SCS Mock 4

SCS | May - Aug 2024

Exam attempted on 2024-08-09 13:27:00

Exam attempted by [redacted]

Marked by Nicholas

Answer for Section 1 | SCS Mock 4

Elapsed Time 58:50

Scenario planning

Commented [TCS1]: Appropriate heading.

Scenario 1 - Successful implementation

The successful implementation of IoT within a business will have positive impact on day-to-day operations, as result of real-time data information. Real-time time would help introduce prediction of threat detection and will lead to improved reaction and action.

Commented [TCS2]: Accurate.

By implementing a IoT Saefwell is a leader in implementing technology innovation and gain new strong position between competitors due to this solution. The IoT helped upgrade client security system, leading to improved relationship with customers.

Commented [TCS3]: Accurate.

Satisfied customers and media attention resulted in improved revenue. New customers got in touch and Saefwell sign off new contracts, securing cash position for the next numbers of month.

Improved system, and happy customers have positive impact on our cashflow. The improved cashflow (money in) proved, that investment in IoT was a good decision. We have received return of investment as per original appraisal.

Commented [TCS4]: Accurate. However, both paragraphs should be consolidated into a single paragraph, as the second point extends from the first.

Tutor's note: Although your answer is accurate, it lacks comprehensiveness as it does not incorporate all relevant information from the scenario and preseen material. To provide a more complete answer, refer to main points 4, 5, and 6 under Scenario 1 for a detailed understanding of what should have been included.

Scenario 2 Post-implementation issues

The concerns highlighted by Bai Jing during first Board meeting after attending Tech Conference have become true reality to Saefwell.

Integration of the systems turns out to be much more complicated. As the result, our system was down sometimes for several hours. Each hour down had impact on revenue number. When our system was down, we were unable to provide a service to our customers.

Commented [TCS5]: Accurate.

Commented [TCS6]: Accurate.

Consequently, number of customers have asked for credit memo for the time that service was not provided. Other customer, who faced issues because of our inability to provide the promised service, made a threat regarding legal issues.

Reputation of Saewfell has been damaged. Consequently, we are unable to sign up new contracts with new customers. The worst is, that even our key customers, who are with us for xx years decided to leave as they faced security issue as results of our issues.

Commented [TCS7]: Your answer correctly identifies the potential impact of reputation damage on Saefwell. However, it's important to remember that this is a scenario planning exercise. You should focus on predicting potential future scenarios rather than stating them as if they have already occurred.

Instead of presenting the information as a current reality, frame it as a potential risk. For example: "The reputation of Saefwell could be significantly damaged if current issues are not addressed. As a result, the company might face difficulties in signing new contracts with prospective customers. More critically, long-standing key customers might consider leaving if they experience security issues due to these problems."

The issues with the IoT, had also impacted our shareholders and Share price. The share price dropped as result of our problem. Unsecure shareholders have decide to sell their shares, leading to further share price drop.

Commented [TCS8]: Your answer correctly identifies the potential impact of shareholders and the shard price of Saefwell. However, as mentioned earlier, it's important to remember that this is a scenario planning exercise. You should focus on predicting potential future scenarios rather than stating them as if they have already occurred.

Scenario 3 Postpone investment and watch

The decision has been made to postpone investment in IoT. The Board is now divided into two groups (1 who vote for implementation and 2nd who vote against). Saefwell lost their opportunity to be first mover in this area.

The decision was made, to ensure that Saefwell is not treated as guinea pig, as the consequences of unsuccessful implementation could be severe (please see scenario 2). As implementing IoT into security sector is new idea, it lead uncertainty around this.

Commented [TCS9]: Accurate.

Commented [TCS10]: Should have justified this point further to gain marks.

Saefwell, can now watch closely how their competitors perform after IoT implementation. If implementation of IoT into security sector will results in a big success, then Saewfell lost their opportunity of the first mover. The company who introduced as first and worked closely with IoT provider on improving gain a strong position on the market.

Although, if introducing of IoT in this sector was a bad idea, Saefwell will be safe and shareholders glad that Board postponed decision.

Conclusion

The 3 scenarios above present 3 possible outcomes linked to decision if Saefwell should and if yes what can expect if IoT is implemented. Scenario planning is used to help understand the best- and worst-case scenario of possible outcomes.

