TEMPLATE

Learning Implementation Roadmap Checklist

A practical, vendor-neutral template for validating an AI and machine learning implementation roadmap before production use. Covers scope, data readiness, baseline approach, validation, security, deployment, and operational handoff with evidence, owners, and acceptance criteria.

Learning Implementation Roadmap Checklist

Use this template to review an AI or machine learning implementation roadmap before production use.

Purpose: verify that the roadmap is ready for controlled release by checking scope, data readiness, model approach, validation, security, deployment, and operational ownership.

How to use this checklist

- Review phase by phase during planning, design review, model approval, and pre-production signoff.
- Mark each item as Pass / Fail / Blocked.
- Capture evidence for every item.
- If a check fails, revise the roadmap before proceeding.

Review record

- Project / model name: _____
- Version: _____
- Reviewer(s): _____
- Date: _____
- Decision: ? Pass ? Pass with conditions ? Blocked ? Fail
- Next review date: _____

Phase 1: Scope and problem definition

Goal: confirm the roadmap solves a clearly defined operational problem and that the learning task matches the intended use case.

Checklist

Check	Status	Evidence / Notes	Owner
Confirm the business or operational problem is written as a measurable outcome, not a vague aspiration.	? Pass ? Fail ? Blocked		
Review the target users, upstream systems, and downstream actions that will consume the model output.	? Pass ? Fail ? Blocked		
Validate that the learning task type matches the use case, such as classification, regression, ranking, forecasting, or anomaly detection.			
Document the exact decision the system will support and the decision that remains under human control.	? Pass ? Fail ? Blocked		
Assign a named owner for scope approval and change control.	? Pass ? Fail ? Blocked		
Review whether the roadmap includes explicit non-goals to prevent scope creep.	? Pass ? Fail ? Blocked		

Evidence to capture

Record the problem statement, use-case diagram, decision boundaries, and owner signoff. If the implementation affects regulated or security-sensitive workflows, capture the approval path and any control requirements that apply.

Acceptance criteria

The roadmap passes this phase only if the objective is measurable, the model task is appropriate, and the human/system boundary is clear. A pass should leave no ambiguity about what success looks like or who is responsible for changes.

Common mistakes

- Describing the roadmap in technical terms without stating the operational decision it supports.
- Allowing multiple target outcomes to share one model plan, which makes validation and acceptance criteria too vague.

Phase 2: Data readiness and lineage

Goal: verify that the roadmap accounts for data availability, quality, provenance, and access controls before training starts.

Checklist

Check	Status	Evidence / Notes	Owner
Confirm all required data sources are identified and mapped to their owners.	? Pass ? Fail ? Blocked		
Review data freshness, completeness, and known quality defects for each source.	? Pass ? Fail ? Blocked		

Validate that training data and inference data are representative of the expected production population.	? Pass ? Fail ? Blocked	
Document where labels come from, how they are generated, and whether label quality has been reviewed.	? Pass ? Fail ? Blocked	
Assign access controls for sensitive or restricted fields used in training or evaluation.	? Pass ? Fail ? Blocked	
Review whether data retention, masking, and deletion requirements are documented.	? Pass ? Fail ? Blocked	
Validate lineage from source to feature to training set to evaluation set.	? Pass ? Fail ? Blocked	

Evidence to capture

Capture schema descriptions, sample extracts, data quality reports, lineage diagrams, label definitions, and access review evidence. If the data includes personal or confidential information, record the handling controls and approvals.

Acceptance criteria

This phase passes only when the roadmap shows that the data is available, lawful or authorized for use, sufficiently stable, and traceable end to end. If lineage cannot be explained, the implementation is not ready for production planning.

Common mistakes

- Assuming training data quality is sufficient because the sample notebook ran successfully.
- Ignoring population drift risk when the data source feeding production differs from the historical dataset.

Phase 3: Baseline, model approach, and experiment plan

Goal: confirm the roadmap specifies a realistic model strategy and a baseline for comparison.

Checklist

Check	Status	Evidence / Notes	Owner
Confirm the roadmap defines a baseline approach, such as rules, heuristics, or a simpler statistical model.	? Pass ? Fail ? Blocked		
Review the candidate model family and document why it fits the data shape, latency needs, and operational constraints.	? Pass ? Fail ?		
Validate that the experiment plan includes reproducible training inputs, hyperparameter controls, and version tracking.	? Pass ? Fail ?		
Document assumptions about feature availability at inference time.	? Pass ? Fail ? Blocked		
Assign ownership for experiment tracking, model artifact storage, and version promotion.	? Pass ? Fail ? Blocked		
Review whether the plan avoids features that would leak future information or unavailable context.	? Pass ? Fail ? Blocked		

Evidence to capture

Keep the baseline definition, experiment matrix, configuration snapshots, feature list, and model version identifiers. If external libraries or managed services are involved, capture the dependency version or service setting that affects behavior.

Acceptance criteria

The roadmap passes when the proposed approach is justified against the baseline and the experiment plan is reproducible. The model must not depend on training-only features or undocumented assumptions about runtime inputs.

Common mistakes

- Treating the first model that improves a metric as production-ready.
- Failing to document which features are unavailable in production, which can create silent training-serving skew.

Phase 4: Validation, metrics, and signoff rules

Goal: ensure the roadmap defines how quality will be measured and what conditions allow release.

