C769 Task 1 IT Capstone Topic Approval Form

The purpose of this document is to help you clearly explain your capstone topic, project scope, and timeline and to ensure that they align with your degree emphasis. Without clearly addressing each of these areas, you will not have a complete and realistic overview of your project, and your instructor cannot accurately assess whether your project will be viable for the purposes of these courses.

Complete this form and send it (via UGCapstoneIT@WGU.edu) to your instructor for approval. Once approved, you will receive a signed document in PDF format that you can upload as part of Task 1.

It is the policy of Western Governors University (WGU) that student capstone projects should not be based on or include, without authorization, restricted information. Restricted information is any proprietary or classified information or material belonging to your employer or any other third party. You acknowledge that you will not use restricted information in your capstone project without obtaining the third party's permission by using the "**IT Capstone Project Restricted Information Authorization Form**" found in the Supporting Documents section of Task 1.

DEGREE EMPHASIS: Bachelor of Science, Cybersecurity and Information Assurance

ANALYSIS:

Project Topic – Implementing a Defense-in-Depth Strategy for SecureBank

Problem Statement or Project Purpose – SecureBank is facing significant cybersecurity risks that threaten the security of confidential data and regulatory compliance. Without a strong security strategy, the risk of data breaches increases, potentially damaging stakeholder confidence. To address these issues, SecureBank must adopt a defense-in-depth strategy that integrates various security measures. This project aims to enhance the bank's cybersecurity through proactive measures and ongoing training, ultimately protecting sensitive data and maintaining stakeholder trust.

DESIGN and DEVELOPMENT:

Project Scope

a. Project Goal(s) and Supporting Objectives – Enhance SecureBank's cybersecurity by implementing a defense-in-depth strategy to safeguard sensitive data and mitigate risks by conducting assessments to identify vulnerabilities and compliance gaps, integrating layered security architectures with advanced threat detection and access controls, establishing a proactive incident response plan and regular testing protocols, and fostering security awareness through ongoing employee training. (Fortinet, n.d.).

b. Project Outcomes and Deliverables –

i. **Vulnerability Assessment Report:** A detailed review of security weaknesses and compliance challenges.
ii. **Layered Security Architecture Design:** Deployment of a comprehensive security framework.
iii. **Incident Response Plan:** Established procedures for handling security incidents.
iv. **Training Program:** Continuous cybersecurity awareness training for staff.
v. **Testing Protocols:** Regularly scheduled security testing protocols for ongoing enhancement.

IMPLEMENTATION and EVALUATION:

Describe how you will approach the execution of your project –

a. **Introduction:** Highlight the importance of cybersecurity in finance and the document's purpose.
b. **Defense-in-Depth Overview:** Define the strategy and its significance in risk mitigation.
c. **Assessment and Audit:** Outline the need for comprehensive security assessments.
d. **Key Findings:** Summarize critical vulnerabilities identified.
e. **Remediation Strategies:** Provide targeted recommendations for each vulnerability.
f. **Layered Security Architecture:** Outline essential elements such as firewalls and access control mechanisms.
g. **Threat Intelligence and Monitoring:** Examine the importance of threat intelligence and the function of SIEM tools.
h. **Incident Response Plan:** Outline essential elements of the IRP and training importance.
i. **Training and Awareness:** Highlight employee training and awareness initiatives.
j. **Regular Testing and Compliance:** Emphasize ongoing assessments and adherence to regulations.
k. **Scalability Considerations:** Address the need for scalable security measures.
l. **Conclusion:** Recap the strategy's importance and need for continuous improvement.

Reference:

- What Is Defense In Depth? Defined and Explained. Fortinet. (n.d.). https://www.fortinet.com/resources/cyberglossary/defense-in-depth

IRB REVIEW:

☑ **This project does not involve human subjects research and is exempt from WGU IRB review.**

COURSE INSTRUCTOR SIGNATURE: James R Ashe

COURSE INSTRUCTOR APPROVAL DATE: Tuesday, October 8, 2024