Additional Dividends

To benefit from gaining the first mover advantage position we need to make an investment first that will affect our cashflow significantly. Implementation of the IoT will require significant investment. Ideally, through equity - by issuing right of shares.

To encourage shareholders to further investment in the company, the additional dividend payment can help achieve the goal. Last year, we have paid out B$ 1,169million as dividends and we had B$1,684 million in the bank which is enough to cover additional 5% of dividends.

Additional payment to shareholders, should be communicated to shareholders as one-off situations, as the thank you for investing the funds in the company and trusting in Board decisions. The Thank you gesture should encourage shareholders to further investment.

The Board should include a letter explaining further plans of the company relating to IoT investment and nicely ask for further support. As shareholders will be advised about the planned investment and possibility of purchasing additional shares at reduced cost they might hold the extra 5% dividends received and re-invest back in Saefwell.

Although, paying out additional dividends will help strength relationship with shareholders, it will also reduce amount of cash available. The date of payment out should be carefully chosen, ensuring day-to-day activities are not affected by the additional payment.

Smart Contract vs Board Accountability for contract risk

Board is responsible for the company actions and outcomes. Decision to hire a specialized consultancy firm, won't change the fact, that Board is held accountable for the results.

If Board decide to work with Smart Contract company, needs to ensure first that employees of the Smart Contract have an experience and knowledge to assist us. As we operate in 74 countries, we require to have a specialist firm that have knowledge relating to these countries and their legal and economical background.

Board can reduce the contract risk, by choosing a proper consultancy company, although it won't mean that Board can't be accountable for the consequences of this decision. The Board is responsible for all win or losses that are happening in company operation.

The CEO would like to not be accountable for contract risk anymore as he is aware how risky it is. It is very difficult to predict an economical situation in different country especially if it is politically unstable country.

Commented [TCS11]: Accurate.

Commented [TCS12]: Accurate yet should have backed your argument with appropriate justifications to gain more marks. Please refer to the 3rd main point of the answer plan under option 3.

Commented [TCS13]: The explanation lacks both comprehension and clarity.

Commented [TCS14]: Should improve. Scenario planning goes beyond merely considering best and worst-case scenarios. Instead, it is a strategic approach used to assess risks, costs, and benefits associated with different actions, enabling the evaluation of a range of potential outcomes.

Commented [TCS15]: Appropriate heading.

Commented [TCS16]: The answer is irrelevant to the requirement. You have discussed how to finance IoT investments, whereas the task is to assess the implications of paying an additional 5% dividend.

Commented [TCS17]: While the answer is correct, it would be more effective to calculate the additional dividend in monetary terms to demonstrate that the company has sufficient funds to cover it. Refer to the 2nd main point of the answer plan for guidance on this calculation.

Commented [TCS18]: Accurate yet could improve. Refer to the 4th main point of the answer plan.

Commented [TCS19]: The response does not address the requirement. It seems you attempted to explain the logic from the 5th main point of the answer plan but did not explain it adequately.

Commented [TCS20]: Could improve. Refer to the 1st and the last main points in the answer plan.

Commented [TCS21]: This should have been the heading.

Commented [TCS22]: Accurate.

Commented [TCS23]: Accurate.

Commented [TCS24]: A similar point was addressed in your first paragraph. Avoid repeating the same answer points multiple times within a sub-task.

Commented [TCS25]: Irrelevant to the requirement.

I am assuming, that Board would like to be held accountable for the contract risk once find out that Smart Contract was a good decision and by signing up and working closely with consultancy company, we have reduced financial and operational implications.

According to Principal Risk, currently all our contracts are reviewed by in-house legal staff. Before the Board decide to sign off the contract with the Smart Contract, we should investigate how good or bad our contracts were signed off. The complexity and nature of the contract can vary, depends from service level and country location.

The contract with Smart Contract should be very carefully reviewed, and Board might decide to reach out to lawyer to ensure that chosen company will take some responsibility for unsuccessful contract, if they ensured before it is good decision.

The Board can reduce the risk, and impact of the risk by hiring the company like Smart Contract for example, but it is only a way of mitigation to reduce the risk impact. The risk will be partially transferred to the contractor, although still we will be paying the price even if it is not monetary it can be reputational as well.

