# Author

## document_25257364-45a6-48d9-b63d-7e96834e619a

Turnitin

### Document Details

Submission ID
trn:oid:::1:3416939292

Submission Date
Nov 18, 2025, 11:43 PM GMT-5

Download Date
Nov 18, 2025, 11:43 PM GMT-5

File Name
tmplqgw3l9_.docx

File Size
22.0 KB

6 Pages

1,471 Words

8,685 Characters

# 0% detected as AI

The percentage indicates the combined amount of likely AI-generated text as well as likely AI-generated text that was also likely AI-paraphrased.

**Caution: Review required.**

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

## Detection Groups

**0** AI-generated only 0%
Likely AI-generated text from a large-language model.

**0** AI-generated text that was AI-paraphrased 0%
Likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

**Disclaimer**
Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely AI generated as AI generated and AI paraphrased or likely AI generated and AI paraphrased writing as only AI generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

## Frequently Asked Questions

**How should I interpret Turnitin's AI writing percentage and false positives?**
The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

**What does 'qualifying text' mean?**
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

# Final Report

# Potential Research Projects for a Simulated ICT Internship

Course Unit:

College:

Student Name:

Student ID:

Submitted to:

Submitted by:

Date:

## Introduction

The simulated ICT internship helped me understand in the way an organisation handles digital solutions and addresses technical issues. Although it was not an actual working environment, the simulation revealed realistic problems, which are encountered in ICT performance. The issues that were highlighted during the tasks were slow and manual processing of support tickets and unsafe digital behaviour by employees. These problems may interfere with operations, cause delays and increase security risks.

Based on these observations, this report focuses on two project ideas. First, automating and analyzing the incident management process to accelerate delays and improve the accuracy of the process. Second, Digital cybersecurity awareness training program to improve the behaviour of the staff and minimise security incidents involving human factors. This report explains each idea with concerning major problem area, advantages, and the process that would be required to initiate every project.

## Idea 1: Improving the Incident Management System through Automation and Analytics

Incident management process involved a lot of manual work. The staff members had the responsibility of sorting, categorising and assigning tickets manually which delay the process and create confusion. These challenges indicated that the organisation needed a more effective and structured way of dealing with incidents. My initial project idea focuses on automation and analytics in improving this process. Automation sort out the incoming tickets, designate them to the right personnel and send notifications in case response time is slow. With the help of analytics, it is possible to detect recurrent issues, monitor the performance, and help managers understand what aspects of the system should be improved.

Peralta, et al (2025) explained that intelligent automation models help in handling incidents more efficiently because they analyse patterns and minimise the manual decision-making. Similarly, Remil, et al (2024) described that, AIOps (Artificial Intelligence to IT Operations) is able to identify the problems at an early stage, categorize incidents and facilitate quicker. This shows

analytics tools assist ICT teams to know why issues occur and how they develop. Spring (2022) identified that human judgment along with automated tools improve efficiency and minimize the workload of the staff. This confirms the fact that automation and analytics may cooperate to build a more trustful system.

One of the advantage of this that management get quick response which bring user satisfaction and decreased daily work interruptions. Time will be saved on sorting tickets manually and they focus more on technical issues. Automation minimizes wrong classification errors, and the analytics assists to identify the recurring problems and eliminate the roots cause. This create more stable ICT environment with less recurring issues.

It has also some limitation. There needs to be efficient and accurate data in the automation systems for operating. The use of AIOps should be properly configured to prevent false alarms or incorrect forecasts Remil et al. (2024). The other issue is that employee members should be trained to operate the new system successfully. Automation replaces human but they know how to supervise and control automated activities.

The organisation needs to start this project by reviewing the current incident workflow. This involves determining the activities that take the longest time and errors that happen most frequently. Then, the basic automation capabilities like automatic ticket routing or priority can be deployed. Subsequently, analytics dashboards may be implemented to monitor the ticket count, response time, and system malfunctions. A small group of staff should be used in a pilot test so that the issues can be identified before expanding the system. The organisation then implement developed automation program and make their tasks easier.

## Idea 2: Developing a Digital Cybersecurity Awareness Training Platform

The second major issue experienced in the simulated ICT internship was the unsafe digital behaviour of staff. Employees opening suspicious emails, weak passwords, or not using the safety measures in tasks. These behaviours put the organisation in danger even with effective technical security systems. The second project will focus on creating a cybersecurity awareness training platform in digital form. This platform teaches the staff valuable security practices, trains them on

how to identify threats and to change their behaviour with time. Short lessons, real examples, quizzes, and reminders can be considered as training modules.

