SwiftTech

Speed, Flexibility, Success

Congratulations! You have recently been hired by SwiftTech as a Cybersecurity GRC analyst! It's a great opportunity for you and the timing couldn't be better for SwiftTech. SwiftTech prides itself on being first-to-market with innovative technology solutions that improve work efficiency for companies around the globe. Part of SwiftTech's success hinges on their ability to overcome obstacles and do everything in their power to develop new ideas as quickly as possible. Their latest product is a Software-as-a-Service (SaaS) solution that makes Project Tracking a breeze. The beta launch has already gotten amazing reviews and some analysts are saying that SwiftTech's ProTrackPlus is a real contender to displace big name legacy Project Tracking software. In fact, SwiftTech has already lined up some potential large customers. A large healthcare system in the state of Minnesota has asked SwiftTech to participate in a Request for Proposal (RFP) process for new project management software. The government of the United Kingdom has also contacted SwiftTech about its software to replace project management software already being used by a number of government agencies.

SwiftTech does have a number of hurdles ahead. SwiftTech started off as a relatively small company. Their flagship product, GreenGrass – a contact management system, was designed and built to be installed on customer owned hardware in a physical location. ProTrackPlus is SwiftTech's first foray into SaaS. SwiftTech wants to follow best practices as they relate to SaaS but they don't want to sacrifice their commitment to agile software development and failing fast. SwiftTech's motto is: Speed, Flexibility, Success!

The major challenge for SwiftTech, however, is that they face a rapidly changing customer landscape that demands a higher level of vendor scrutiny. Prospective customers now expect new vendors to sign complex Master Service Agreements which dictate specific requirements for cybersecurity and governance, risk, and compliance programs. Many of the requirements are rooted in regulatory compliance or a potential customer's appetite for risk. They also, at a minimum, expect SaaS vendors to provide a SOCII report which helps establish a baseline for cybersecurity controls and validates their effectiveness.

SwiftTech does not currently have a SOCII report but they recently hired an outside firm, Firehawk Security, to perform a readiness assessment in preparation for pursuing a SOCII attestation report. SwiftTech's Chief Information Security Officer (CISO) has asked that you review Firehawk Security's recommendations and follow through on several action items. The CISO's email is below:

Welcome to SwiftTech! As we discussed during your interview, SwiftTech is very interested in obtaining a SOCII attestation report. We recently hired Firehawk Security to perform a readiness assessment, and I'd like for you take lead on remediating some of their findings/recommendations. I know you're the right person for the job. Specifically, I would like for you to:

1. **Security Posture** - Write a paragraph that explains SwiftTech's overall cybersecurity risk posture. You know a little about SwiftTech's goals and what drives its success. In the first sentence, you should describe SwiftTech's cybersecurity risk posture as Risk Accepting, Risk Neutral, or Risk Averse. In the remainder of the paragraph, please go on to explain why you chose your position on SwiftTech's risk posture and support your explanation with key facts from your knowledge about SwiftTech.
    a. Please include your paragraph in a separate slide in the provided presentation
2. **Relevant Frameworks** - Based on what you currently understand about potential customers for ProjectTrackPlus and the attached MSA excerpt from a healthcare provider in Minnesota, identify two or three regulatory frameworks, standards, or guidance that you believe we should use to measure our existing security controls and incorporate into our risk management framework. Please write an explanatory paragraph that clearly identifies the frameworks you've chosen and explains why you chose those frameworks.
    a. Please include your paragraph in a separate slide in the provided presentation

3. **Audit Against Frameworks** - After you have identified relevant security frameworks, please examine the attached diagrams. There is a SwiftTech Network diagram and a Data Flow diagram for our new ProTrackPlus product. Firehawk has already reviewed these and made notes about some areas of concern. I want to make sure we're all on the same page, so I'd like for you to compare their notes against the frameworks you've chosen to work from. You should be able to either validate or discard each concern. Don't forget to use the attached MSA as well. There may be specific security requirements that are more stringent in the MSA than those required by the compliance frameworks you've chosen.
    a. Please annotate your answers in the presentation provided by Firehawk on a separate slide. For instance, for the first item (which mentions AES-128 encryption) is that the correct level of encryption, is it too low, what should we be using based on your research from item 2 above?
4. **Risk Assessment** – We also need to perform a risk assessment this year. I want to keep it simple, so I went ahead and started a basic risk assessment just using the controls that Firehawk pointed out. Please only use those items - the same controls that you've been working with in Item 3 above. Based on your knowledge of GRC can you complete the risk assessment? Here are a few things to keep in mind:
    a. A control, or lack of control could create multiple risks
        i. I added a second placeholder for any control items that I felt had at least two risks that might be associated. Please try to come up with a primary and secondary risk for those items.

   b. I also created logical Risk Categories to correspond with each risk. Please choose the risk category that you feel best corresponds to your state risk.
   c. Please make sure to include your reasoning as to why a particular risk's likelihood and impact are scored as high, medium, or low.
   d. Please make your changes in the included RiskAssessment spreadsheet.

5. **Security Policy Development** – I started to put together a new Information Security Policy but, frankly, I'm too swamped to finish it. I'd like for you to finish writing the policy to incorporate just the sections that relate to the controls pointed out by Firehawk. Make sure whatever we say in the policy aligns to the best practices that you've developed in your previous work and please make sure those practices are explicit in the policy.
   a. Be sure to read the whole policy carefully. There may be something in it that isn't congruent with our new goals.
   b. Please make your changes directly in the include Security Policy document.
6. **Governance** – I'm very concerned about maintaining great End User Management controls. Based on your assessment of the end-user management controls pointed out by Firehawk, can you please design governance mechanisms to make sure we are always in compliance? For instance:
   a. For password length – how can we make sure all our users always have the right password length (whatever that is based on your assessment) – and successfully audit against the control
   b. Please include your ides in a separate slide in the provided presentation

Oh, by the way, can you get all this done by the end of the day? I have got a meeting with our executive leadership team in the morning and they’re expecting a status report.

Welcome Aboard!