INFO 6008 - S2023

Test - 01

Gihan Shamike Liyanage

1142109

IT Auditing

06/06/2023

A picture containing font, graphics, graphic design, logo

Description automatically generated

TEST 1 – worth 35 Marks

There are five questions.

You may cite from these articles **ONLY** for your reasoning and answers. Take your time when you read these articles.

How you reason is how you will be marked.

I have provided the minimum and maximum length I need for each question via word count. Your responses should be 1.5 spaced – Font: Calibri. Marks will be deducted for poor grammar, sentence structure and spelling.

Please provide a Title page with your name, student ID and date. Please save your file as 6008 S2023 Test 1, last name, and date in (June 2023)

Q1. Read the following excerpt of this article and then answer the question that follows:

Choosing plan B - Danone rethinks the idea of the firm

A tradition of pursuing lofty social goals is going further - [**Business**](https://www.economist.com/business/)[Aug 9th, 2018 edition](https://www.economist.com/printedition/2018-08-11)

Aug 9th, 2018 - PARIS

THE food industry is going nowhere. Pretty pictures on food packets mislead. Big companies have disconnected people from their sustenance. Consumers, especially millennials, are sceptics about industrial-scale food production. Even sellers of healthy products, such as mineral water, spread harm—just look at billions of their plastic bottles that choke the oceans.

Such views are commonly heard among food activists, radical bloggers, or anti-capitalists. Yet these come from Emmanuel Faber, who runs Danone, a large French food company. Mr. Faber (pictured) frequently sounds like a doomsayer about his own industry—and about capitalism more broadly. “A revolution” and the end of globalisation are nigh, he says.

Danone is well-placed to spot such changes. With its headquarters in Paris, the company sells to over 130 countries and made nearly €25bn ($28bn) in revenues last year. Mostly it sells dairy goods such as Activia yogurt, mineral water (in plastic bottles) such as Evian or Volvic, and baby food. Mr. Faber sees change driven mostly by the new habits of consumers in rich countries. “People are walking out of brands that they’ve been consuming for decades,” he says. Millennials in particular do not think their food system works and are shopping locally, favouring smaller producers, and buying organic, plant-based or GM-free products.

Danone’s answer is to rethink the motivating idea of the company. That means rejecting the Anglo-Saxon idea that a firm exists primarily to maximise the welfare of its owners, the shareholders. Danone is pursuing what Mr. Faber sees as a more meaningful goal. The “purpose of this firm is not to create shareholder value”, he says. Instead, it is to get healthy food to as many mouths as possible, benefiting everyone from suppliers to consumers to owners.

The ISACA Code of Professional Ethics requires ISACA members and certification holders to do the following (taken directly from [www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx](http://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx)):

***3.****Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.*

**Q1. You are an ISACA member and an internal auditor at Danone. After reading the above article, do you believe, Danone is abiding by the ISACA code of ethics? Please explain your reasoning Min 150 words Max 250 words. 5 Marks**

Answer:

The ISACA Code of Professional Ethics expects its members to act in the best interests of stakeholders, maintain high standards of conduct, and avoid damaging their profession or the Association.

According to the article, Mr. Emmanuel Faber, the CEO of Danone, has a different view of the company’s purpose. He rejects the idea that maximizing shareholder value is the primary goal and instead emphasizes the importance of providing healthy food to as many people as possible, benefiting suppliers, consumers, and owners alike. This approach aligns with stakeholder capitalism, which prioritizes the interests of various stakeholders. Danone seems to be following the ISACA Code of Professional Ethics by considering the needs of consumers, suppliers, and owners.

Other than that Danone acknowledges the concerns and preferences of consumers, particularly millennials, by adapting its business model to offer local, organic, and plant-based products. This demonstrates a commitment to serving stakeholders. Furthermore, the article doesn't provide detailed information about Danone's practices, it indicates that the company is addressing the changing needs and expectations of its stakeholders. However, a more thorough examination of Danone's operations and adherence to ethical principles would be necessary to make a definitive judgment on its compliance with the ISACA Code of Professional Ethics.

