification or accountability of tapes actually being recorded by facilities management.	Weakness
Data Security	Lack of auditing keycard access by appropriate IT personnel spills over into non-detection of unauthorized physical access.	Weakness
Change Management	Lack of a centralized Change Advisory/Control Board deviates from industry practice for change management procedures.	Weakness
Change Management	Lack of evidence of conversion controls for data transfers between systems; no internal auditing of the conversion process exists.	Weakness
Change Management	Lack of contingencies in the formal change procedures for these areas: backout plans after the change, monitoring of user rights/privileges during the change, the handling and documentation of emergency changes in times of crises.	Weakness
Change Management	FFC has formal documented change procedures with approval from department managers, the VP of Applications, and end-users where necessary.	Strength
Change Management	Both programmers perform changes in a separate development/ test environment with test data, not live data.	Strength
Change Management	The second programmer functions as a quality control measure for the changes performed by the first programmer.	Strength
Change Management	Programmers perform adequate testing prior to implementation (integration, volume, user acceptance, etc. testing)	Strength

Change Management	A securely stored audit trail exists of updated systems documentation from programmers and the change request log	Strength
Change Management	IT operations implements applications changes after changes are approved by the VP of Applications in formal procedures.	Strength
Change Management	FFC actually followed formal change management procedures when changing bio-code payment systems (as per audit team).	Strength
Change Management	VP of Applications stores Change Management documents in a fireproof vault in his office.	Strength
Business Continuity Planning	FFC performs a backup of its data and software on a daily basis	Strength
Business Continuity Planning	FFC has no current documentation of Business Continuity Planning or Disaster Recovery Plan whatsoever.	Weakness
Business Continuity Planning	Backups are only stored once a week at an off-site location.	Weakness
Business Continuity Planning	Lack of testing backup tapes in the past year and no plan to test backup tapes in the future.	Weakness

Part B: Risk Assessment for Each ITGC Area (Low, Medium, High)

ITGC Area	**Risk Assessment**
IT Management	Medium
Systems Development	Medium
Data Security	High
Change Management	Low
Business Continuity Planning	High