5.2.1.1 CRIPAL

CRIPAL is an acronym the author has established to cover the following high level 'primary' security goals (the following definitions are the author's own): -

- C = Confidentiality – The restriction of information and/or assets (both physical and logical) to authorised entities/individuals only.

- R = Reliability – The ability to access and use information and/or assets (both physical and logical) consistently without disruption

- I = Integrity – The maintaining of information and/or assets (both physical and logical) in their complete and intended form.

- P = Privacy – The ability for an entity/individual to choose with whom to share their 'Private' information and/or assets (both physical and logical), without concern of impermissible access and/or use.

- A = Availability – Constant and timely access to information and/or assets (both physical and logical) for authorised entities/individuals.

- L = Legitimate Use – Use of information and/or assets (both physical and logical) is undertaken by authorised entities/individuals who have the legal rights to conduct actions through propriety.

A vulnerability will be characterised by one or more of the letters of this acronym that relate to the specific categories above, e.g., if the vulnerability exposes Confidentiality as a weakness, a "C" will be placed in the CRIPAL column.

5.2.1.2 STRIDE

STRIDE is a method used by Microsoft [19] to help categorise threats during software development. In the context of this project, STRIDE helps to add a low level granularity to the previous 'CRIPAL' column. Similarly to CRIPAL above, any of the letters that make up the STRIDE acronym can be used as an entry within the TVAC table.

The STRIDE acronym is explained in more detail through Table 2 below: -

STRIDE Categories	STRIDE Definition	More Common Interpretations
(**S**)poofing	Using another person's authentication information, such as User ID & Password.	Authentication, Masquerade, Man in the Middle.
(**T**)ampering (**R**)epudiation	Malicious modification of data. Users who deny performing an action. Non-repudiation refers to the ability of a system to counter repudiation threats.	Integrity Violations. Non-Repudiation.
(**I**)nformation Disclosure	Information/data exposure to individuals who are not supposed to have access to it.	Confidentiality and/or Privacy Violation.
(**D**)enial of Service	Deliberate attempt to prevent legitimate users from using a service or system.	DOS (Denial or Disruption of service), DDOS. Reliability & Availability Violation.
(**E**)levation of Privilege	Where an unprivileged user gains privileged access. An example of privilege elevation would be an unprivileged user who contrives a way to be added to the Administrators group.	Access Control. Permissions and Rights Violation.

Table 2. STRIDE Table.