Information Technology General Controls Audit - Foods Fantastic Company

CIS 401 Section 97563

Team 101

[redacted]

[redacted]

Jensen Nielsen - 1218181731

[redacted]

EXHIBIT 3
Report Guidance
IT General Controls Risk Assessment Report Foods Fantastic Company

Background and Purpose:

Foods Fantastic Company (FFC) is an organization operating in the food industry, boasting a complex IT infrastructure to support its diverse operations. With an IT department actively engaged in implementing major projects over the past three years, FFC has integrated technology into critical facets of its business, including ERP systems, e-commerce platforms, and communication systems. The IT General Control (ITGC) review is important for FFC due to the organization's reliance on its IT landscape for processes within the value chain. Additionally, with recent challenges noted in project timelines and budgets, along with growing concerns of information security issues arising from former employees, the ITGC review serves as a crucial mechanism to identify and address potential vulnerabilities, optimize project success, and improve overall IT governance at Foods Fantastic Company.

Scope:

During our scope at Foods Fantastic Company (FFC), our audit encompassed a comprehensive evaluation of the information technology governance and controls landscape. We thoroughly went over FFC's IT policies, procedures, and practices, aiming to align the complexity of their technology with organizational objectives. When it came to the IT General Controls (ITGCs), we closely examined their management structure, the effectiveness of IT projects, and the alignment of IT strategies with overall business objectives. Our focus extended to critical areas such as security protocols, disaster recovery plans, while also making sure to meet industry standards, notably the Payment Card Industry Data Security Standard (PCI DSS). By thoroughly analyzing the company's security policies, change management procedures, and the integration of agile methodologies, our audit offered detailed insights and recommendations to strengthen FFC's IT framework.

Findings:

Starting with the IT management of FFC, there are positives and negatives that have been discovered. When meeting with the CIO, we were informed that the IT strategic plan was developed three years ago and is consistent with other corporate strategic plans. The CIO also mentioned the plan is reviewed and revised annually to outline objectives and strategies that the information systems group should implement to assist the organization in meeting the overall business objectives. The organization is also benefiting from the use of a hybrid cloud architecture to keep the essential business systems on the private cloud, and other business operations deemed not as crucial on a public cloud for easier access. By keeping certain systems on the private cloud, in the event of an attack, the IT department will restore operations by utilizing the backups on the private cloud. These are strengths to the organization in one sense, however there are some weaknesses that were identified that prevent these strengths from being fully operational and effective. The IT steering committee should be addressed immediately because with the current member selection, there is not a proper level of reporting taking place. If the IT steering committee replaced the CFO with the Director of Information Security, the IT Steering committee could present their plan to the CFO, who would then hold approval over the process ensuring the proper checks and balances were in place. Another major concern that was uncovered is that there is not an actual DRP in place for the IT department. Even though the company claims to have a plan in place, not having it documented correctly allows a preventable

risk to still exist.

Moving on to FFC's systems development, more unnecessary risks were uncovered during the audit. The most concerning came from the meeting with the VP of the Internal Audit team. During this meeting, it was discovered that the relationship between the IT team and internal audit team is creating a problem for the organization's systems development procedures, leading to most projects being over budget and taking longer than expected. Getting the internal audit team more involved with the IT management team could potentially eliminate this issue because with the proper guidance from the internal audit team, there would be less mistakes, leading to faster turnaround and implementation. The main positive in the systems development area of FFC is that the company is transitioning to an agile/scrum management style, which is much more effective in today's business model. Also, the CIO is overseeing all systems development projects, and reviews all of the expenses at the end of each month to compare to the overall budget. Even though the company is struggling to stay under budget, the proper documentation and approval is taking place.

During our debriefing with the Director for Information Security(DIS), we learned some good things and we learned some inefficiencies that can directly contribute to making the company more effective. Firstly, something really concerning that we learned in the first few sentences was that the Director of Infrastructure Delivery(DID) bears many of the responsibilities that should be the concern of the DIS. The DID is responsible for most logical controls such as implementing new users/hires into the employee database, assigns user privileges, changing user IDs for terminations/promotions and more. The Infrastructure Delivery team handles these tasks and reports any abnormalities to the DID who then reports it to the DIS. The DIS should have their own team or the DID's team should report to the DIS regarding these specific matters. This is inefficient and leaves an air gap between what's going on in Information Security and the person responsible for Information Security. The biggest security concern perhaps comes from the fact that workstations stand idle for 60 minutes before shutting off, and application connections remain intact for up to 2 hours of being idle. This is plenty of time for a bad actor to come in physically and tamper with the workstation or access session remotely. Especially, when you consider the company is federated through Single Sign-On(SSO), access to one application is access to all.

The DID department as we stated previously, is responsible for all the reporting essentially regarding information security. They relay the message along, if it becomes important enough then the DIS is notified. Now, we'd like to speak on some of the positives of the IS policy. There are mandatory password lengths, 90 day expiration on passwords(should be shorter), reusing of passwords up until 2 passwords ago(should be more), etc. Included in the policy as well are a variety of employee internet use protections such as anti-virus, phishing filters, firewalls , VPN, DMZ for private cloud and more. They are also now looking into being compliant with PCI-DSS as transactions have crossed the compliance threshold. This is extremely important and should be a focal point. In the beginning, the CFO stated that he wanted the IT aspect of the company to be more efficient. The solution quite possibly has already been rejected by the company. FFC has marginal log-analysis capabilities, which can be solved with a SIEM. The company considers this cost prohibitive, however the data aggregation would save time and money if it were implemented today. Even if it weren't it would be when a major cyberattack hits the company, because poor log analysis and network monitoring almost always leads to breaches.