Q2. Flexibility

A firm’s ability to respond to changes in its environment both rapidly and at low cost

Oct 9th, 2009

“In a business context, flexibility can refer to a number of different ideas. Today its most common usage is in the workplace where it refers to such things as flexitime, variable hours, and extended periods of leave. But the word has a longer pedigree in the area of strategy, where it generally refers to a firm's ability to respond to changes in its environment both rapidly and at low cost. In the (limited) sense that strategy is an unchanging commitment to something, it is the antithesis of flexibility.

A firm's strategic flexibility depends partly on its liquidity since its ability to respond speedily is inevitably determined by its access to funds. But more importantly it depends on its organisational structure, on the way in which its various units work with each other, and the freedom they have to take decisions on their own initiative.

The trade-off between flexibility and firmness has been a long-running subject of management discussion. Julian Birkinshaw, a professor at London Business School and author of “The Flexible Firm”, wrote an article in the summer 2004 edition of the *Sloan Management Review* called “Building Ambidexterity Into an Organisation”. In it he says:

For a company to succeed over the long term it needs to master both adaptability and alignment—an attribute that is sometimes referred to as ambidexterity.”

**Q2. You are a CISA auditor, and you know that when properly implemented, Information Security Governance is management’s visibility of, and control of, the entire information security management system.**

**As an auditor, you also know that governance is a process whereby senior management exerts strategic control over business functions through policies, objectives, delegation of authority, and monitoring.**

**Lastly, as an auditor, you also agree that governance is management’s oversight for all other business processes to ensure that business processes continue to effectively meet the organization’s business vision and objectives.**

**However, after reading the article you highlight the following from the above article “For a company to succeed over the long term it needs to master both adaptability and alignment—an attribute that is sometimes referred to as ambidexterity.”**

**As an auditor for a company’s information system, what would you look for in an enterprise that would suggest it is ambidextrous. What in particular would indicate to you that the enterprise is mastering both adaptability and alignment? Minimum 150 - Maximum 250 words - 5 Marks**

Answer:

As an initial step, I would see how well the company responds to changes in its environment. Can they quickly identify and deal with emerging threats and vulnerabilities in their information system? Being proactive in assessing risks and taking action would show that they can adapt to evolving cybersecurity challenges.

Next, I would examine the organization's structure and decision-making processes regarding information security. An adaptable and aligned company would have a system that balances flexibility and firmness. They would delegate authority to different units, giving them the power to make timely decisions while still staying aligned with overall security goals and policies. I would also evaluate how well the company adjusts its security controls and measures to address new risks. Can they adopt emerging technologies, follow industry best practices, and have effective incident response and recovery processes in place? Being adaptable in these areas would demonstrate their ability to respond quickly to changing threats.

Finally, I would look for evidence of ongoing monitoring and evaluation of their information security management system. An adaptable and aligned company would regularly assess the effectiveness of their security controls, measure performance against set metrics, and make data-driven adjustments to stay in line with their business objectives.

In general, an adaptable and aligned company in terms of information security would show a combination of responsiveness and consistency. They would be able to respond effectively to changes in threats and regulations while still maintaining a strategic approach to managing information security.

Auditing the auditors

An ex-PricewaterhouseCoopers’ man tilts at the Big Four

[**Finance & economics**](https://www.economist.com/finance-and-economics/)[Feb 13th 2003 edition](https://www.economist.com/printedition/2003-02-15)

Feb 13th, 2003

NO MATTER what the Big Four accounting firms do to mend their ways after Enron and the collapse of Arthur Andersen, their audits will still be unreliable. So, declares not an accountant-bashing shareholder activist, but Jonathan Hayward, a former partner of PricewaterhouseCoopers, who for years led the firm's efforts to improve its auditing methods.

Even if accounting firms are banned from carrying out other services for audit clients, says Mr. Hayward, they will still be beholden to the executives who hire and fire them. Just as important, the bond created by working closely together under pressure means that auditors too rarely challenge management.

Big audit firms, says Mr. Hayward, compete not on the quality of their audits but on the services, they can offer their clients. Trainee accountants fresh from university do the vast majority of audit work, counting things and ticking boxes without having to think much. Such inexperienced audit teams are unlikely to spot trouble.

