Research Methods Module - Reflective Piece

What: Description of Experience

This module developed research competencies that I did not expect to find relevant to my current role as Director of Cloud Services. My day to day work focuses on SRE and platform reliability, and while security is part of what my team handles, I would not describe our approach as proactive. We respond to incidents and meet compliance requirements, but strategic security thinking has not been central to how I operate. This module changed that perspective.

The coursework progressed from ethics discussions through quantitative methods to a literature review and research proposal. Discussion 1 examined the ACM Malware Disruption case, where security professionals deployed a counter worm against a malicious hosting provider. Discussion 2 analysed research integrity through Abi's dilemma on selective data reporting. Units 7 and 8 covered inferential statistics and data visualisation, requiring hypothesis testing and chart creation with written interpretations.

The literature review examined cloud security risks, drawing on Correa et al.'s (2023) analysis of 200 AI governance documents. My research proposal investigated how conflicting pressures between deployment velocity and security compliance create undocumented APIs. I proposed the ASTAM framework (Agile Zero Trust Alignment Model), combining governance matrices with automated policy enforcement. I chose this topic because I wanted to explore what gap AI and automation could fill in cloud services, and focusing on security seemed like it would give me a concrete angle to work with.

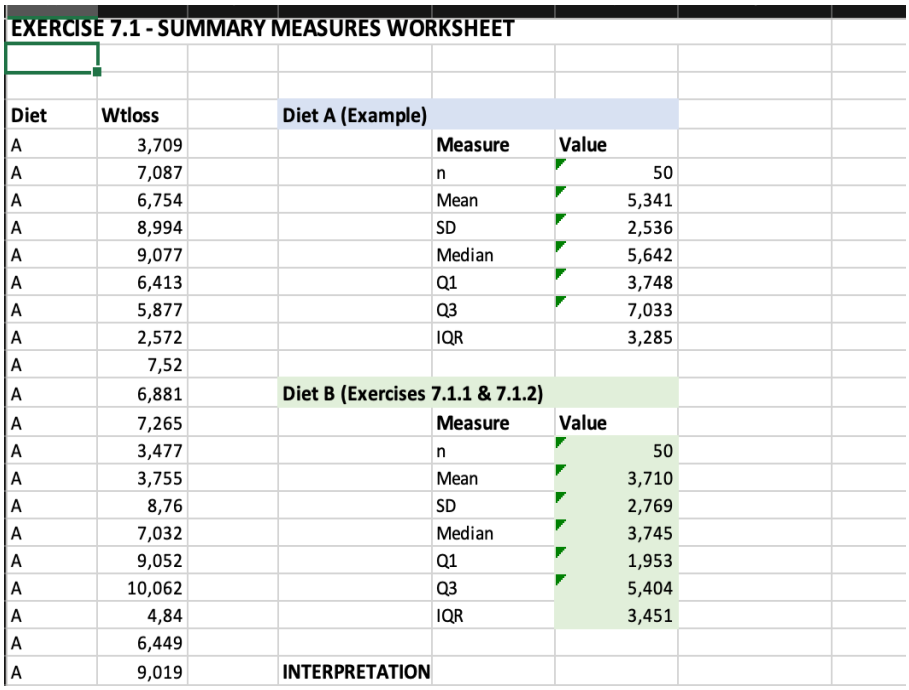
So What: Analysis and Interpretation

Emotional Response and Behavioral Analysis

The literature review process was where things clicked for me. Reading through academic sources on cloud security, I kept recognising problems my team deals with regularly. Misconfigured access controls, unclear ownership between platform and application teams, security practices that slow down deployment. These are not unique to my organisation. The research showed me that these patterns are well documented across the industry, yet most companies are not doing much to address

them structurally. That realisation was frustrating but also motivating. It suggested that meaningful improvement is possible if someone actually applies what the research recommends.

The statistics exercises were difficult at first. I found the material hard to digest and felt behind compared to where I thought I should be. Determining when to use a paired versus independent t test, understanding what the F test actually measured, interpreting p values correctly. None of it came naturally. I had to spend extra time with Berenson, Levine and Szabat (2019) working through examples before the logic started making sense. By the end of Unit 8, I could complete the exercises confidently, but I remember the early frustration clearly.



EXERCISE 7.1 - SUMMARY MEASURES WORKSHEET

Diet	Wtloss		Diet A (Example)		
A	3,709			Measure	Value
A	7,087			n	50
A	6,754			Mean	5,341
A	8,994			SD	2,536
A	9,077			Median	5,642
A	6,413			Q1	3,748
A	5,877			Q3	7,033
A	2,572			IQR	3,285
A	7,52				
A	6,881		Diet B (Exercises 7.1.1 & 7.1.2)		
A	7,265			Measure	Value
A	3,477			n	50
A	3,755			Mean	3,710
A	8,76			SD	2,769
A	7,032			Median	3,745
A	9,052			Q1	1,953
A	10,062			Q3	5,404
A	4,84			IQR	3,451
A	6,449				
A	9,019		INTERPRETATION		

Figure 1: Unit 7 Summary Measures worksheet demonstrating statistical analysis skills

Reflecting on my behaviour during the ethics discussions, I noticed I wanted clear rules to follow. The malware disruption case frustrated me because both sides had valid arguments. Protecting users from a malicious network seemed obviously good, but bypassing legal authorisation to do it violated principles I also believed in (Holzer and Lerums, 2016). Sitting with that tension rather than resolving it felt uncomfortable. I am used to making decisions and moving on, not dwelling in ambiguity. The module pushed me to accept that some professional situations genuinely do not have clean answers.

