

# **The Effect of Adaptive Education Intervention on the Ability and Aptitude in Cybersecurity Career Paths: A Quasi-Experimental Study**

# Project Team

## La Trobe University

- Dr Javed Morshed Chowdhury

## Australian Catholic University

- A/Prof Bhavani Sridharan
- **Dr Kamanashis Biswas**

# Motivation

- High rate of students' attrition and low success rate
- Huge labor market demand
- Massive skills gap in cybersecurity and related areas
- Courses may or may not align with their ability to cope with the learning requirements
- Mismatch between ability and aspiration

# Project Goals

- Support students with an informed decision-making process
- Create awareness about diverse cybersecurity roles which require different knowledge, skills and aptitudes.
- Motivate students to realize their dream jobs through effective educational intervention initiatives
- Design, develop and implement personalized, engaging and motivating adaptive learning intervention activities/resources
- Evaluate the effect of this intervention on the outcome variables

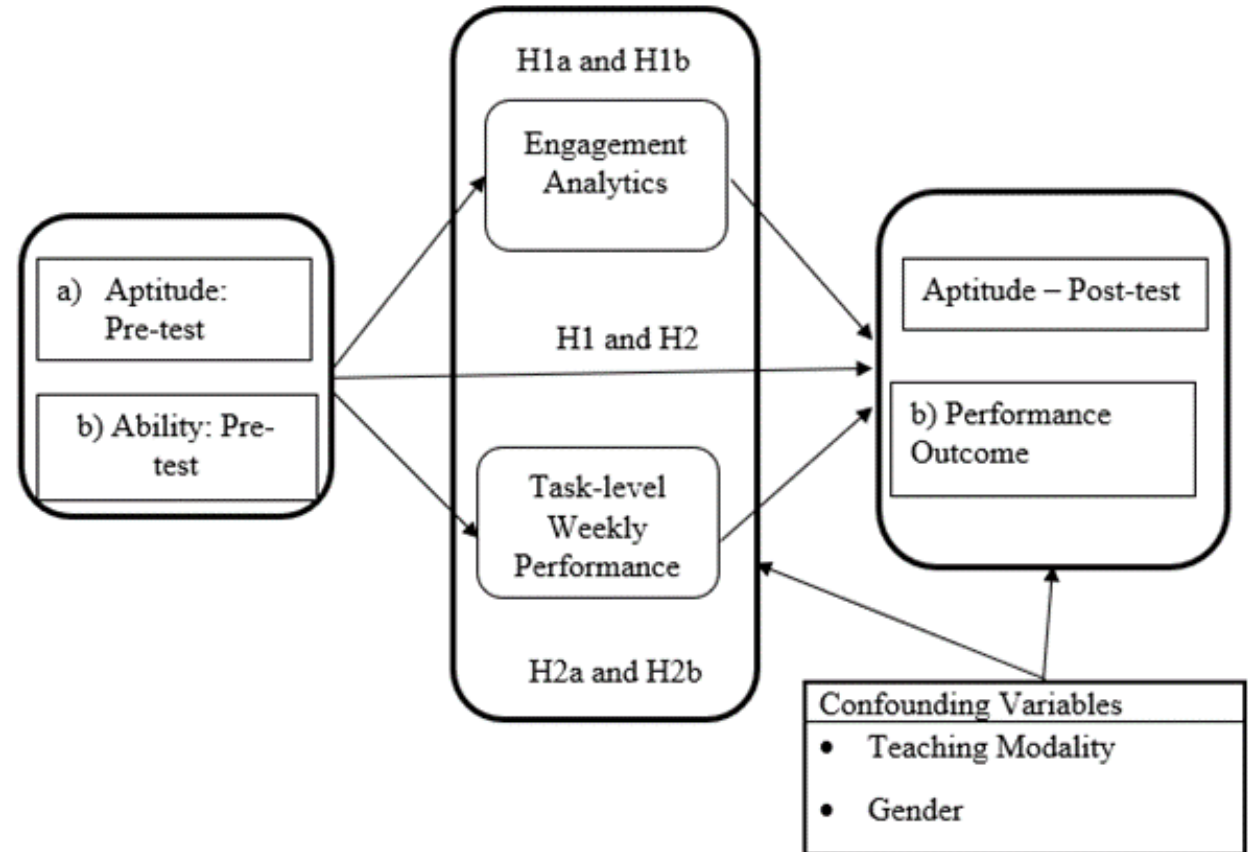
# Project Activities

## Key underpinning theories

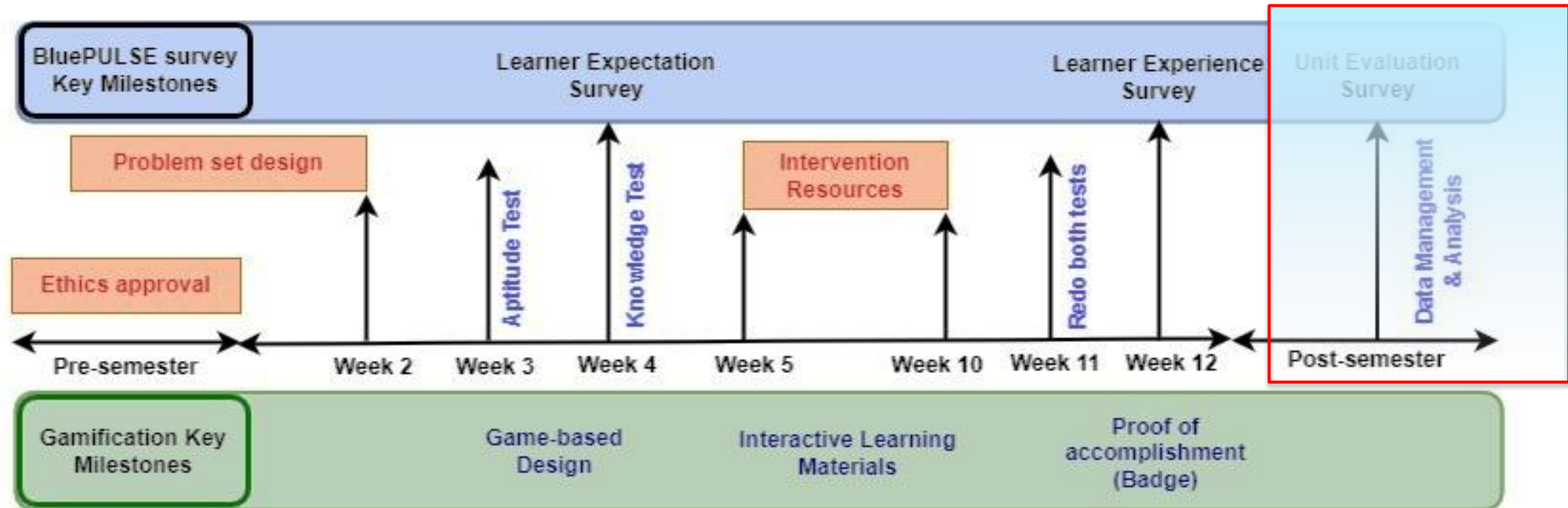
- Theory of Self-determination
- Zone of Proximal Development (ZPD)