After all, The Board is responsible and accountable for all decisions.

Tutor's note: The answer requires significant refinement. It lacks an evaluation of the board's accountability regarding contract risk management. Please refer to the masterclass and answer plan for detailed guidance on this topic.

Please do not hesitate to contact me if you have any further questions.

Thank you

Senior Finance Manager.

Commented [TCS26]: Irrelevant to the requirement.

Commented [TCS27]: Accurate.

Commented [TCS28]: It would be more precise to phrase it as: "Evaluate the effectiveness of Saefwell's current contract risk management processes."

Commented [TCS29]: Accurate yet lacks precision. Please refer to the 3rd main point off the answer plan.

Commented [TCS30]: Your point is unclear and needs further elaboration.

Answer for Section 2 | SCS Mock 4

Elapsed Time 60:00

Team Building

Saefwell is likely to face change management issue while setting new team for IoT adoption. The current team was set up on temporary basis and it is time now to set up a team that would look after IoT permanently.

It is important to have a clear communication with the current team and with potential new members of the team. Incorrect or inadequate information might lead to confusion and dissatisfaction.

It is possible that members of the current team, would like to stay in this position permanently. It is important to ensure that these members are taken into consideration when the new group will be created. If we exclude employees, who were temporarily assigned to IoT project, assuming they are not interested in permanent position we might expected their resignation notice or lack of engagement in their previous position.

The members of the team will face integration challenges, as they will have to learn how to work together. New people, different work culture and different work approach might result is tension between team members, which might negatively have impact on operational side of the business. To reduce the risk associated with group integration, it is worth to set up regular catch-up meetings to review the tasks and help each other. Also, members of the team, should have some time together to get to know each other better.

Bringing Snr Project Manager from MIT, who has great knowledge on IoT should help in building new team that under his supervision will learn how to cover gaps in knowledge. I am assuming his experience can also help with team building to ease the transition period.

Differentiation strategy in light of working with TechGuard

Adopting Digital Risk Compliance Platform in advance to required data might have positive impact on company differentiation strategy within industry. Introducing the solution sooner than required, enable us to test and fix issues when a time is for it.

Implementing DRCP will lead to automated risk assessment, which will provide real-time data, which could simplify Saewfell risk report process. Security management would be improved by continuous threat monitoring, which should result in early detection and quicker response to the threat.

Decision regarding implementing DCRP is supported by our values innovative. We have a chance to be a leader in security sector as DCRP has limited capacity for next 2 years. The limited capacity, give us competitive advantage as we will have an opportunity to learn in own pace, and provide improved service to our customers, while our competitors will be still working using traditional data source.

It looks like DRCP platform will be compatible with our systems it should lead to seamless data flow and improved efficiency. The 6,000 user accounts for the next 2 years will provide insight into platform ability. The beta testing phase will allow TechGuard team to work on platform improvements.

The new regulatory regarding Digital Risk can motivate Saefwell to join TechGuard and work with them, as it would be seen as forward-thinking strategy to our stakeholders. The earlier implementation of the solution, reduce the risk on non-compliance.

Commented [TCS31]: Should improve. Refer to the answer plan.

Commented [TCS32]: As the SFM, it is your responsibility to outline the change management issues associated with setting up the new IoT team. Your answer did not address this effectively. Please refer to the points highlighted under the sub-heading “Internal Conflicts” in the answer plan for detailed guidance.

Commented [TCS33]: Although the provided recommendations may help ease tensions between the current and new team members, you have not sufficiently described the potential internal conflicts that could arise. Your approach should have first identified the issues leading to resistance to change before suggesting recommendations to manage the transition. Instead, you highlighted recommendations without fully addressing the initial step of understanding the factors contributing to resistance. For detailed guidance, please refer to the answer plan and the masterclass.

Commented [TCS34]: Accurate.

Commented [TCS35]: Accurate.

Commented [TCS36]: The answer needs significant improvement. You have not adequately addressed the potential resistance the company might face when appointing the head of IoT, nor have you provided recommendations to overcome these issues. Please refer to the points highlighted in the answer plan under the relevant sub-heading for detailed guidance.appointing the Head of IoT.

Commented [TCS37]: Appropriate heading.

Commented [TCS38]: Lacks clarity.