**Q3. You are the CISO of a Silicon Valley CO going public. In prepping to list the company on the NASDAQ, you recognize that you need an external audit of your IT controls. You have been a fan of the Big Four and you read the above article.**

**From a *risk management perspective*, outline the dangers of “counting things and ticking boxes without having to think much”. Please support your answer with at least 2 examples. 7.5 marks – Min 300 words - Max 400 words**

Answer:

Depending on a superficial approach, like just ticking boxes, during an external IT audit can be risky for a company when preparing to go public. It may result in incomplete risk assessment, important vulnerabilities being overlooked, and emerging threats not being addressed.

A checkbox-style audit often focuses on checking if control measures are in place without fully evaluating the risks they are meant to address. This incomplete risk assessment approach lacks critical thinking and analysis needed to understand the company's specific risk situation and the impact of emerging threats. For instance, if the auditors only check basic security controls like firewalls and antivirus software, they might miss significant risks factors. They may not consider the need for more advanced measures to mitigate specific risks, like Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or data loss prevention systems. A comprehensive cybersecurity program should include multiple layers of protection, including network security, endpoint security and incident response capabilities.

Today’s world technology and cybersecurity constantly evolve, with new threats emerging all the time. A checkbox-style audit that relies on predefined controls might not keep up with these emerging risks, leaving the company exposed to new attack methods. For example, if the auditors only rely on standard checklists, they might not address emerging risks like cloud security, mobile vulnerabilities, or social engineering. These risks require a proactive and adaptable risk management approach, not just a checkbox mentality.

Moreover, this superficial approach undermines the effectiveness of the audit by missing control weaknesses that malicious actors could exploit. Gaps in security controls might go unnoticed, leaving the organization vulnerable to data breaches or unauthorized access.

To mitigate these risks, it is crucial to engage external auditors who take a comprehensive and risk-based approach. They should consider the organization's specific context, address emerging threats, and have experienced auditors with technical knowledge and critical thinking skills. By adopting a more thoughtful and holistic audit process, organizations can enhance their risk management, strengthen their security, and protect their assets and reputation more effectively.

**Q4. NIST Cybersecurity Framework (NIST CSF)**

Lately, ABC Inc. has been a target of a number of hacks and ransomware attacks. You are a cybersecurity expert/consultant and you have been hired by ABC Inc, a large enterprise.

In your preliminary discovery you note that ABC Inc. does not have a security framework in place. Security is managed informally.

**You recommend the NIST CSF.**

Your task now is to convince ABC Inc. to implement the NIST Cybersecurity Framework.

**In your own words, convince ABC Inc’s Management and INFO SEC Teams the need to implement the NIST CSF and, explain in simple terms, the 5 steps of the NIST CSF. Bear in mind some members of ABC Inc’s Management and INFO SEC Teams do *not* *understand risk frameworks*.**

**To conclude, tell me why the NIST CSF is a decent framework to implement.**

**7.5 marks Max 250 words**

1. Step 1: Identify
2. Step 2: Protect
3. Step 3: Detect
4. Step 4: Respond
5. Step 5: Recover

Short Conclusion:

Answer:

Recent series of hacking and ransomware incidents targeting ABC Inc., it has become evident that company’s current approach to security management, which is informal and lacks a structured framework, is no longer sufficient to protect organization from cyber threats. Therefor I would strongly recommend implementing the NIST CSF as a comprehensive solution to bolster the company’s defenses and ensure the security of valuable assets. The NIST CSF is a renowned cybersecurity framework that has gained recognition and support from government agencies, industry experts, and organizations worldwide. NIST CSF consists of 5 phases and those are Identify, Protect, Detect, Respond and Recover.

**Identify**: The NIST CSF's first phase entails understanding and controlling our cybersecurity risks. This can be used to undertake a thorough analysis of systems, networks, and data to find weaknesses, threats, and potential effects. This stage enables clearly grasp the risks which organizations face and organize security efforts into the highest priority areas.

**Protect**: After determining risks, the NIST CSF directs the company in putting in place the necessary protections to secure important assets. In order to reduce vulnerabilities and prevent unauthorized access, it offers guidance for creating access controls, network security measures, employee awareness programs, and other security practices.

**Detect**: The framework emphasizes the significance of ongoing cybersecurity event monitoring and detection. It motivates organizations to put in place preventative measures like intrusion detection systems, log analysis, and security incident response procedures to quickly identify and address possible risks.