## Key needs for motivating students

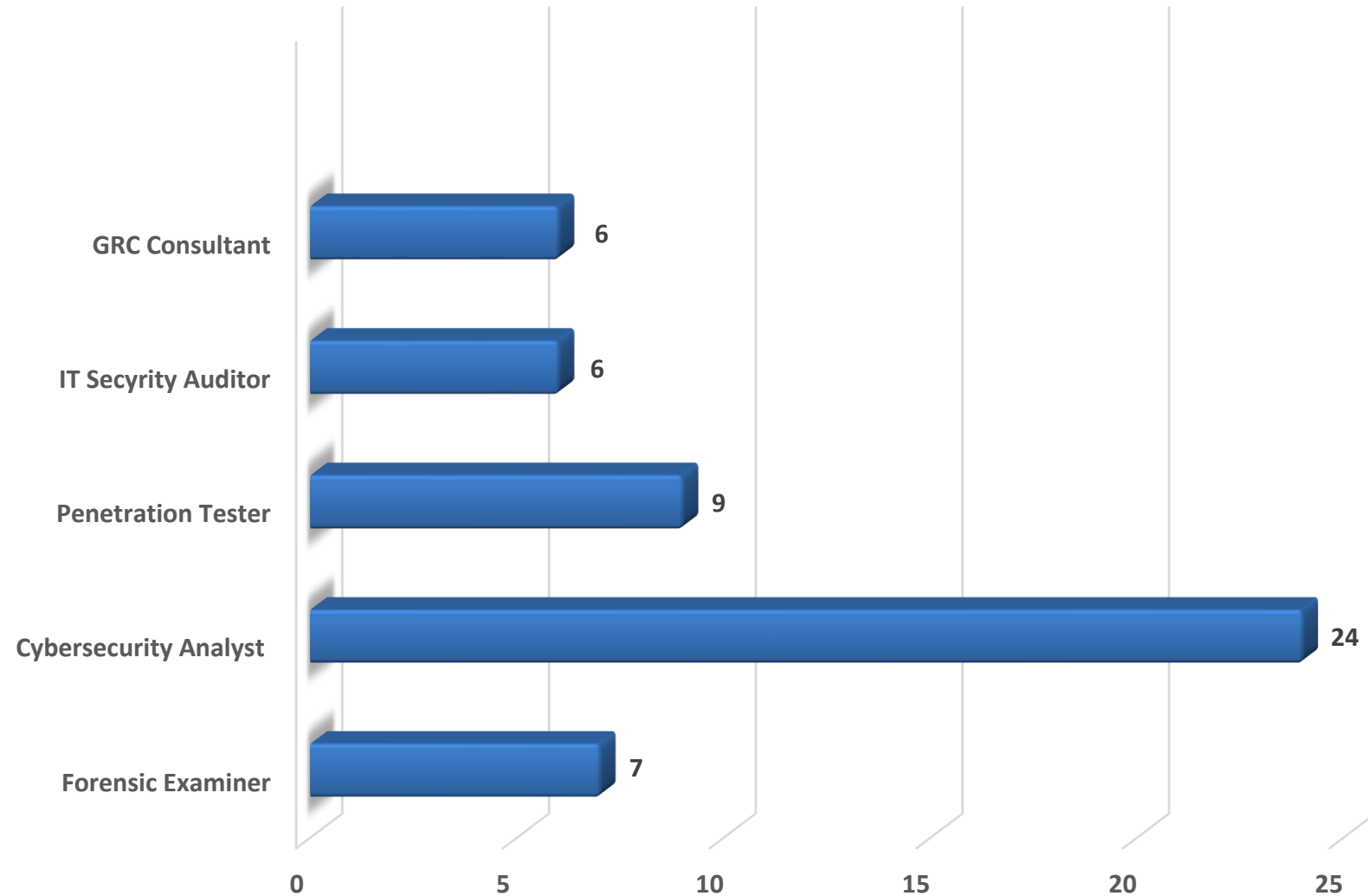
- Autonomy
- Competence
- Relatedness



# Project Milestones



# 1<sup>st</sup> Knowledge Test Results



# Intervention Resources

- Online course
- Tutorials
- Videos
- Presentations
- Cybersecurity standards



**OWASP** PROJECTS CHAPTERS EVENTS ABOUT

## WSTG - Latest

Home > Latest > 3-The OWASP Testing Framework

### Penetration Testing Methodologies

#### Summary

- [OWASP Testing Guides](#)
  - [Web Security Testing Guide \(WSTG\)](#)
  - [Mobile Security Testing Guide \(MSTG\)](#)
  - [Firmware Security Testing Methodology](#)
- [Penetration Testing Execution Standard](#)
- [PCI Penetration Testing Guide](#)
  - [PCI DSS Penetration Testing Guidance](#)
  - [PCI DSS Penetration Testing Requirements](#)
- [Penetration Testing Framework](#)
- [Technical Information Security Testing and Assessment Testing Methodology Manual](#)

