tmforum checklist

AI PROCUREMENT

- [ ] Stakeholders identified and engaged.[1]
- [ ] Conduct ethical assessment prior to initiating procurement.[2]
- [ ] Verify that the planned procurement is aligned with organisational policies relating to AI.
- [ ] Assess performance targets for AI system.[3]
- [ ] Address rights and licensing issues especially where the client is supplying training data to the vendor.
- [ ] Ensure a mechanism is available to support traceability of delivered models and any inherited artefacts.
- [ ] Agree responsibilities for 'digital safety testing'.[4]
- [ ] Identify requirements for model explainability and interpretability for this procurement.
- [ ] Consider whether the environmental costs of model training and operation are justified.
- [ ] Confirm the vendor is legally qualified to sell in the intended region/industry.
- [ ] Identify and address any regulatory and statutory restrictions on the type of software being acquired.
- [ ] Seek compliance with TM Forum AI Management Standards.
- [ ] Obtain Model Data Sheet as part of the delivery.[5]

tmforum guidance

AI PROCUREMENT

1. **Chain of custody** It's important to establish a chain of custody that will run throughout all stages of the AI lifecycle. At each stage, everyone involved should be able to identify their immediate upstream and downstream stakeholders. Certain roles may still be required at end-of-life in order to handle any subsequent issues and enquiries that arise.

2. **Ethical assessment** This should determine that the proposed application is reasonable, proportionate, safe, and respects relevant legislation.

3. **Performance targets** In many cases it will be possible to determine, up-front, what level of performance is required from the system for it to be useful and cost-effective.

4. **Digital Safety Testing** It should be possible to demonstrate to regulators and other stakeholders that testing has taken place to ensure that the AI system is free from significant flaws such as bias, confounding, susceptibility to adversarial attack and data poisoning.

5. **Model data sheet** The vendor should provide documentation of the key features of the AI system (eg purpose, provenance, performance, safety and limitations). Ideally this should be provide in a consistent format such as the TM Forum's Model Data Sheet.

tmforum checklist

AI PRE-DEVELOPMENT

- [ ] Stakeholders identified and engaged.[1]
- [ ] Conduct ethical assessment prior to initiating development.[2]
- [ ] Verify that the planned development is aligned with organizational policies relating to AI.
- [ ] Identify requirements for model explainability and interpretability for this procurement.
- [ ] Consider whether the environmental costs of model training and operation are justified.
- [ ] Training and validation data obtained with appropriate quality. Provenance established and recorded. Data secured for future availability.
- [ ] Inherited artefacts identified and provenance recorded.[6]
- [ ] Suitably qualified team assembled.[7]
- [ ] Data tests conducted to address coverage, accuracy (eg of labelling), potential for poisoning.[8]
- [ ] Assess performance targets for AI system.[3]
- [ ] Create baseline model.[9]
- [ ] Test and validation protocols created and peer reviewed.[10]
- [ ] Create a Digital Safety test plan.[4]

tmforum guidance

AI PRE-DEVELOPMENT

1 **Chain of custody** It's important to establish a chain of custody that will run throughout all stages of the AI lifecycle. At each stage, everyone involved should be able to identify their immediate upstream and downstream stakeholders. Certain roles may still be required at end-of-life in order to handle any subsequent issues and enquiries that arise.

2 **Ethical assessment** This should determine that the proposed application is reasonable, proportionate, safe, and respects relevant legislation.

3 **Performance targets** In many cases it will be possible to determine, up-front, what level of performance is required from the system for it to be useful and cost-effective.

4 **Digital Safety Testing** It should be possible to demonstrate to regulators and other stakeholders that testing has taken place to ensure that the AI system is free from significant flaws such as bias, confounding, susceptibility to adversarial attack and data poisoning.

6 **Inherited artefacts** This means pre-existing AI components that are being used to build the system, eg models / model weights being used for transfer learning, word embeddings etc.

7 **Qualifications** In addition to technical qualifications, it may be appropriate to consider whether the development team is representative of the communities likely to be affected by the AI system. In other words, do they have a shared interest in ensuring correct and non-discriminatory functioning of the system?

8 **Data testing** It may be appropriate to document the risks arising from the outcome this testing so they are visible and can be addressed at other stages in the development.

9 **Baseline model** Where appropriate, consideration should be given to creating a simple baseline model whose performance can be used in setting targets for subsequent development in terms of cost and effectiveness.

10 **Test & Validation** Ideally the protocols for testing and validating performance of an AI system should be established early on and be subject to independent review with the aim of identifying and eradicating issues with treatment of data, data leakage, proxy outcomes etc. The key here is to 'cross-check' and obtain a diversity of views.

tmforum checklist

AI POST-DEVELOPMENT

- [ ] Stakeholders identified and engaged.[1]
- [ ] Test plans validated and completed.[11]
- [ ] Test plans validated and completed.[12]
- [ ] AI Model issue/defect list recorded.[13]
- [ ] Scope and type of behavioural variation documented.[14]
- [ ] Appropriate AI operational warrants have been obtained from the development team, signed off and are recorded in well know location or repository.[15]
- [ ] Complete a Model Data Sheet for the finished AI system.[5]
- [ ] Known deployment list created and recorded.[16]

tmforum guidance

AI POST-DEVELOPMENT

1 **Chain of custody** It's important to establish a chain of custody that will run throughout all stages of the AI lifecycle. At each stage, everyone involved should be able to identify their immediate upstream and downstream stakeholders. Certain roles may still be required at end-of-life in order to handle any subsequent issues and enquiries that arise.

2 **Ethical assessment** This should determine that the proposed application is reasonable, proportionate, safe, and respects relevant legislation.

