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 our organizations Internet Security Policy.

…

Thank you again.

- Eric Webb

(CISSP)

# Internet Security Policy

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

(current workplace, family business, etc.)

2. Define the current state of the Information Security Policy that is in place for the

relevant topic selected above

sss

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

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. (SABSA, COBIT,CMM)

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). (Hint: Gap analysis of the

unmitigated risk)

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

(Hint: list in chapter 7, p. 47)

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

in chapter 8, p. 78)

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

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

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)

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.

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

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.

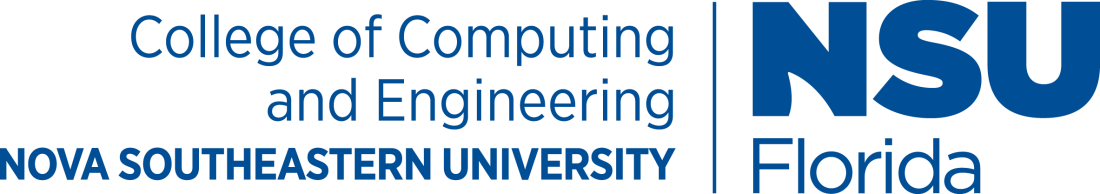
# References

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

**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