Commented [TCS39]: Accurate.

Commented [TCS40]: Your answer is accurate but could be improved. The initiative also aligns with another value: “responsiveness.” Additionally, it supports the vision of “becoming the most trusted service provider.” For a more comprehensive answer, refer to the first main point of the answer plan.

Commented [TCS41]: Incorrect. Having a limit, such as restricted access in this instance, hinders the opportunity to achieve market leadership.

Commented [TCS42]: Incorrect. The limited capacity and the fact that the DRCP is still in its testing phase constrain its competitive advantage. If the DRCP fails to deliver the intended benefits due to software errors, it could lead to a competitive disadvantage. Please refer to the last main point of the answer plan for further details.

Commented [TCS43]: Irrelevant to the scenario, as once the DRCP-backed services are introduced to the market, Saefwell cannot afford delays in learning or making improvements. If customers using DRCP-backed services experience disruptions, while competitors using traditional systems offer reliable service, Saefwell’s offerings will be viewed unfavourably compared to competitors.

Commented [TCS44]: As previously mentioned, the software’s testing phase diminishes its competitive advantage.

Commented [TCS45]: Accurate, but you should have explained how early compliance with digital risk regulations can lead to a competitive advantage. Refer to the 2nd main point of the answer plan for detailed guidance.

The DCR is 20% more expensive than standard risk tracker. The cost of B$ 5million over 2 years, is a substantial investment, and might require a careful cost-benefit analysis, to ensure that benefits outweigh the cost. The investment will help us build a name and prestige in our sector as we will be seen as a leader of innovation.

Implementing DRCP suggest that Saefwell will be able to introduce differentiation strategy within industry, at the same time will improve efficiency leading to improved profit.

Share Price

It is recommended to sign up agreement with TechGuard describing type of information can be shared through the media. The clause should state that only information accepted by both sides can be made publicly available.The information shared will have impact on share price, and taking into consideration it is testing hase, not always we will have good news to share. It is important to ensure that updates provide is true, although carefully checked and reviewed, to not make panic if one of the test fail.

The correlation with TechGuard company will have impact on Saefwell reputation and viceversa. As the product is new and is still in testing phase it is crucial to ensure that only appropriate information are shared with wider group. The good news will strenght Saefwell reputation, more likely improving further revenue and profit as we have a chance to gain new customers, after a 2 years trial, when limit of 6,000 wan't be in place anymore. The future opportunity might encourage stakeholders/shareholders today to invest more and strenght share price today to benefit in future from new technology and higher dividends payments.

The exclusive access to the platform service, is itself big opportunity and make big step ahead of our competitors. Our competitors have access just to standard platforms. It Is recommended to highlight this exclusive access regulary and describe advantage of using premium service. Automated risk report, faster threat detection fits perfectly to our values.

It is also recommended, during advertising highlight the prestige and high-quality service that comes with DRCP.

To ensure that all information's are shared in appropriate manner, Saefwell might hire independent consultant, who will be able to evaluate the deal with TechGuard. The positive opinion of consultant will have positive impact on share price.

Above recommendations should help build a stakeholders and shareholders faith in Saefwell's and have positive impact on share price.

Please do not hesitate to contact me if you have any further questions.

Thank you

Senior Finance Manager.

Commented [TCS46]: Instead of merely suggesting that the board conduct a cost-benefit analysis, it is your responsibility as the SFM to provide a detailed evaluation that allows the board to weigh the costs and benefits of the investment. This evaluation should guide their decision on whether to proceed with the investment. Refer to the answer plan for a structured approach to highlighting the pros and cons of the investment, particularly in relation to how the software impacts Saefwell's competitive advantage.

Commented [TCS47]: Your answer is accurate but lacks justification to maximize marks. The relevant justifications are detailed in the second paragraph of your response. To achieve full marks, you should have linked these justifications more clearly to your arguments.

Commented [TCS48]: You should have outlined the steps the company needs to take to sustain its competitive advantage. Please refer to the 5th main point of the answer plan for detailed guidance.

Commented [TCS49]: Appropriate heading.

Commented [TCS50]: Accurate.

Commented [TCS51]: A similar point was covered in your previous paragraph. Avoid repeating the same information within the same sub-task.

Commented [TCS52]: Accurate.