Checklist

Check	Status	Evidence / Notes	Owner
Confirm the roadmap defines primary and secondary metrics aligned to the business outcome.	? Pass ? Fail ? Blocked		
Review threshold values for acceptance, including minimum performance and maximum allowed error or false-positive rate.	? Pass ? Fa		
Validate that evaluation data is separate from training data unless an alternate validation method is explicitly justified.	? Pass ? Fai		
Document any segment-level checks needed for important user groups, regions, classes, or traffic patterns.	? Pass ? Fail ? Blocked		
Assign a reviewer for metric interpretation and release recommendation.	? Pass ? Fail ? Blocked		
Review whether the plan includes robustness checks for missing data, edge cases, and adversarial or malformed inputs where relevant.			
Validate that the roadmap defines a fail condition, not just a target score.	? Pass ? Fail ? Blocked		

Evidence to capture

Store evaluation reports, confusion matrices or equivalent outputs, threshold justification, and segment analysis. If the use case is safety- or security-relevant, capture the review notes that explain why the selected acceptance criteria are sufficient.

Acceptance criteria

The roadmap passes only if metrics map directly to the operational objective, thresholds are explicit, and failure conditions are written in advance. Release approval should be possible without interpretation debates.

Common mistakes

- Relying on one aggregate metric and missing poor performance on a critical segment.
- Setting a target score without defining what happens if the model misses it by a small margin.

Phase 5: Security, privacy, and misuse controls

Goal: verify that the implementation roadmap accounts for risks introduced by data access, model behavior, and integration points.

Checklist

Check	Status	Evidence / Notes	Owner
Confirm the roadmap identifies sensitive data classes and the controls applied to them.	? Pass ? Fail ? Blocked		
Review whether access to training data, model artifacts, and inference endpoints is restricted by role.	? Pass ? Fail ? Blocked		
Validate that secrets, keys, and credentials are stored and rotated through approved controls.	? Pass ? Fail ? Blocked		
Review whether prompt injection, data poisoning, model extraction, or other misuse scenarios have been considered where relevant.	? P		

Confirm privacy controls for minimization, masking, retention, and deletion are documented and enforceable.	? Pass ? Fail ? Blocked		
Validate that any external service, API, or library dependency has been reviewed for security impact.	? Pass ? Fail ? Blocked		
Confirm incident response steps exist for data exposure, model misuse, or unauthorized access.	? Pass ? Fail ? Blocked		

Evidence to capture

Capture security review notes, access control records, dependency review results, privacy approvals, and incident response links. If the model interacts with privileged workflows, record the abuse cases considered and the corresponding mitigations.

Acceptance criteria

The roadmap passes when the security and privacy controls are explicit, enforceable, and matched to the actual risk profile of the system.

Phase 6: Deployment, rollback, and operational handoff

Goal: confirm the roadmap defines how the model will move into production safely and who owns it afterward.

Checklist

Check	Status	Evidence / Notes	Owner
Confirm the rollout plan includes deployment stages, gates, or a phased release strategy.	? Pass ? Fail ? Blocked		
Review rollback criteria and the mechanism for reverting to a previous model or fallback logic.	? Pass ? Fail ? Blocked		

Validate that monitoring covers performance, data drift, latency, error rates, and service health.	? Pass ? Fail ? Blocked	
Confirm alert thresholds and response owners are documented for quality degradation or system failure.	? Pass ? Fail ? Blocked	
Review retraining triggers, change management, and approval requirements for future model updates.	? Pass ? Fail ? Blocked	
Confirm the operational team has runbooks, support contacts, and escalation paths.	? Pass ? Fail ? Blocked	
Validate that ownership transfers from the build team to the runtime support team are explicit.	? Pass ? Fail ? Blocked	

Evidence to capture

Capture deployment plan, rollback steps, monitoring dashboard references, alert definitions, runbooks, and operational signoff. Include any post-launch review schedule or maintenance obligations.

Acceptance criteria

The roadmap passes only if the team can deploy, monitor, recover, and operate the system without relying on undocumented tribal knowledge.

Common mistakes

- Assuming deployment success means operational success.
- Failing to define rollback criteria before launch.
- Leaving monitoring responsibilities unclear after handoff.

Final release decision

Use the table below to summarize phase outcomes.

Phase	Result	Notes
Scope and problem definition	? Pass ? Pass with conditions ? Blocked ? Fail	
Data readiness and lineage	? Pass ? Pass with conditions ? Blocked ? Fail	
Baseline, model approach, and experiment plan	? Pass ? Pass with conditions ? Blocked ? Fail	
Validation, metrics, and signoff rules	? Pass ? Pass with conditions ? Blocked ? Fail	
Security, privacy, and misuse controls	? Pass ? Pass with conditions ? Blocked ? Fail	
Deployment, rollback, and operational handoff	? Pass ? Pass with conditions ? Blocked ? Fail	

Final recommendation

- Approve for production use when all phases pass and any conditions are documented.
- Block release when any phase is failed or blocked without an approved mitigation plan.

Final approver: _____

Approval date: _____

Quick review reminders

- A model that trains successfully is not automatically production-ready.
- Data lineage and access controls are part of readiness, not optional extras.
- Metrics must map to the business objective, not just a technical benchmark.
- Rollback and monitoring should be defined before launch, not after an incident.
- Ownership must be explicit from planning through operations.

Optional appendix: evidence log

Item	Link / Location	Notes
Problem statement		
Use-case diagram		
Data quality report		
Lineage diagram		
Baseline definition		
Experiment matrix		
Evaluation report		
Security review		
Deployment plan		
Rollback runbook		
Monitoring dashboard		
Operational handoff		