Hadlington (2017) explained security incidents is the human behaviour, and risky online actions that are misunderstood by staffs. This shows that training minimizes impulsive decision and improve judgment. Similarly, Parsons et al. (2017) describe that effective cybersecurity training enhances knowledge and minimizes errors. This indicates that the digital learning tools assist employees in learning the main issues related to phishing, password safety, and secure data handling. This clearly highlights the need for digital platform that is constantly updated and will involve employees in learning.

The training offers several advantages by providing practical and convenient education to the employees. The platform will be able to monitor the progress, detect those areas where the employees fail, and provide reminders in case of new risks.

There are also some limitations. The employees might not attend the training without knowing the importance. Awareness programs cannot be successful without motivation Alshaikh (2020). The training material should be applicable to real life scenarios at the workplace. The other concern is to update the content with the emerging threats. Parsons et al. (2017) caution that the outdated training materials is less effective. It is also necessary that organisations provide support of the training by clear policies and commitment of the leaders to enhance the impact.

The organisation should start this project by identifying the most common risky behaviours among the employees. Online platform must be created for brief lessons, videos, and examples. A test group of employees would be able to test the platform to give feedback. Once the pilot version is done, the full version may be rolled out to the entire staff. The material must be updated on a regular basis and employees reminded and new learning modules provided to keep them in touch.

## Discussion

Both project ideas focused on improving the ICT environment of the organisation with different aspects. Idea 1 improves technical processes by automating and using analytics, and Idea 2 enhances human behaviour by training. The two concepts mitigate risk, enhance efficiency, and

lead to sustainable stability over the long term. The main similarity is that both focus on avoiding problems and creating reliable ICT environment. However, they are different in terms of approach. The efficiency of the system is in Idea 1, whereas the attention is paid to people and behaviour in Idea 2. Idea 1 is beneficial in the short term in terms of operational boost and idea 2 is beneficial in the long term in terms of security gains. They complement one another and contribute a balanced ICT strategy.

## Reflection

The simulated ICT internship helped me understand real-life ICT issues. I observed problems, analyse them and convert them into ideas about research projects. It shows me the interaction between technical systems and human behaviour within an organisation. Idea 1helped me understand the importance of automation and data and Idea 2 provide significance of constant learning and the behaviour of staff. This experience enhanced my skills of critical thinking and prepared me to work in the field of ICT in the future.

## Conclusion

These projects were focused based on challenges realized during the simulated ICT internship. The first proposal was to improve how incident management will be automated and analytical, and the second proposal was to develop a digital cybersecurity awareness training platform. Both have advantages to the organisation, and cover different areas ICT performance. They are used together to promote technical enhancement and human consciousness. These provide insight into future real life problem solving scenario in ICT environment.

## Reference

Alshaikh, M 2020, 'Developing cybersecurity culture to influence employee behaviour: A practice perspective', *Computers & Security*, vol. 98, article 102003. Available from: https://doi.org/10.1016/j.cose.2020.102003

Hadlington, L 2017, 'Human factors in cybersecurity: examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours', *Heliyon*, vol. 3, no. 7, e00346. Available from: https://doi.org/10.1016/j.heliyon.2017.e00346

Paralta, A, Olivas, JA, Romero, FP & Navarro-Illana, P 2025, 'Intelligent Incident Management Leveraging Artificial Intelligence, Knowledge Engineering, and Mathematical Models in Enterprise Operations', *Mathematics*, vol. 13, no. 7, article 1055. Available from: https://doi.org/10.3390/math13071055

Parsons, K, Calic, D, Pattinson, M, Butavicius, M & McCormac, A 2017, 'The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies', *Computers & Security*, vol. 66, pp. 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Remil, Y, Bendimerad, A, Mathonat, R & Kaytoue, M 2024, *AIOps Solutions for Incident Management: Technical Guidelines and a Comprehensive Literature Review*, arXiv preprint. Available from: https://arxiv.org/abs/2404.01363

Spring, M 2022, 'How information technology automates and augments work: A model for human–machine collaboration in professional service', *Journal of Organizational Computing and Electronic Commerce*. Available from: https://doi.org/10.1002/joom.1215