**DIGITAL FORENSIC INVESTIGATION**

week1 Introduction  
1. Introduction to the course

SP 800-86

## Guide to Integrating Forensic Techniques into Incident Response

Date Published: August 2006

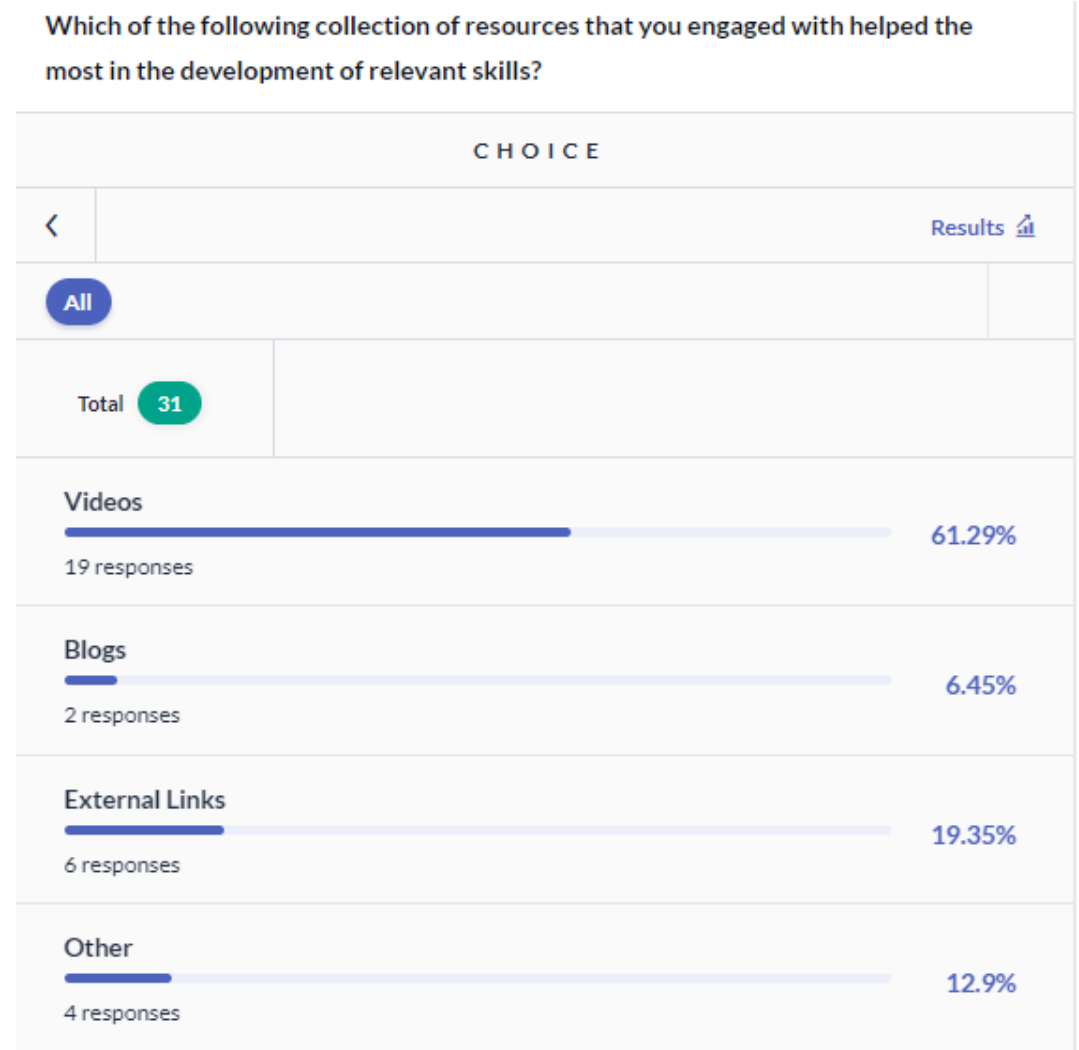
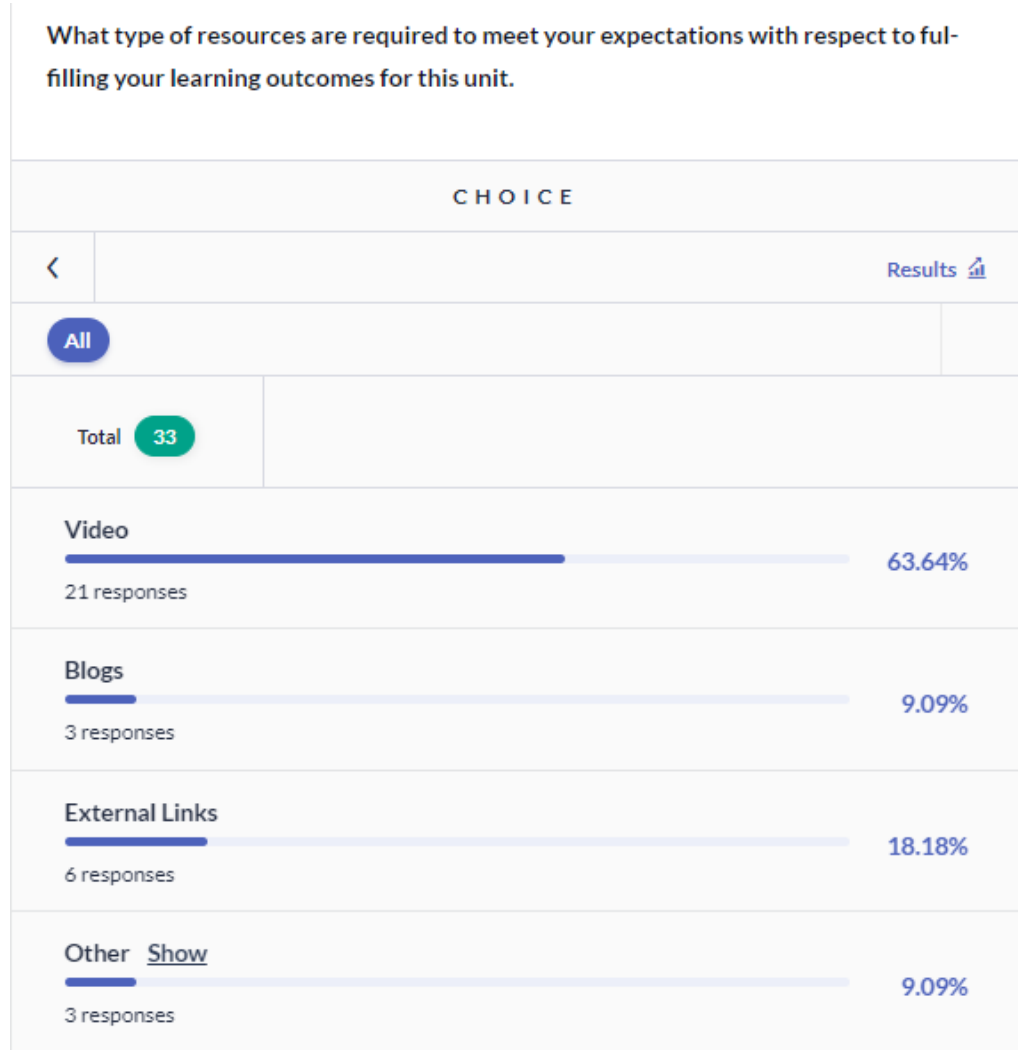
**Author(s)**  
Karen Kent (NIST), Suzanne Chevalier (BAH), Tim Grance (NIST), Hung Dang (BAH)

