Post-Market Monitoring Plan Template

EU AI Act — Article 72 Compliance Framework

A practical Post-Market Monitoring Plan template designed for providers of high-risk AI systems under Regulation (EU) 2024/1689.

This document provides a structured framework for monitoring deployed AI systems, detecting operational risks, documenting corrective actions, and maintaining continuous compliance throughout the system lifecycle.

Annex IV-Aligned Monitoring Framework

- Incident Response Pipeline
- Compliance Documentation

Document Type
AI Compliance Template

Prepared by
AI Governance Desk

How to Use This Template

This document provides a structured template for establishing a Post-Market Monitoring Plan for high-risk AI systems under the EU Artificial Intelligence Act (Regulation (EU) 2024/1689). It is designed to support organizations in documenting monitoring procedures, operational oversight, and corrective response mechanisms once an AI system has been deployed in real operating environments.

The template aligns with the monitoring obligations outlined in Article 72 and the technical documentation requirements described in Annex IV of the Regulation.

Who Should Use This Template

This template is intended for organizations responsible for developing or placing high-risk AI systems on the European Union market. It is particularly relevant for providers that must demonstrate ongoing compliance with EU AI Act lifecycle governance requirements.

Typical users include AI developers, compliance and governance teams, risk management specialists, legal and regulatory departments, and organizations responsible for maintaining technical documentation supporting AI system conformity.

What This Template Helps You Do

The Post-Market Monitoring Plan outlined in this document provides a structured approach for tracking how AI systems perform once they are operating in real-world conditions.

The framework helps organizations establish monitoring processes, collect operational data, evaluate emerging risks, and document corrective actions when system performance deviates from expected outcomes. It also supports traceability, ensuring that monitoring activities can be demonstrated during regulatory review or market surveillance audits.

How to Complete the Monitoring Plan

Each section of this template should be completed using information specific to the AI system being monitored. Organizations should describe the monitoring mechanisms they operate, the data sources used to evaluate system performance, and the governance procedures used to assess monitoring results.

The objective is not simply to document monitoring activities, but to demonstrate that the organization maintains continuous visibility over system performance and can respond effectively to operational risks.

Structure of the Template

The template is organized to reflect the monitoring lifecycle expected under the EU AI Act. It guides organizations through documenting monitoring objectives, data collection mechanisms, performance indicators, escalation procedures, incident response workflows, and corrective action processes.

When completed, the monitoring plan should form part of the technical documentation package required under Annex IV and serve as operational evidence that the provider maintains a functioning post-deployment oversight system.

Table of Contents

This document provides a structured Post-Market Monitoring Plan template aligned with Article 72 of the EU Artificial Intelligence Act. The sections below guide organizations through documenting monitoring objectives, governance responsibilities, operational signals, incident handling, and audit-ready evidence required for high-risk AI systems.

Definitions and Key Terms

The following definitions clarify key concepts referenced throughout this Post-Market Monitoring Plan template. The terminology reflects the language used in Regulation (EU) 2024/1689 (EU Artificial Intelligence Act) and related lifecycle governance practices for high-risk AI systems.

Provider

The natural or legal person, public authority, agency, or other body that develops an AI system or has an AI system developed and places it on the market or puts it into service under its own name or trademark, in accordance with Regulation (EU) 2024/1689.

Deployer

A natural or legal person, public authority, agency, or other body that uses an AI system under its authority, except where the system is used in the course of a personal non-professional activity.

High-Risk AI System

An AI system classified as high-risk under the EU AI Act, typically because it is used in contexts that may significantly affect safety, fundamental rights, or important societal functions. These systems are subject to strict requirements under Title III, Chapter 2 of the Regulation.

Post-Market Monitoring

A structured and documented process through which providers continuously collect, review, and evaluate information about the performance and risk profile of an AI system after it has been placed on the market or put into service.

Monitoring Plan

A documented framework describing how post-deployment monitoring activities will be conducted, including data sources, monitoring metrics, governance procedures, escalation mechanisms, and corrective action processes.

Serious Incident

An incident or malfunctioning of an AI system that leads, or could potentially lead, to harm to health, safety, or fundamental rights, and which must be reported to relevant authorities in accordance with Article 73 of the EU AI Act.

