|  |  |  |
| --- | --- | --- |
| **Objective** | **Basic Controls** | **Specific Item** |
| E1 – Scope for Use | PR.03 - Understand Requirements | PR.03.10 – Functional requirements for the HLMA should be specified. These should define what the HLMA is supposed to do and should be appropriate to the scope. |
|  |  | PR.03.20 – Non-functional requirements of the HLMA should be specified. These should define how the HLMA operates and some requirements should be related to the 5 facets of trustworthiness: Safety; Reliability; Availability; Resilience; and Security (TSFdn, 2016). |
|  |  | PR.03.40 – Use cases should be understood and documented. These should outline how the user interacts with the HLMA and there should be focus on what the software does. |
| E2 – Coding Practices | TE.02 – Make appropriate tool choices | TE.02.20 – All code produced for the HLMA should be writing according to a coding standard to ensure there is consistency. |
|  | TE.03 – Follow structured design | TE.03.30 – Any code libraries/components that are being re-used should be checked they are from a trusted source. |
|  | TE.05 – Seek trustworthy realisation | TE.05.65 – All code components that are sourced externally should be checked for malware. |
|  | TE.07 – Practice hygienic coding | TE.07.10 – Ensure that all data being inputted into the HLMA is validated, i.e., ensure that the user cannot submit malicious syntax when using the app to update user information (profile details or tracker items) |
|  |  | TE.07.25 – Ensure that all data being outputted by the HLMA is validated. By default, sensitive user information should not be visible on a user profile. |
|  |  | TE.07.35 – Make sure that there are consistent camel case notation being used throughout the code. |
| E3 – Use Tools Effectively | TE.02 – Make appropriate tool choices | TE.02.10 – Choose a programming language that is suitable for mobile development and document the risks associated with this language. |
|  | TE.08 – Use methodological production | TE.08.30 – Production tool checking features should be enabled and used for debugging/monitoring of the HLMA |
| E4 – Defect Management | PR.07 – Maintain defect management | PR.07.10– All defects identified during the realisation of the HLMA should be recorded onto a Trustworthy Software Defect and Deviation List (R-TSDDL) and assessed quickly. |
|  | PR.07 – Maintain defect management | PR.07.20– Any defects identified once the HLMA is live should still be recorded onto a R-TSDDL and patched as soon as possible through a defined process. |
|  | TE.08 – Use methodological production | TE.08.30 – All errors, warning and exceptions generated by the production tool should always be fixed before the HLMA goes live. |
| E5 – Artefact Management | PH.02 – Understand requirements | PH.02.10 – Ensure that a GitHub repository is setup for the version control. This should be privately accessible. |
|  | PR.06 – Perform trusted software asset management | TE.03.30 – Ensure that there are regular reviews for all software artefacts. They should be protected and the version history should be up to date. |
|  | TE.09 – Perform internal pre-release review | TE.09.50 – A Trustworthy Software Release Notice (TSRN) should be produced and approved by the project manager. This should include how the facets of trustworthiness were considered during requirements specification, development, and release. |