Gap Analysis



**Assessor Instructions:**

* For each section, specific details must be provided about the current state, strengths, and gaps related to the corresponding best practice based on the information provided in Con’s email.
* Students need to identify for the following two practices (see benchmark answer below):
  + Cyber Security Systems Review Plan
  + Open Communication Among Staff
* The information under the Action column is clear and actionable, providing a foundation for improvement in cybersecurity practices.
* Students' description of the current state may vary, but it needs to relate to the applied practice and the information provided in the Con’s email.
* Students can provide different strengths, but their response needs to relate to the applied practice. A specific strength must be identified for the video tutorials, as per Con’s email. A benchmark answer is provided below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Applied Practice** | **Current State**  [Describe the current state.}  (Approximate word count: 20 – 50 words) | **Strengths**  [Provide one (1) strength of the applied practice.} | **Gaps**  [Identify areas where the review plan falls short, such as lack of automation or coverage of emerging threats.]  (Approximate word count: 20 – 50 words) | **Actions**  [Specify at least one (1) action that needs to be undertaken to address the gap. If there is no gap identified, you can leave this section blank.) |
| **Cyber Security Systems Review Plan** | <<Insert your response here>>  *Benchmark Answer:*  *Our Cyber Security Systems Review Plan is in place but lacks comprehensive coverage, as identified in the recent communication from Con Kafatos.*  *The existing system review does not integrate emerging threat intelligence sources, potentially leaving the organisation exposed to new and sophisticated threats.* | <<Insert your response here>> | <<Insert your response here>>  *Benchmark Answer:*  *The lack of integration with emerging threat intelligence sources, hindering our ability to proactively identify and mitigate new threats promptly.* | <<Insert your response here>>  *Students can suggest different actions, but their response needs to relate to the identified gap.* |
| **Cyber Security Instructional Guide** | <<Insert your response here>> | <<Insert your response here>> | <<Insert your response here>> | <<Insert your response here>> |
| **Video Tutorials on Device Setup** | <<Insert your response here>> | <<Insert your response here>>  *Benchmark answer:*  *The video tutorials were very helpful as they made the process easy and quick, even for the staff members who were not familiar with the applications.* | <<Insert your response here>> | <<Insert your response here>> |
| **Physical Security Plan** | <<Insert your response here>> | <<Insert your response here>> | <<Insert your response here>> | <<Insert your response here>> |
| **Open Communication Among Staff** | <<Insert your response here>>  *Benchmark answer:*  *Open communication channels have fostered a culture of awareness and accountability among staff members.*  *Inconsistencies in enforcing cybersecurity protocols have been reported, as highlighted in the communication from Con Kafatos.* | <<Insert your response here>> | <<Insert your response here>>  *Benchmark answer:*  *Inconsistency in enforcing cybersecurity protocols poses a risk, potentially leading to gaps in implementation.*  *Challenges reported by staff members in ensuring that best practices are consistently followed throughout the organisation.* | <<Insert your response here>>  *Students can suggest different actions, but their response needs to relate to the identified gap.* |