The primary issue with Change Management was vaguely addressed within the previous paragraphs by way of other topics, but we would like to focus on it. Specifically, addressing the issues within the organization's privileges. Access logs haven't been reviewed in over 6 months

and HR's terminations report wasn't applied to privileges until 3 weeks (on average) after the DID received the report. Meaning, a fired employee could use their former credentials in order to access company infrastructure and make changes. Contractors and third-party services have gone into the server room(in which there are no cameras) to perform unsupervised labor. The authorization aspect of change management is something that should be of the utmost importance when revising the strategies of the company. Also mentioned, was the fact that all change management procedures in terms of infrastructure availability were properly followed. The company did not have to resort to any failover or redundancy options. While this is good, it doesn't change the fact that lack of authorization control organization could lead to a change in the good standing of availability.

In terms of a BCP, we discovered that FFC does not have one because management believes that it would be cost prohibitive for an organization of their size, this is a concerning point of weakness for FCC. There is a DRP in place, which is a strength, however it is barebones and the CFO is not aware of the level of detail or even the decision making criteria for when the plan would be implemented. This is of great concern, because with no BCP, and only a simple DRP with minimal supervision and testing, in the event of a security breach FFC's only option is their DRP. There was no mention of the DRP being tested. The only mention of data and software being backed up was in basic services provided by third party private cloud architecture, with no mention of any business involvement. We also learned that FFC ensures availability of its systems by contracting a third party infrastructure as a service provider. There were no incidents in the past fiscal year that required FFC to recover its systems using backups.

Conclusion:

Given the findings listed above, FFC's assessed level of ITGC risk is medium/high. There are some correct measures in place, such as having an IT strategic plan that has been developed within the past 5 years, having it reviewed annually, having strong password restrictions in place, applying the least privilege principle, and having a DRP that was produced by the IT department. There are others, however the bigger focus should be on the weaknesses that still exist, and were created from human error. The CFO for instance, is not up to date on the company's current DRP and the cost that would be associated with it, creating cause for concern in terms of responding to a disaster. In terms of preventing an incident, there are no cameras in the server room which has had two incidents in the last 12 months, there is not a SIEM system in place to log and monitor system access, the least privilege policy in effect is not properly enforced by employees, the employee responsible for monitoring the third party backups have not been checked up on. Overall, there is a lot of room for improvement and the best place to start is with a BCP. This is the biggest threat to FFC being able to withstand an attack and continue business operations when a situation does in fact take place.

EXHIBIT 4
Foods Fantastic Company IT General Controls Matrix

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

ITGC Area	Risk Assessment
IT Management	Medium
Systems Development	Medium
Information Security	High
Change Management	Medium
Business Continuity Planning	High

Part B: Detailed Strengths and Weaknesses

ITGC Area	Summary of Issue	Strength or Weakness
IT management	IT strategic plan that was developed 3 years ago, and is reviewed and revised annually by the IT Steering committee.	Strength
IT management	utilizes a hybrid cloud architecture, private and public clouds, with a centralized set of information systems	Strength
IT management	CFO oes not have direct insight into the DRP for IT including but not limited to recovery cost, time, and the decision-making process that would be involved	Weakness
IT management	IT Steering committee should report to the CFO instead of including the CFO in the committee	Weakness
Systems Development	Recently adopted the agile/scrum methodology and is the in the process of transitioning from waterfall methodology	Strength
Systems Development	CIO oversees the departmental expenses and compares them to monthly budget ensuring adequate documentation	Strength
Systems Development	Over last 3 years, project performance was 25% over initial time schedule indicating improper time management	Weakness
Systems Development	The IT team has a cordial relationship with the internal audit team that needs to be addressed. Rarely asking for input or advice is one of the leading causes to the lack of success with IT project implementation.	Weakness
Information Security	Strong password policy and software tools that prevent employees from falling victims to cyber attacks	Strength
Information Security	Strong reporting standards on all things that involve data and user privilege changes.	Strength
Information security	The well thought out user privilege policy is usually not enforced properly by staff.	Weakness
Information Security	No centralized log analysis tools such as a SIEM. Should consider investing in state-of-the-market tools.	Weakness
Information Security	Encrypts all packets that are sent over the public internet.Devices are also encrypted.	Strength
Information Security	Demilitarized zone for private cloud to filter traffic coming into the intranet.	Strength

Information Security	Passwords not displayed on screens	Strength
Information Security	Single Sign-On, prevents employees from each having multiple credentials which are more credentials floating around waiting to be compromised.	Strength
Information Security	Password lockouts. After 3 attempts personnel must contact the ID team directly to get their account reinstated. Prevents password spraying and other attacks.	Strength
Information Security	Apply the principle of least privilege. Prevents unnecessary security incidents by giving access to only files that are needed for their role.	Strength
Information Security	The Infrastructure Delivery team is responsible for creating and authorizing users. DIS has unnecessary personnel between them and access controls.	Weakness
Information Security	Zero requests to view and surveillance footage from within the last 12 months.	Weakness
Information Security	Termination report isn't applied until 3 weeks after it is received by the DID. Even longer before the CIS is notified about it.	Weakness
Information Security	2 incidents in the environment room in last 12 months	Weakness
Information Security	No surveillance camera in the server room	Weakness
Information Security	Idled workstations for up to 1 hour power on and 2 hours with live connections	Weakness
BCP	DRP that was developed by IT, hasn't had to be used in the past fiscal year	Strength
BCP	No BCP has been developed as management believes it is cost prohibitive for an organization of their size	Weakness
BCP	Backups are handled by third party infrastructure as a service providers and not actively monitored or checked on by FCC	Weakness
BCP	FCC has not had to recover its systems using a backup in the past fiscal year	Strength
BCP	no business involvement in DRP	Weakness