5 **Model data sheet** The vendor should provide documentation of the key features of the AI system (eg purpose, provenance, performance, safety and limitations). Ideally this should be provide in a consistent format such as the TM Forum's Model Data Sheet.

11 **Test plan completion** Testing declared in the pre-development stage should be checked for completion and recorded as done if appropriate. Deltas to the test plan should be validated and recorded.

12 **Development review** The development process and outcome for this model should be reviewed and an overview of the process along with important decisions taken during the process and any lessons learned should be documented and recorded. The review should be conducted whether or not the outcome was successful.

13 **Model issues & defects** Perfect projects are unusual; a list of known defects and fixes (if undertaken) should be created and maintained for the model. This should be available for inspection by all deployment owners, and should be available to be amended in light of deployment experience.

14 **Behavioural variation** Some systems may have predefined behavioural variation programmed in and some have adaptive or online learning components. This expectation and the drivers for it should be recorded and retrievable.

15 **AI operational warranty** Constraints and limitations on the safe operation of the model should be declared.

16 **Deployment tracking** Preparations should be made to track deployments of the model. In due course this will include those currently in use and those that have been withdrawn.

tmforum checklist

AI DEPLOYMENT

- [ ] Stakeholders identified and engaged.[1]
- [ ] Confirm development history is preserved.[17]
- [ ] Confirm all testing has been completed.
- [ ] Confirm AI operational warranty is in place and is consistent with planned deployment.[18]
- [ ] Define and agree AI model contract and ensure this is enforceable.[19]
- [ ] Where appropriate, ensure a model fail-safe mechanism is in place.[20]
- [ ] Establish end-of-life plan.[21]
- [ ] Verify that the planned deployment is aligned with organisational AI policy.
- [ ] Confirm all regulatory considerations on data access, privacy and geographic restrictions on where systems and data can be run or moved have been addressed.

tmforum guidance

AI DEPLOYMENT

1 **Chain of custody** It's important to establish a chain of custody that will run throughout all stages of the AI lifecycle. At each stage, everyone involved should be able to identify their immediate upstream and downstream stakeholders. Certain roles may still be required at end-of-life in order to handle any subsequent issues and enquiries that arise.

17 **Development history** All elements necessary to reproduce the system should be stored and discoverable based on the identity of the system to be deployed. Test plans and results should also be preserved so it can be understood what aspects of the systems were tested and how it performed.

18 **AI warranty** The planned deployment should be consistent with the limits and constraints declared in the AI operational warranty. If this is not the case, mitigating actions to manage the risks should be in place and documented.

19 **AI model contract** A 'contract' identifying dependencies and constraints for the safe and correct operation of the AI system should be in place. The system implementation should provide the means to validate and enforce the contract (eg by supporting the TM Forum AI Management APIs).

20 **Fail-safe** Where the model can mobilize resources independently, measures need to be developed to stop a potential runaway.

21 **End-of-life plan** The end-of-life requirements for this system should be documented prior to deployment. This should identify retention periods for all historical information relating to the system (eg development history, chain-of-custody, audit logs).

tmforum checklist

AI IN-LIFE 

- [ ] Stakeholders identified and engaged.[1]
- [ ] Confirm AI operational warranty is still valid.[22]
- [ ] Confirm defects, incidents and failures since last review have been recorded.
- [ ] Conduct review of AI model performance.[23]
- [ ] Solicit and record views of stakeholders.
- [ ] Review and update AI model contract.[24]

tmforum guidance

AI IN-LIFE 

1 **Chain of custody** It's important to establish a chain of custody that will run throughout all stages of the AI lifecycle. At each stage, everyone involved should be able to identify their immediate upstream and downstream stakeholders. Certain roles may still be required at end-of-life in order to handle any subsequent issues and enquiries that arise.

22 **AI operational warranty review** Checks should be undertaken to ensure the warranty remains consistent with the deployment and that any violations have been investigated.

23 **AI performance review** Defects, incidents and failure should be investigated and the ongoing performance of the system reviewed to check that continues to operate adequately and safely.

24 **AI model contract review** It is to be expected that changes to the AI model contact will be necessary during the life of the system. In any case the contract should be checked periodically to ensure it remains appropriate and is being properly enforced.

tmforum checklist

AI END OF LIFE

- [ ] Stakeholders identified and engaged.[1]
- [ ] All deployment instances checked and confirmed as closed and impact on dependent systems checked.[25]
- [ ] Items recorded in development checklists are secured and available for review as appropriate in line with organisational policy.
- [ ] All in-life reviews completed and in-life review process stopped.[23]
- [ ] System stakeholders interviewed and stakeholder views recorded as per In-life checklist and aggregated for review.
- [ ] Confirm all local, regional, company and international data retention and model retention requirements have been considered and met.
- [ ] End of life review conducted as appropriate, key issues identified and recorded.[26]
- [ ] Appropriate interventions in organisation policy and practice identified and actioned.[26]
- [ ] Project recorded as closed.

tmforum guidance

AI END OF LIFE

1 **Chain of custody** It's important to establish a chain of custody that will run throughout all stages of the AI lifecycle. At each stage, everyone involved should be able to identify their immediate upstream and downstream stakeholders. Certain roles may still be required at end-of-life in order to handle any subsequent issues and enquiries that arise.

23 **AI performance review** Defects, incidents and failure should be investigated and the ongoing performance of the system reviewed to check that continues to operate adequately and safely.

25 **Dependent systems** As well as checking that all deployed instances have been shutdown, an important check here is that all dependent systems have been identified and the impact on these is understood.

26 **End of life review** This should be based on the end of life plan (created at deployment time. It is also an opportunity to review key events in the life of the AI system and extract any relevant learning for the organisation, in particular where changes or improvements to organisation AI policy and practice have been identified.