ISEC-655 Fall 2022

Dr. Michelle Ramim

Eric Webb

Assignment #2 Executive Summary

November 27th, 2022

Dear Executives,

I have been tasked with conducting a formal review of the organizations device sanitation policy. Please see my detailed narrative below for basing future decisions on this subject matter.

Thank you again.

-Eric Webb

(CISSP)

**Old Computer and Device Sanitation Policy.**

1. Provide an overview of a small, medium, or large business that you are familiar with

The company is a very large and well respected company. Currently there is a sanitation policy loosely enforced and defined. New hires are seeing old worker accounts on their laptops. The machines are not being sanitized properly. The policies defined state that machines should be properly sanitized before giving to the new hires but no procedure is concretely defined.

2. Define the current state of Old Computer and Device Sanitation Policy.

Current state is a CMM3:*Senior Management and information security management have determined the levels of risk that an organization will tolerate and have standard measures for risk/return ratios. (Brotby, 2009)*

If they begin to enforce and manage old computer and devices sanitation properly. They could become a CMM4*:Responsibilities for information security are clearly assigned, managed and enforced.(Brotby, 2009)*

3. Select one of the approaches that we learned about including:

3.1. Indicate which approach you have selected and provide a brief logical support for your selection

The Capability Maturity Model gives an evolutionary path of increasingly organized and systematically more mature processes. It is used to develop and refine the security development process.

3.2. Complete an analysis for each element, attribute, and characteristic using the framework to determine the gap between the current state and the desired state related to the policy area selected.

Old computer and devices sanitation responsibility must be defined for all employees and contractors. Effort needs to be made to prevent old accounts from not being sanitized.

3.3. Describe the unmitigated risk(s) from the current policy, and what it will require to “fill” the gap. Specifically, will it require different processes, technologies, controls, and so on to address the unmitigated risk(s)

There are a few unmitigated risks from the previous accounts not being properly sanitized.

*A- It exposes residual data of companies past endeavors.*

*B- Backdoor could have been left by previous worker.*

*C- New worker could use old account to masquerade.*

To fill the gaps, policies must enforce procedures to properly sanitize devices.

3.4. Define the desired information security governance objectives and outcomes.

Hint: list in chapter 7, p. 47)

Management should have defined job responsibilities and procedure ownership for the IT sanitation team. All personnel should be aware of the responsibilities and ownership of assets and services that manages old computer and devices sanitation. Residual accounts should not be on new hire laptops.

3.5. Define the desired security risk management objectives and outcomes. (Hint: list

in chapter 8, p. 78)

To fill the gap,

3.6. Suggest the time recovery objectives associated with the plan that you are

proposing to address the unmitigated risk(s). (Hint: p. 78)

To fill the gap,

3.7. Develop an information security strategy or suggest how to adjust the existing

security strategy related to the area that you selected (Hint: p. 90)

To fill the gap,

3.8. Suggest an implementation plan, list the resources needed, and a plan on how to

gather support from the board of directions/senior management.

To fill the gap,

3.9. Suggest a metric and monitoring process as well as compliance (Hint: p. 90)

To fill the gap,

3.10. Provide your opinion about the potential challenges with the executive

board as well as the implementation/compliance strategies. Are the objectives

realistic and achievable? Are the objectives likely to achieve the desired

outcomes? Predict the chances of success.

To fill the gap,

# References

Rasner, G. (2018) "Front Matter," in Cybersecurity and Third-Party Risk: Third Party Threat Hunting, Wiley, 2021.

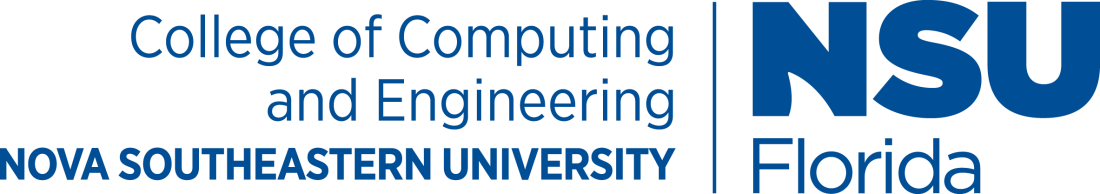
Ryan, O. (2016, June 8). *Third-party governance and Risk Management: Deloitte: Risk Services*. Deloitte. Retrieved November 11, 2022, from

https://www2.deloitte.com/cbc/en/pages/risk/articles/third-party-governance-and-riskmanagement.html

Brotby, K. (2009). Information security governance (1st ed.). John Wiley & Sons, Inc.

Amiri, A. (2007). Dare to share: Protecting sensitive knowledge with data sanitization. *Decision Support Systems*, pp*.* 181-191.

**Certification of Authorship of Doctoral Course Assignment**



Submitted to: Dr. Ramim

Student’s Name: Eric Webb

Date of Submission: November 27th, 2022

Purpose and Title of Submission: Assignment #2 Executive Review

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this purpose.

Student's Signature: ERIC WEBB