What Produced My Learning

The tutor feedback on my literature review was particularly useful. One suggestion was to extend the synthesis to include comparative evaluation between sectors or deployment models, such as public versus hybrid cloud. I had not thought to structure the analysis that way, and it exposed a gap in how I was approaching the material. I was treating cloud security as a single domain when the risks and mitigations actually differ significantly depending on architecture choices. This is something I want to explore further, potentially comparing how organisations with different deployment models handle the velocity versus security tension I examined in the research proposal.

Reading sequence mattered. Engaging with Correa et al. (2023) after the ethics discussions showed that the gap between principles and implementation I observed in individual cases exists at global governance level. The research found that 91.6% of AI governance documents are non-binding, and over half fail to define what they mean by AI. This connected directly to what I see at work, where security policies exist on paper but enforcement mechanisms are weak or absent. Creswell and Creswell (2018) on mixed methods then helped me design a research approach that could investigate both the measurable prevalence of workarounds and the human reasons behind them.

Evidence of Skills and Knowledge Developed

Statistical analysis capability improved substantially. The completed worksheets in Units 7 and 8 demonstrate that I can now select appropriate tests, formulate hypotheses, and interpret results correctly. More importantly, I can evaluate statistical claims in research papers rather than accepting conclusions uncritically. This matters for my role because vendor reports and industry surveys often present statistics that do not hold up under scrutiny.

Critical evaluation developed through the literature review. Moving from summarising sources to synthesising arguments required examining assumptions and positioning claims within broader debates. The questionnaire critique in Unit 6, analysing the System Usability Scale, reinforced this by requiring me to identify design limitations in a widely used instrument rather than accepting its validity at face value.

Research design skills emerged from the proposal development. Understanding how to structure a mixed methods study, anticipate ethical considerations, and design data collection instruments gives me a framework for approaching problems systematically rather than relying on intuition alone.

Now What: Action Plan and Future Application

ASTAM Framework Implementation: I am already using elements from the research proposal to change how my team approaches DevOps procedures. The governance matrix concept from ASTAM provides a structure for mapping security checkpoints to sprint activities without creating the bottlenecks that push developers toward workarounds. This is an ongoing experiment, but early results suggest we can reduce undocumented configuration changes by making the approved path faster than the shortcut.

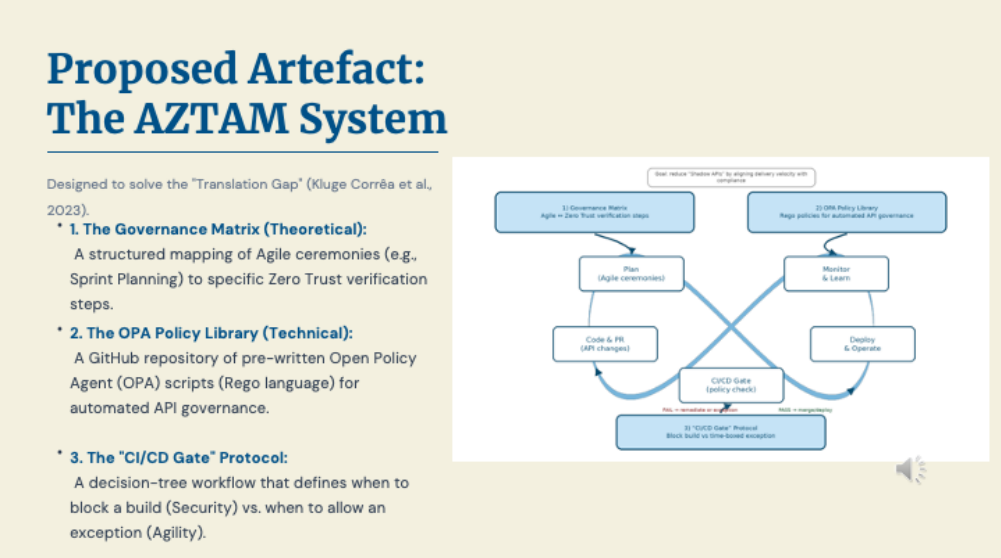


Figure 2: The ASTAM framework from my research proposal, now being piloted in my team's DevOps workflow

Comparative Deployment Analysis: Following my tutor's feedback, I want to extend the literature review analysis to compare security practices across public, private, and hybrid cloud deployments. My organisation uses a hybrid model, and understanding how our risk profile differs from pure public cloud implementations would inform better resource allocation for security investment.

Qualitative Skills Development: The research proposal requires interview analysis capabilities I have not yet developed. Over the next six months, I plan to complete

training in thematic coding, which will support both the academic research and my professional need to understand why teams make the security decisions they do.

References

Berenson, M.L., Levine, D.M. and Szabat, K.A. (2019) *Basic Business Statistics: Concepts and Applications*. 14th edn. Harlow: Pearson.

Correa, N.K., Galvão, C., Santos, J.W., Del Pino, C., Pinto, E.P., Barbosa, C., Massmann, D., Mambrini, R., Galvão, L., Terem, E. and de Oliveira, N. (2023) 'Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance', *Patterns*, 4(10), pp. 1-15.

Creswell, J.W. and Creswell, J.D. (2018) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th edn. London: SAGE Publications.

Dawson, C.W. (2015) *Projects in Computing and Information Systems: A Student's Guide*. 3rd edn. Harlow: Pearson.

Head, M.L., Holman, L., Lanfear, R., Kahn, A.T. and Jennions, M.D. (2015) 'The extent and consequences of p-hacking in science', *PLOS Biology*, 13(3), e1002106.

Holzer, G. and Lerums, J. (2016) 'The ethics of hacking back: Weighing the options', *Journal of Cybersecurity*, 2(1), pp. 37-48.

Saunders, M.N.K., Lewis, P. and Thornhill, A. (2019) *Research Methods for Business Students*. 8th edn. Harlow: Pearson.