**Respond**: In this stage NIST CSF assists in creating a successful response strategy in the unfortunate case of a cybersecurity incident. It describes actions to prevent further incidents, lessen their effects, protect evidence, and quickly resume normal activities. This proactive approach enables the company to minimize downtime, limit financial losses, and maintain the trust of our stakeholders.

**Recover**: The framework's last stage is all about getting back to business as usual after a cybersecurity event. It enables the organization to create a thorough business continuity strategy, set up backup and recovery procedures, and draw lessons from the incident to strengthen security posture moving forward.

As conclusion, in order to strengthen company’s cybersecurity defenses and provide a disciplined strategy to managing risks, ABC Inc. must implement the NIST CSF. Adopting this methodology will help to quickly recover from incidents, identify and eliminate vulnerabilities, safeguard organization’s assets and quickly identify possible threats.

**CEOs Love to Hear 'Yes' But Need 'No, No, No'**

<https://www.bloomberg.com/opinion/articles/2022-06-07/ey-split-shows-why-successful-ceos-need-to-hear-no>

Photographer: H. Armstrong Roberts/ClassicStoc/Archive Photos

*By Paul J. Davies*

June 7, 2022, at 12:00 a.m. EDT

In business and life, “Yes” opens doors to opportunity and growth. “No” holds you back.Say yes once and a decision is made. A no will be unwelcome and you might need to repeat it to get the message through.

Executives and investors often reward agreement and are reluctant to pay for skepticism. But easy consensus can be dangerous, while naysayers are often undervalued.

What got me thinking about this was news that the big-four accounting firm, EY, is considering a split into consulting and audit businesses. The former is what investors will want to own: Consultants are paid handsomely to agree that an idea is good and then spend hours working how to make it happen.

The audit folk meanwhile are lower-paid markers of homework, there to make sure that corners haven’t been cut or liberties taken with assumptions or income. Executives resent their cost and interference; investors see them as a safety net that is only noticeable when it fails. Nobody really wants them there, but when things go wrong everyone demands to know why they didn’t stop it.

The same thing happens regularly in banking and investing. After Credit Suisse Group AG lost $5.5 billion, more than any other bank, on the collapse of Archegos, the massively overleveraged hedge fund-like family office, the inquest uncovered how the people in risk and credit control lost their power to say no.

The independent report commissioned by the Swiss bank into the disaster found that its risk team monitoring hedge fund clients had been steadily “hollowed out” and left with fewer, less experienced staff. Other banks probably made similar mistakes but not quite so spectacularly.

Back in 2008 when Lehman Brothers failed, ex-employees said there had been little internal dissent: It was bad for your career. In fact, after the crisis the firm spawned, the industry recognized that numerous banks had disempowered their credit officers in the rush to create and securitize as many new mortgages and other loans as possible. Bankers and their bosses just wanted to keep dancing until the music stopped, in Citigroup Inc.’s then-Chief Executive Officer Chuck Prince’s infamous line.

In the aftermath, British playwright David Hare dissected how greed had completely overtaken fear. His production was entitled “The Power of Yes.”

Today’s investors are petrified of a collapse in high-growth technology stocks, which have been driven upward partly by the mathematics of ultra-low interest rates but also by the firehose of cash aimed at them by investors clamoring to shout yes at some founder’s vision.

In their desire to go along with these new leaders, investors have sometimes willfully surrendered their power to say no. Big tech firms like Google parent Alphabet Inc. and Facebook (now Meta Inc.) popularized the use of dual-class share structures, where voting power remains in the hands of founders and owners have little say.

The pinnacle of this era will be remembered as the $100 billion Vision Fund attached to Softbank Group Corp. of Japan. Its excitable and impulsive leader, Masayoshi Son, set out with a mission to buy into the ideas of as many technology prophets as possible with as much money as they could take. There was a culture of sycophancy towards Son and abnormally high-risk tolerance at the fund, a Bloomberg Businessweek investigation found in 2019.

The fund is now nursing billions of dollars in losses on ventures like WeWork, the temporary office-rental company that was less a tech firm than an ever-expanding party, or even a mass delusion: The book about its bright, brief flaring is called “The Cult of We.” It had limitless ambitions, now it just lets short lease work spaces.

