**Objectives**

Do the authors of the report outline clear cyber security goals or objectives? If so, state the cyber security objectives.

|  |
| --- |
| * Data stored safely inside or outside the company * Adequate protection to sensitive data * Data transmit in safe environments * Enough control of personal devices |

**Assessment of Cyber Risk**

How would you rate the overall quality of the assessment of cyber risk within the report?

 very poor

 poor

 fair

 good

 very good

 excellent

 exceptional

Do the authors thoroughly consider the context of risk assessment? If so, state the aspects of context considered. If not, state what the authors should improve.

|  |
| --- |
| * External factors including: legal environment, possible attacks, etc. * Internal factors including: use of personal devices.   The authors can improve by considering more internal factors, such as the organisation's business and financial objectives, capabilities of processes, etc. |

Do the authors appropriately identify cyber risks? If so, state the sources of evidence and process to determine relevancy. If not, state what sources of evidence the authors should consider.

|  |
| --- |
| * In risk assessment: Storage of Data and Documents paragraph 2, the authors give real numbers and related regulations from cloud provider, which shows that personal data on cloud platform can be accessed by governments or organisations and proves that the risk of losing data control. * In risk assessment: Freedom of Information and other requests paragraph 2, the contents demonstrate that increasing financial loss can be made when the company has failed to comply with obligations to provide personal information as required, which testifies the risk of companiesâ€™ failures in complying with obligations or unable to access personal data required by the government.   The authors have given some good examples as sources of evidence, and they may need to consider evidence of risks in regards to personal devices, public network environment, etc. |

How would rate the analysis of the identified cyber risks?

 too heavy

 about right

 too light

How would rate the evaluation of the identified cyber risks?

 too heavy

 about right

 too light

**Policy**

Does the policy appear to communicate a strategy for dealing with perceived cyber risks?

 Yes

 No

 Don't know

Does the policy demonstrate an understanding of the asset(s) to be protected? If so, state the asset(s) you perceive the policy is attempting to protect. If not, state the asset(s) the authors may want to consider.

|  |
| --- |
| The policies listed in the report protect assets including personal data, copyrighted material and credentials on personal devices. The authors may also want to protect some other assets like possible financial loss. |

Does the policy reflect consideration of domain best practice, rules and regulation?

 Yes

 No

 Don't know

**Metrics**

Do the authors attempt to understand what the success of the intervention would look like? If so, state how they determine the success of the intervention. If not, suggest how the authors could determine the success of the intervention.

|  |
| --- |
| All sensitive data and important copyrighted material will only be stored and transmitted inside the company, and all the business processes and personal devices used to login need to be issued and managed by IT team. There is a tiny suggestion that the authors may want to add some detailed descriptions about the implementation of policies as well as the successful intervention in this report. |

Do the authors attempt to understand the implication of any suggested interventions? If so, state how they explain the implication of any intervention. If not, suggest how the author could better understand and explain the implication of intervention.

|  |
| --- |
| The authors may would like to give more explanations about the expected intervention in the company, they may also need to list some specific requirements in data transmit, personal devices management, etc. |

**Communication**

Does the policy communicate directives in a clear and concise manner to all stakeholders? If so, indicate how the policy communicates effectively. If not, indicate how the authors could improve clarity of communication.

|  |
| --- |
| The policies listed in the report introduce the importance of IT team which is supposed to responsible for management data and personal devices. Regular data protection good-practice sessions which will be held with each department are helpful staf to understand the basic of personal cloud as well as company policies. For more internal communications, the authors may consider possible ways to communicate with stakeholders for better implementation. |

How would rate the number of references in the report?

 too heavy

 about right

 too light

One-page review

The one-page review should have 1-inch margins all around, A4-size, 12-point font and be in PDF format. The one-page should prioritise areas of improvements for the authors. Teams may want to consider the questions within the interactive rubric when they create their one-page review. In the review, teams should support other teams in improving their drafts, by

* advising the authors what they should **start** demonstrating in the report that is currently missing or incomplete, e.g. proper identification of cyber risks.
* advising the authors what they should **stop** doing within the report itself, e.g. what is not working or is causing confusion. ·
* advising the authors  what they should **continue** doing within the report itself, e.g. referencing strong evidence that cements arguments.

Teams should view the review as opportunity to prioritise to authors what would dramatically improve the draft report. Team members may think there are many areas of improvement, but they should demonstrate that they have prioritised key areas of improvement. Teams are encouraged to discuss and decide the key areas of improvement. Teams should offer advice on how to improve the draft, even if the draft itself is sparse, lacks content or has taken the wrong direction.

**1 page review**

The report focuses mainly on the protection during data transmit, also personal devices management, which are necessary to solve problems and make a safer environment for personal cloud usage. But there might be some improvements can be made as below. Start • More specific descriptions about the successful intervention The authors actually already explain the possible improvements in data protection, effective management, etc. They may want to add a simple paragraph to list these and explain clearly about the successful intervention they may expect.[*This goes back to us needing to change last page to talk about metrics, so yeah.*] • Consider more about the company’s business and financial objectives The authors take the factors including legal environment, use of personal devices, etc. into account to list all possible concerns and risks. They may also would like to analyze the possible effect of company’s business and financial objectives. [*Maybe but its not my area so I’m not sure*]• More communications with stakeholders and staff in policies The authors have listed some really effective policies in data protection, personal device management, etc. They may want to consider policies that could possibly communicate effectively with stakeholders. [*Could be a good idea.*] Stop • Duplicate descriptions in risk assessment There are some duplicates in risk assessment, like the Storage of Data and Documents paragraph 3 and Extensibility and accessibility of applications and other concerns paragraph 2 & 3,[*second review also said we’re repeating ourselves, need to find it and fix it.*] and it would be a little confusing although sometimes these risks do have connections with each other. The authors may need to reorganize these contents and try some different ways to explain them. Continue • Risk assessment: Collusion Concerns Paragraph 1 & 2 The authors give some really good examples to explain the risks in regards to collusion concerns, but they may also want to explain more explicitly about the way these facts affect cyber risks. [*I’ll have a look and see if I can be clearer and more explicit.*] • Personal clouds vs. business-based clouds It would be better if the authors could consider some explanation about the concerns and risks coming from the differences between these two cloud providers. • Collusion concerns and risks assessment Although the concerns and risks issued by the authors are very clear and persuasive, they cannot be controlled or improved by the policies listed in this report. The authors may want to introduce more examples and effective ways to connect these concerns and risks with the company, also find some possible ways to internally control business processes and protect personal data. [This is actually a really good point, we should talk about risks we can have actionable policies for, or in discussion outright say which risks are important but aren’t actionable.]