Commented [TCS53]: Accurate.

Commented [TCS54]: A similar point was covered in your previous paragraph. Avoid repeating the same information within the same sub-task.

Commented [TCS55]: Instead of relying on consultants' services, it is more effective to use analysts' briefings. Investors are more likely to trust insights from capital market analysts—professionals with expertise in the area—rather than consultants. Refer to the 1st main point of the answer plan for further guidance.

Answer for Section 3 | SCS Mock 4

Elapsed Time 60:00

Internal Controls

Before any new controls are implemented, it is recommended to review our current Policy, especially the section regarding Digital Security. We need to ensure we have clear position regarding digital security, so our employees are aware about expectation and consequences of not-complying.

Considering the current incident, when one of our engineering shared his password and own username to the hackers is crucial to ensure company has clear policy in place describing how they are enhancing security and consequences for employees if they don't comply with it.

The updated policy should clearly state what information can be and what never can be shared with the third party. Saefwell should also make a direct contact with the suppliers/customers and choose the point of contact. Each person who will be called will have to be verified to ensure that we talk to the person that we think we talk. Ideal would be create an app, that can be shared with our customers/suppliers that generate one-off code that can be provided during a call. Although setting up few questions and verify them on the start of conversation should work as well for some time.

The policy should have in place continuous digital awareness training, followed by short tests that require achieving particular level to pass the test. The failure, automatically require re-do the learning session and take new test.

All our portals and websites. That require login's should have 2FA option turn on. Even if the username/password will be accidently shared, the hacker won't be able to access as he doesn't have the access to the application that's generates the codes.

The above controls should have positive impact on Digital Safety, especially social engineering.

Internal Audit

Internal Audit will start the test from checking if all our employees who should be trained regarding digital safety, have take the test and if they did pass the assessment. The assessment result will highlight the weak spot within organization and IA will have solid start point.

All emails have business nature and are owned by company. IA team should start checking the emails starting from people who have failed or have achieved the lowest score during assessment. This test, will help identify if the results of the tests, truly illustrates the higher risk linked to the particular person.

All external call are recorder. IA should ask for access to all recoding and identify the phone numbers, that are not in our system. This approach will help to identify potential social engineering calls who tries to gain trust before they do start asking questions regarding passwords and access.

It is recommended for IA to make a calls and emails to members of our company. The team should try to convince them to share their username and password. It will require more than couple calls/attempts but should help identify a potential area that require improvement.

As the last incident proved, the details to our engineers were listed on their social media profiles, Saewfell should make annotation in Policy document, that employees should not provide the workplace in their social media profiles. The IA should go through all social media profiles that our employees have to see what data is shared.

Tutor's note: The answers for sub-tasks (a) and (b) need significant refinement. These sub-tasks are interconnected: in sub-task (a), you were expected to recommend internal controls based on the information in the scenario, while in sub-task (b), you were to suggest tests to verify employee compliance with the controls recommended in sub-task (a). Because the internal controls you recommended were not foolproof, this has negatively impacted your marks for sub-task (b). Please consult the masterclass and answer plan for detailed guidance.

Commented [TCS56]: Appropriate heading.

Commented [TCS57]: Accurate.

Commented [TCS58]: As the SFM, your role is to outline the specific policies that should be included in the recommended policy statement. You have not provided foolproof and practical policies that take into account Saefwell's internal dynamics and the details presented in the scenario.

Commented [TCS59]: The recommendations are highly impractical given Saefwell's internal dynamics. As a global leader in the sector, verifying all incoming calls is not feasible due to the sheer volume of both local and international communications. Additionally, routing calls through an app would be overwhelming, and implementing verification questions could alienate stakeholders, damaging relationships.

Commented [TCS60]: Accurate, but should be improved. You should have detailed what should be covered in the recommended tests. Refer to the 1st sub-bullet point under the heading "Controls" for guidance.

Commented [TCS61]: Irrelevant to the scenario. Note that using 2FA is ineffective in cases of phishing attacks, as victims will also share their 2FA code, just as they would share their username and password.

Commented [TCS62]: Appropriate heading.

Commented [TCS63]: Accurate yet need to improve. Refer to the 1st main point of the answer plan.

Commented [TCS64]: Instead of implementing this practice, it is more effective to follow the recommendations outlined in the 3rd main point of the answer plan.

