1. **Project Title**

A framework for prioritising security compliance control outputs in a public cloud environment.

1. **Significance/Contribution to the discipline/Research Problem**

The increased use of public cloud for business workloads has led to the need for custom security compliance controls (policies & guardrails) that are tailored to internal standards, unlike standard benchmarks, such as CIS. CIS has a two level system that has been translated into severity ratings by public cloud providers for easier prioritisation of compliance issues on their platforms. However, there appears to be a lack of standardisation in the CIS ratings between public cloud providers and no framework to reference with regards to rating custom policies in order to prioritise outputs.

CIS - <https://www.cisecurity.org/cis-benchmarks/>

1. **Aims and Objectives**

The overall aim is to create a versatile rating framework that could be used for cloud infrastructure non-compliances in a similar way to how CVSS is utilised for vulnerabilities. As a non-compliance does not always constitute a vulnerability, a new framework is required to ensure this is considered.

The underlying objectives of the framework include:

* The standardisation of compliance control ratings across public cloud platforms for use in businesses leveraging a multi-cloud strategy.
* The standardisation of ratings between out-of-the-box, e.g. CIS, and custom security compliance controls to ensure clarity around business priorities and compliance reporting.
* Allow businesses to tailor control severity ratings to consider the business impact of non-compliance events in their public cloud environments, based on the presence of critical business processes for example.

1. **Key literature related to the project**

CVSS Scoring: <https://www.first.org/cvss/>

OWASP Risk Rating: <https://owasp.org/www-community/OWASP_Risk_Rating_Methodology>

1. **Description of artefact(s) that will be created (if applicable)**

A usable framework, preferably a programme where a user can input values and receive a rating for the control.