Corrective Action

A measure taken by the provider to address identified risks or non-compliance issues in an AI system. Corrective actions may include model updates, retraining, system configuration changes, operational restrictions, or temporary suspension of system functionality.

Section A — System Overview

This section documents the basic identification and operational context of the AI system subject to post-market monitoring. The information provided here establishes the scope of monitoring activities and links the monitoring plan to the system described in the technical documentation required under Annex IV of the EU AI Act.

System Information Field	Description / Entry
AI System Name	
System Version / Model ID	
Provider Organization	
Intended Purpose of the AI System	
High-Risk Classification (Annex III Category)	
Deployment Environment (e.g., web platform, enterprise system, embedded device)	
Primary Users and Affected Persons	

Compliance Note

The information recorded in this section should correspond to the system description contained in the provider's technical documentation. Any material changes to system functionality, intended purpose, or deployment environment should trigger a review of the monitoring plan.

Section A • 01 — System Overview

This section captures additional operational and technical context necessary for effective post-market monitoring. The information recorded here helps aligns monitoring activities.
to the system's architecture, data flows, and operational deployment environment.

System Information Field	Description / Entry
Primary Deployment Locations (e.g., EU member states, internal enterprise environment)	
System Architecture Reference (link or reference to architecture documentation)	
Primary Data Inputs (e.g., structured data, sensor inputs, user-generated content)	
System Outputs / Decisions (e.g., predictions, classifications, recommendations)	
External Dependencies (e.g., APIs, third-party models, data providers)	
Related Technical Documentation (e.g., risk management file, model documentation, evaluation reports)	

Implementation Tip

Where possible, reference existing internal documentation rather than duplicating system descriptions. The monitoring plan should remain consistent with the technical documentation maintained under Annex IV of the EU AI Act.

Section B — Monitoring Objectives

This section defines the objectives and operational scope of the post-market monitoring system. The purpose is to ensure that the AI system continues to operate in accordance with regulatory requirements, expected performance levels, and the risk management framework established during system development.

Monitoring activities should focus on identifying performance degradation, emerging risks, bias patterns, operational anomalies, and safety concerns that may arise once the system is deployed in real-world environments.

Monitoring Objective	Description / Monitoring Focus
Safety Monitoring	**Detection of operational risks that could affect the health, safety, or rights of individuals interacting with or affected by the AI system.**
Performance Monitoring	**Continuous assessment of model accuracy, reliability, and stability during real-world deployment.**
Bias and Fairness Monitoring	**Identification of potential disparities or unintended bias across demographic or operational groups.**
Robustness and Drift Monitoring	**Detection of changes in input data distributions, concept drift, or environmental changes that may impact system performance.**
Security and Misuse Monitoring	**Observation of system misuse, adversarial inputs, or cybersecurity-related anomalies that may compromise system integrity.**

Scope Guidance

Monitoring activities should reflect the level of risk associated with the AI system and the contexts in which it is deployed. Providers should ensure that monitoring signals are capable of detecting operational risks that may emerge after deployment.

Section B • 01 — Monitoring Scope and Frequency

This section defines how monitoring activities are operationalized once the AI system is deployed. It describes the signals that are monitored, the frequency at which monitoring reviews occur, and the responsible roles assigned to evaluate monitoring outputs.

Monitoring schedules should reflect the level of risk associated with the system and the operational environments in which it is deployed.

Monitoring Signal	Monitoring Method	Review Frequency	Responsible Role
Model Performance Metrics	Automated monitoring dashboards and evaluation pipelines	Weekly or continuous monitoring	ML Operations Team
Input Data Distribution / Drift	Statistical drift detection and monitoring tools	Weekly review	Data Science Team
Bias and Fairness Indicators	Fairness evaluation metrics across	Monthly review	Responsible AI / Compliance Team
Operational Errors or System Failures	System logs, monitoring alerts, and error tracking systems	Continuous monitoring	Engineering Team
User Complaints or Deployer Feedback	Feedback channels, support tickets, or internal reporting tools	Monthly review	Product or Governance Team
Security and Misuse Signals	Security monitoring tools, anomaly detection, misuse detection	Continuous monitoring	Security / Risk Team

Monitoring Note

Monitoring frequencies should be reviewed periodically to ensure they remain appropriate for the operational risk profile of the AI system. High-risk deployments may require more frequent monitoring and faster escalation procedures.

