Checklist for Developing Artificial Intelligence - Machine Learning Software

Configuration Management (CM)

- Is the AI/ML constituent life-cycle data managed according to configuration management principles?

  - ○ Versioning: [ ] Yes [ ] No
  - ○ Baselining: [ ] Yes [ ] No
  - ○ Change control: [ ] Yes [ ] No
  - ○ Reproducibility: [ ] Yes [ ] No
  - ○ Problem reporting: [ ] Yes [ ] No
  - ○ Archiving and retrieval: [ ] Yes [ ] No
  - ○ Retention period: [ ] Yes [ ] No

Quality/Process Assurance (QA)

- Are quality/process assurance principles applied to the development of the AI-based system?

  - ○ Independence level: [ ] Yes [ ] No

Reuse Assessment (RU)

- Has an impact assessment been performed before incorporating a trained ML model into an AI/ML constituent?

  - ○ Considered factors: [ ] Yes [ ] No

- Has a functional analysis been performed to confirm the adequacy of a COTS ML model to the requirements and architecture of the AI/ML constituent?

  - ○ Result: [ ] Yes [ ] No

- Have unused functions of a COTS ML model been analyzed and prepared for deactivation?

  - ○ Result: [ ] Yes [ ] No

Surrogate Model (SU)

- Has the accuracy and fidelity of the reference model been captured to support verification of the accuracy of the surrogate model?

  - ○ Result: [ ] Yes [ ] No

- Have additional sources of uncertainties linked with the use of a surrogate model been identified, documented, and mitigated?

  - ○ Result: [ ] Yes [ ] No

Explainability (EXP)

- Has the list of stakeholders requiring explainability been identified, along with their roles, responsibilities, and expected expertise?

  ○ Stakeholders: [ ] Yes [ ] No

- Have the needs for explainability been characterized to support development and learning assurance processes?

  ○ Result: [ ] Yes [ ] No

- Are methods in place at AI/ML item and/or output level satisfying specified AI explainability needs?

  ○ Result: [ ] Yes [ ] No

- Can the AI-based system deliver an indication of the level of confidence in AI/ML constituent output?

  ○ Result: [ ] Yes [ ] No

- Can the AI-based system monitor that its inputs are within specified operational boundaries?

  ○ Result: [ ] Yes [ ] No

- Can the AI-based system monitor that its outputs are within specified operational performance boundaries?

  ○ Result: [ ] Yes [ ] No

- Can the AI-based system monitor that AI/ML constituent outputs are within specified operational level of confidence?

  ○ Result: [ ] Yes [ ] No