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: B.S. Information Technology

ANALYSIS:

Project Topic – Modern Security Information and Event Management (SIEM) Systems

Problem Statement or Project Purpose – The purpose of this project is to highlight the importance of IT security and how a SIEM system can be a crucial pillar in both the passive and proactive protection of an IT environment. The IT field is always expanding and changing. As it expands and new technologies are introduced, businesses integrate the new technologies into their companies to capitalize on their benefits. Unfortunately, with new technologies come new vulnerabilities and bad actors who will attempt to capitalize on those vulnerabilities. In recent times, many businesses have neglected to modernize their IT security systems to keep up with the ever-changing landscape, to their detriment. Many of these businesses have suffered significant financial and reputational losses due to bad actors exploiting vulnerabilities in their security systems to manipulate and/or steal data; some businesses have suffered critical blows to their public image when it was publicly revealed that the causes of these breaches could have been easily avoided if they had simply used modern (and sometimes already standardized) security implementations. When implementing new technologies, businesses need to remember to keep their security systems updated as well. One critical part of the IT security infrastructure in today's world is a SIEM. Modern SIEMs implement advancements in AI to more efficiently analyze data logs to detect vulnerabilities and respond to threats.

DESIGN and DEVELOPMENT:

Project Scope

a. **Project Goal(s) and Supporting Objectives** – The goal of this project is to guide a hypothetical business (TransBrasil Logistica) in implementing a modern SIEM system into their IT infrastructure. TransBrasil, a relatively small shipping company, has just received their first major contract from Vicente Industria LTDA, a large Brazilian parts supplier. TransBrasil's small IT team has normally manually analyzed data logs infrequently to spot any potential threats. With this new contract, and the increased data traffic that will inevitably come because of it, the IT Department Head has notified his superiors that they will need to upgrade their security systems to be able to handle the increased traffic and guarantee security for the data that their new client will bring. The current way of manually analyzing logs will be far too slow and too infrequent to be a viable security solution. Understanding the risks that an underdeveloped and underprepared security environment could have on their business at such an important time, TransBrasil's executives have given their IT department the green light to find an implement an effective solution to this problem as fast and efficiently as possible. The IT Department head believes a SIEM system would be a practical and cost-effective way of solving this problem.

   Supporting objectives would be the individual steps necessary to get the SIEM integrated into their business, from analyzing their existing systems to choose the best SIEM for their business, to final implementation of the SIEM and continued maintenance.

b. **Project Outcomes and Deliverables** – The outcome is that the business will have successfully integrated a modern SIEM into their business, a critical piece of IT infrastructure that will help them in keeping their data protected.

   - The deliverables will be the successful completion of the steps necessary to implement the SIEM:
     1. Define the business objectives for the SIEM.
     2. Analyze the current systems to choose the best SIEM solution.
     3. Plan the physical and logical integration of the chosen SIEM into the current system.
     4. Deploy and configure the SIEM, to include testing and optimization.
     5. Integrate the automation of the SIEM by setting up machine learning and data feeds.
     6. Continual maintenance. Plan for updates and keep the staff up to date on new system updates and features.

IMPLEMENTATION and EVALUATION:

Describe how you will approach the execution of your project – I will describe each of the steps in more detail, the business' choices and decisions on each step (e.g., which SIEM solution they decided to purchase or implement), and the outcomes or consequences of their decisions.

IRB REVIEW:

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

COURSE INSTRUCTOR SIGNATURE:

James R Ashe

Jim Ashe, Ph.D. Mathematics

COURSE INSTRUCTOR APPROVAL DATE:

1/25/25