Section B • 02 — Escalation Thresholds

This section defines the escalation thresholds used to determine when monitoring findings require investigation, internal escalation, or corrective action. Clear threshold criteria help ensure that operational risks are addressed promptly and that monitoring outputs translate into appropriate governance responses.

Escalation procedures should be proportionate to the nature of the monitoring signal, the severity of the risk identified, and the potential impact on health, safety, fundamental rights, or system reliability.

Monitoring Signal	Alert Condition	Escalation Action	Responsible Role
Model Performance Degradation	Accuracy or reliability falls below predefined performance threshold	Initiate model performance investigation and review system outputs	ML Operations Team
Data Distribution Drift	Significant shift detected in input data distribution or operational environment	Conduct drift analysis and assess whether retraining or recalibration is required	Data Science Team
Bias or Fairness Deviation	Fairness indicators exceed accepted disparity thresholds	Escalate to Responsible AI governance review and assess need for mitigation	Responsible AI / Compliance Team
Operational System Failure	Repeated system errors, interruptions, or degraded service availability	Initiate engineering diagnostics and remediation process	Engineering Team
Security or Misuse Event	Suspicious activity, adversarial behaviour, or potential system misuse detected	Escalate to security response procedures and risk management review	Security / Risk Team

Escalation Guidance

Escalation thresholds should be reviewed periodically to ensure they remain aligned with the operational risk profile of the AI system. Providers should also ensure that escalation procedures connect clearly with incident management, corrective action processes, and Article 73 reporting obligations where applicable.

Section C — Monitoring Data Sources and Signals

This section identifies the operational signals and data sources used to monitor the performance, reliability, and risk profile of the AI system once it has been deployed. Effective post-market monitoring depends on collecting signals from multiple technical and operational sources.

Monitoring inputs should provide sufficient visibility into system behaviour, enabling providers to detect emerging risks, operational anomalies, or unintended impacts that may arise during real-world use.

Signals should be collected from system telemetry, user feedback channels, operational logs, and external sources where relevant.

Data Source	Monitoring Signals Collected	Responsible Role
System Logs and Telemetry	**System errors, processing latency, usage metrics, system availability indicators**	**Engineering / ML Operations**
Model Evaluation Pipelines	**Model accuracy, confidence scores, prediction distributions, performance benchmarks**	**ML Operations Team**
Data Drift Monitoring Tools	**Changes in input data distributions, feature drift, environmental shifts**	**Data Science Team**
User Feedback Channels	**User complaints, operational feedback, reported anomalies**	**Product / Governance Team**
Customer Support Records	**Recurring user issues, operational complaints, service disruptions**	**Support Operations**
Security Monitoring Systems	**Suspicious activity, misuse attempts, adversarial interactions**	**Security / Risk Team**

External Sources and Societal Risk Signals

In addition to internal operational monitoring signals, organizations may also consider external sources of information when evaluating the real-world impact of deployed AI systems.

Article 72(2) of the EU AI Act refers to monitoring information that may arise from "other sources." These sources may provide insights into potential harms or risks that are not immediately visible through technical system monitoring alone.

Examples of external monitoring signals may include:

- User complaints and dispute mechanisms
- Customer support escalations
- Feedback from deployers or affected persons
- Findings from consumer protection organizations
- Regulatory inquiries or enforcement actions
- Independent research or expert analysis

Incorporating external monitoring signals can help organizations identify emerging risks affecting individuals or fundamental rights and strengthen lifecycle oversight of high-risk AI systems once deployed.

Compliance Insight

Post-market monitoring should not rely solely on technical system telemetry. Real-world risk signals often emerge through user feedback, complaints, regulatory inquiries, and independent oversight mechanisms.

Implementation Note

Monitoring signals should be aggregated through centralized monitoring dashboards where possible. Consolidating monitoring inputs improves visibility into system behaviour and allows providers to identify patterns or emerging risks that may not be visible from individual signals alone.

Section C • 01 — Monitoring Signal Classification

This section categorizes the monitoring signals collected from operational systems and defines how these signals are translated into measurable indicators. Establishing clear signal classifications helps ensure that monitoring outputs can be interpreted consistently and acted upon when risk thresholds are reached.