Table of contents

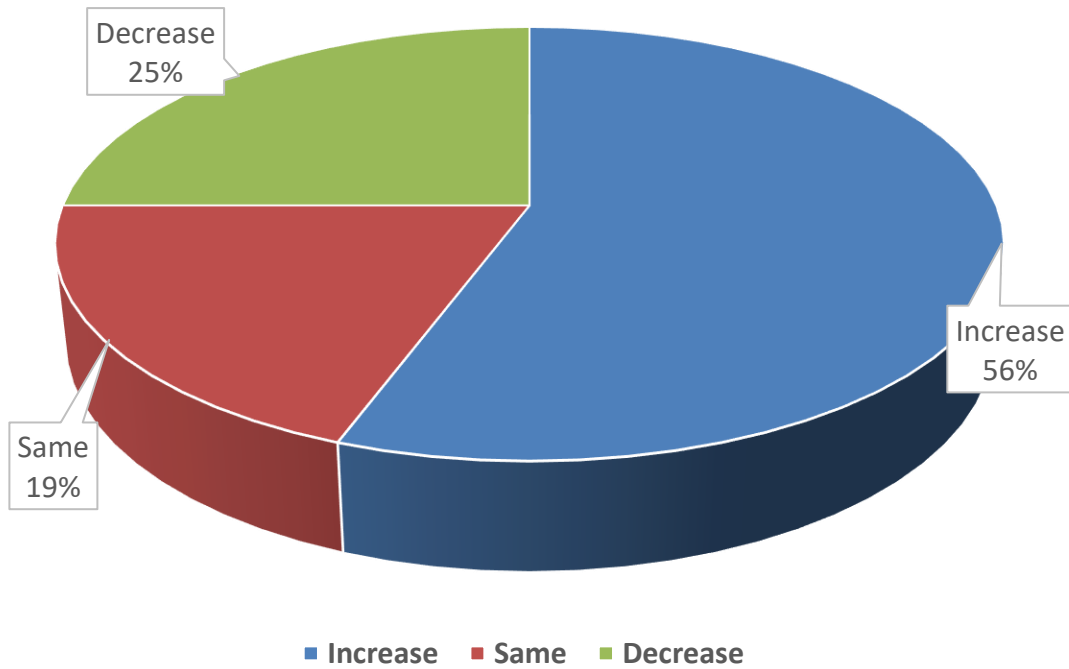
1. [Forensic Examiner Resources](#)
2. [Cybersecurity Analyst](#)
3. [Penetration Tester](#)
4. [IT Security Auditor](#)
5. [GRC Consultant](#)