The recent tech boom, like many manias before, is full of visionaries who turned out to be either wrong, unsavory, or incompetent. It also enabled outright deception, in which internal and external dissent were thoroughly suppressed. Among them is Theranos Inc. founder Elizabeth Holmes, who was convicted this year of fraud. Meanwhile, Wirecard AG’s former CEO, Markus Braun, awaits trial in Germany and EY’s auditors are among those facing some blame (and lawsuits). However, the payments company was adept at squeezing EY: When Wirecard entered the DAX 30 in 2018, it was paying annual audit fees of barely more than $2 million — a small fraction of other German blue-chips.

It’s hard to judge how much good the guardians of quality or risk should cost: Most companies don’t set out to defraud or just screw up. We could live in a world without scams, or one without the risk of making bad loans or investments, but the cost to progress would be great. As economist Dan Davies writes in his study of the history of fraud, “Lying for Money”: “It is highly unlikely that the optimal level of fraud is zero.” Without the risk of theft or loss, we’d never have invented international trade, the limited-liability company or even paper money.

We have to say yes to get anywhere, but too many yes men are a problem everywhere. All kinds of CEOs succumb to overconfidence when they surround themselves with panderers, according to James Westphal, professor of business administration at the University of Michigan’s Ross School of Business. A study he was involved with a decade ago, and that he replicated for a recent book, found an insidious effect of flattery and opinion conformity. CEOs who were swamped in it would not change strategy when their businesses underperformed.

Forget progress: Saying yes can just as easily cause stasis or decay. Harvard Business Review has reams of articles on the need to throw off the wet blanket of groupthink and dumb agreement. Failure to do so is how incumbents like IBM or Nokia got disrupted by Dell’s PCs, or Apple’s iPhone.

For political leaders, especially autocrats, having no deputies who will voice unpopular opinions can open terrible traps. Russia’s invasion of Ukraine might never have happened had President Vladimir Putin’s deputies given him a realistic idea of both the state of his armed forces and the determination of Ukrainians to defend their homeland.

**As an external IT auditor, how would an audit help you advocate a resounding No as a recommendation. In your answer, provide 2 scenarios of controls where a NO would help you, the auditor. Explain why a No or Nos is/are for the betterment of the enterprise. (Entity controls: Policy, Governance, Frameworks, Controls etc.). Min 200 words - Max 300 words – 10 marks**

Answer:

As an external IT auditor, conducting an audit can help advocate for a resounding "No" in certain scenarios where it is in the best interest of the business. ABC Inc. doesn't have strong policies and governance controls during the audit. This means they don't have clear rules for things like access control, data classification, incident response, or change management. In these cases, I would recommend saying "No" to the current situation and advise implementing comprehensive policies and governance frameworks. By having proper controls in place, ABC Inc. can ensure consistency, accountability, and better risk management.

Effective access controls guarantee that users have authorized access to IT systems, networks, and data in accordance with their job duties. The risk of unauthorized access, data breaches, and fraud can be reduced by saying "No" to excessive access privileges and poor task segregation. A strong authentication system, role-based access controls, frequent access reviews, and user activity monitoring may be suggested by the auditor. The organization can protect sensitive information, uphold data integrity, and adhere to regulatory requirements by implementing appropriate access restrictions.

Another scenario involves identifying weaknesses in technical controls. This could include things like poor network setup, weak passwords, lack of extra security measures, or outdated software with known issues. Here, saying "No" is crucial to emphasize the need for better technical controls. By implementing strong security measures like network segmentation, strong authentication, and regular software updates, ABC Inc. can reduce the risk of unauthorized access, data breaches, and malware attacks.

In these cases, saying "No" helps bring attention to the weaknesses in ABC Inc.'s controls. It highlights the need for improvement and encourages the company to take proactive steps to enhance its security. By making clear "No" recommendations, ABC Inc. can align its practices with industry standards and regulations. Executives and stakeholders may initially resist these controls due to potential inconveniences or added costs, it is the auditor's responsibility to advocate for their implementation in order to safeguard the organization's interests in the long run. Ultimately, this approach creates a more secure environment, protecting the company from cyber threats and improving its overall risk management.