Commented [TCS65]: Implementing such a measure is highly impractical given Saefwell's extensive workforce of over 400,000 employees and its global client base. Recording all calls and tracking millions of phone numbers would be unfeasible and inefficient.

Commented [TCS66]: Your response is accurate. However, it would be clearer to use the term "penetration testing" instead.

Commented [TCS67]: Accurate.

Commented [TCS68]: It is impractical to suggest that the IA review all social media profiles of Saefwell's 400,000 employees, especially considering that each employee may have multiple accounts across various platforms (e.g., Facebook, YouTube, Instagram, Twitter, TikTok). This would make the process extremely cumbersome. For a more practical approach to monitoring social media profiles, refer to the 3rd main point in the answer plan.

Disciplinary Action

The reviewed and updated policy will help make a clear communication to employees regarding digital securtity and consequences of non-complying. Additionally Internal Audit test will help eastabilish if actions taken have improved employees knowledge and awareness leading to safer work environment.

The disciplinary action should only be implemented, if employee signed the updated policy, completed all the training and assessment and in purpose shared the data that he was not allowed to. Otherwise, the employees should be asked to take additional training, additional assesment to ensure their knowledge is definietly up to date. The IA team can make more tests around the employees who breaks the rules. For the first offence the employee should receive the warning, the second time can lead to withold payrise or bonus. This consequence will keep employees awake and they will think twice before they share sensitive data with 3rd party.

In case, when employee has failed twice and he has two wanings already - company should consider termination of the contract if this person doesn't comply for 3rd time - it can be disciplinary action or through the agreement behind closed doors. Conscious non comply to Saefwell Policy should be considered as offend and treat as such. In this case the company can make a decision about disciplinary action as it was breaching internal controls that have impact on company safety and could exploit company for legal fees and lost revenue.

Each case should be treat separetly and investigated carefully before any action is taken.

Please let me know if you need any additional information.

Thank you

Senior Finance Manager

Commented [TCS69]: Appropriate heading.

Commented [TCS70]: The introductory paragraph is unnecessary. Instead, address the requirement directly.

Commented [TCS71]: Accurate, but should have also included the need for disciplinary action in cases of failure to comply with regulations. Refer to the last main point in the answer plan.

Commented [TCS72]: Accurate.

Commented [TCS73]: Accurate, but these points should have been consolidated into a single paragraph for clarity.

Commented [TCS74]: It is important to enforce disciplinary action to deter other employees from repeatedly breaching internal controls.

Commented [TCS75]: Accurate.

Commented [TCS76]: Accurate.

Grade

Task		Allocated	Gained	Success %
1	a	25	17	68%
	b	10	5	50%
	c	15	6	40%
2	a	12.5	6	48%
	b	25	5	20%
	c	12.5	9	72%
3	a	17	5	29%
	b	16.5	7	42%
	c	16.5	10.5	64%
Total		150	70.5	47%

Pass Mark	**80**
Marks Gained	**70.5**
Grade	**FAIL**

- *Note that the areas highlighted in yellow depict the sub tasks in which you have not exceeded the threshold success rate of 54%.*

General Comments

The overall quality of your responses needs significant improvement. Many answers reflect gaps in theoretical knowledge, which has adversely affected the quality of your evaluations.

Further, there is a tendency to repeat the information presented in each scenario when developing the answers, which should be avoided to ensure clarity and conciseness in your responses.

It appears that you referred to the masterclass or answer plan before attempting the mock exam. As emphasized in the webinars and workshops, as well as in feedback for mock 3, you are expected to attempt the mock independently to identify and address any shortcomings. Referring to answers beforehand undermines the purpose of practicing under exam conditions, as it does not allow you to fully assess your own understanding and abilities. This adversely affects your claim to a pass guarantee, as it bypasses the intended learning process and practice conditions.

To gain a better understanding of the expected approach, please consult the Answer Plan for Mock 4 and watch the Masterclass videos related to Mock 4.

For those sub-tasks where your performance is subpar (highlighted in yellow), it is advisable to redevelop your answer plans. Compare your updated answer plans with those provided by TCS to pinpoint areas where your understanding may be lacking.

In terms of formatting, ensure that you write a paragraph for each answer point.