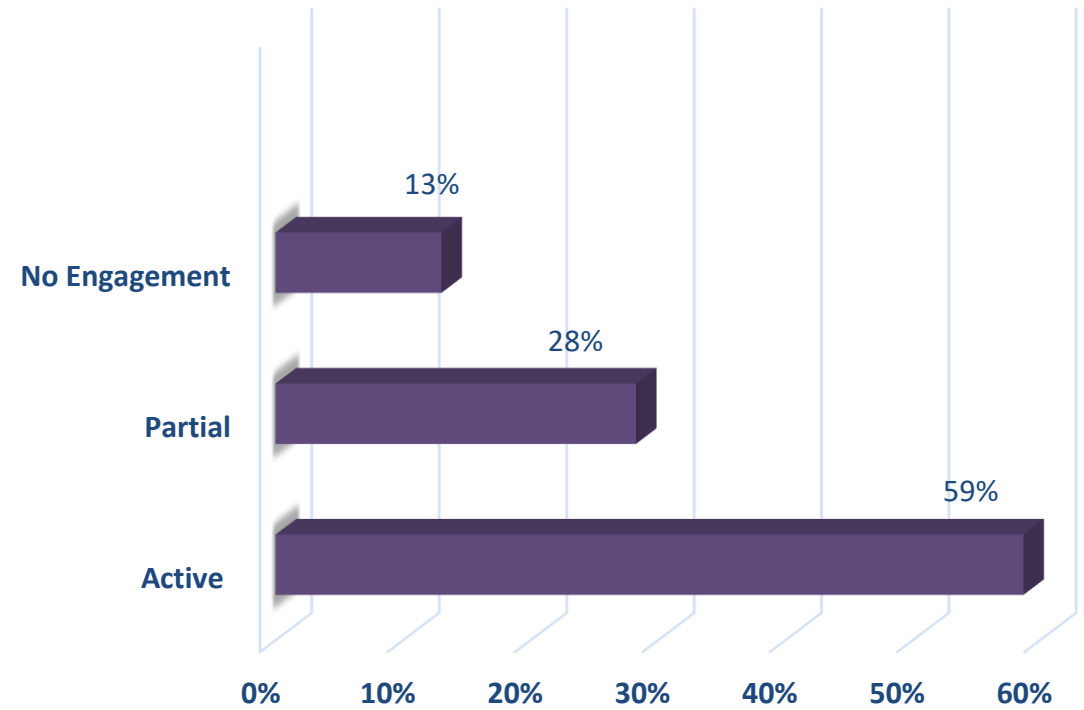
# Expectation Survey Results



# 2<sup>nd</sup> Knowledge Test Results



## Participation



# Limitations

- Learning resources
- Mostly theoretical
- Participation
- Preliminary results
- Partial view

# Ongoing Plan

- Thorough Analysis
- More user friendly resource design
- Embed practical activities
- Experiment with year 3 and postgrad units

**Thanks for your attention!**



[kamanashis.biswas@acu.edu.au](mailto:kamanashis.biswas@acu.edu.au)