Workplace AEDT Checklist

Last Updated: October 17, 2024

☐ Engage key stakeholders to gather input, buy in, and engagement

- Talent/recruiting
- HR
- Legal
- Privacy
- IT
- Sales
- Applied Science SMEs
- Leadership / Sponsorship
- Accessibility
- Procurement
- Cybersecurity
- Facilities
- Customer support
- Public Policy
- Internal Audit

☐ With key stakeholders, develop workflows or processes for workplace AI/ML models, applications, and systems including how they will be reviewed, approved, and assessed

- Decide on role of the key stakeholders – decision-making body, information sharing, governance, etc.
- Identify points of contact for each stakeholder group and who needs to sign off at what stage.
- Agree on intake tool/template and process, including estimated timelines for review
- Agree on process, including who will review what and when, and how you will determine and classify the risk of the application. If creating different risk levels there may be different review paths
- Identify, track applicable laws and regulations and where they will impact stakeholder business, processes
    - Provide regular updates to key stakeholders
    - Keep Public Policy in the loop for suggestions on improvements to bills
- Identify technical requirements for monitoring risks and enforcing internal policies and processes (Bias testing, toxicity, etc.)
- Agree on steps for business owner to obtain approval for new models, systems
- Develop plan for how to determine what AIML is currently launched – this can include
    - Surveying different business lines
    - Prohibited Use case check (working backwards from Feb 2 for EU AIA)
    - Edge cases – what could fall into this but doesn't really
    - Repository for information
    - Annual baselining / update process to ensure nothing new comes through without knowledge (checks and balances).
- Develop business requirements for when and how to conduct risk assessments
    - How and where is the information documented

    - What assessments are needed (AI risk assessments, including conformity assessments (as necessary), data protection or privacy risk assessments, security assessments, ethics assessments, bias assessments, etc.)
    - Who signs off and accepts the risk (legal vs business team)
- After review and approval, how are mitigating measures tracked to completion, what are the deadlines for model improvements, what does baselining look like (monthly/annual)
    - How are remediations tracked and reported
    - How will escalations be addressed, handled
    - Who is responsible for monitoring and addressing non-conforming AI, responding to internal and external reports

☐Draft and implement an AI policies and/or guidelines

- Align to stakeholder agreement
- May need to be use case specific; identify prohibited and high-risk use cases
- Consider how to manage development vs deployment of AI models, systems
- Consider activities beyond HR and IT
- Develop guardrails to enable the business
- Determine either a cadence for review and update or decision to keep policy high-level, as AIML innovation moves faster than some policies can be updated.

☐ Identify existing internal policies, guidelines that can be updated to help manage workplace AI risk

- Data classification and handling policies
- Procurement policies
- Social media policies
- IT and Electronic communications monitoring policies
- Training data policies – acceptable use
- Ad hoc policies, for example 'Recording, Transcription, and Summarization'

☐ Review existing applicant and employee notices to determine whether updates for AI/ML use cases are necessary – consider especially:

- Automated decision making with legal impact
- Profiling
- Processing sensitive personal data, including opt-in and opt out requirements
- Model training (including vendor training) on applicant/employment data
- Disclosures regarding bias testing
- Individual rights

☐ Develop policies, guidance for addressing where and how notice of AI/automated decision-making and consent/choice requirements are required to be disclosed (e.g. for applicants, workers where consent may be required)

- Identify stakeholders (e.g. employment legal, HR, talent, vendor)
- Develop approved language and procedures for requesting changes

- Document where are consent/choice is stored
- If consent is required, work with teams to understand how withdrawal of consent will work

☐ Develop guidelines, playbooks for procurement

- Update RFP questions to address AI for workplace, HR systems (bias testing, audits, risk management procedures, etc.)
- Contract clauses to address developer vs deployer obligations
- Vendors rights in processing applicant/worker data for training purposes
- Data retention policies

☐ Develop and implement AI training and awareness targeted at the workplace

- Consider role-based training for HR, IT, and Procurement to address workplace specific AI
- Annual retraining
- New Hire training