Monitoring signals should be mapped to defined performance metrics, evaluation thresholds, and responsible owners. This structure enables organizations to respond quickly when monitoring results indicate emerging operational risks.

Monitoring Signal	Metric / Indicator	Risk Threshold	Monitoring Owner
Model Accuracy	Accuracy score, prediction reliability	Accuracy drops below defined model performance threshold	ML Operations Team
Prediction Distribution	Changes in prediction patterns across inputs	Significant deviation from baseline distribution	Data Science Team
Input Data Drift	Statistical distribution of input features	Drift score exceeds defined drift tolerance	Data Science Team
System Reliability	Error rates, service availability, system uptime	Error rate or downtime exceeds operational tolerance	Engineering Team
User Feedback	Volume of complaints, reported anomalies	Spike in negative feedback or repeated issue reports	Product / Governance Team
Security Signals	Suspicious usage patterns or adversarial inputs	Confirmed misuse or abnormal security event	Security / Risk Team

Monitoring Guidance

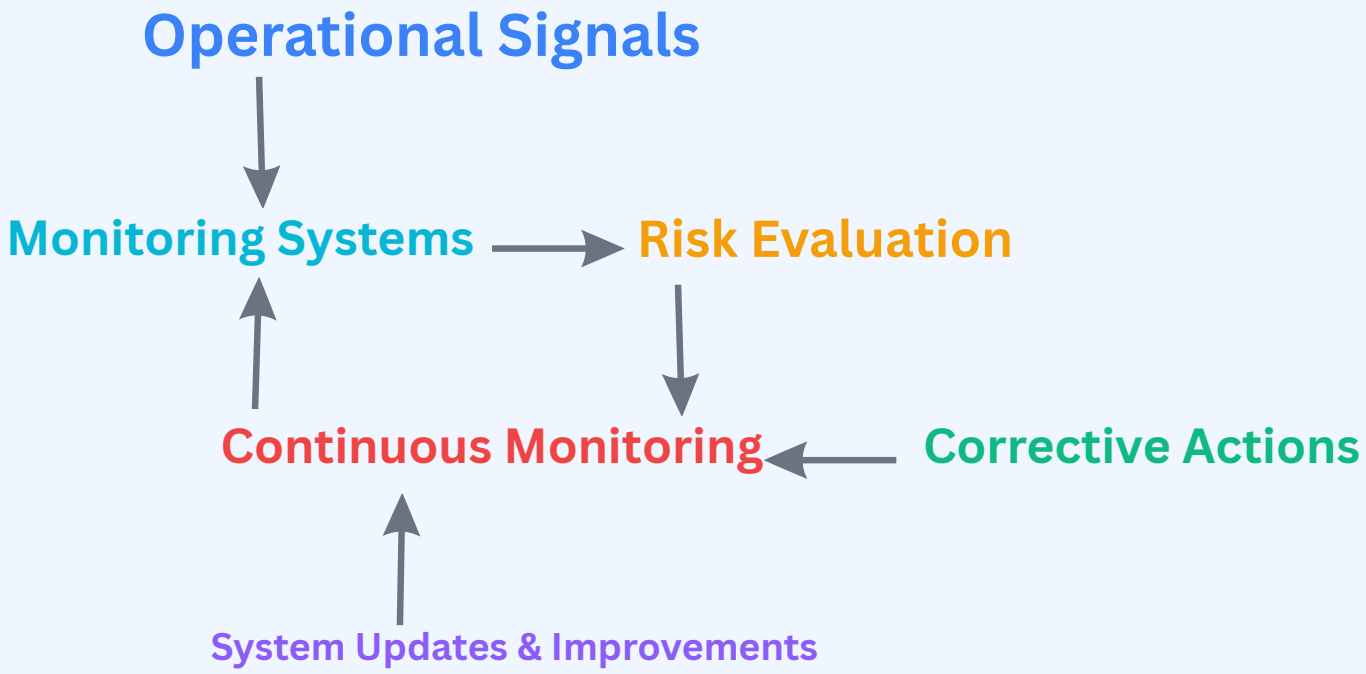
Signal classification frameworks should be reviewed regularly to ensure that monitoring metrics remain aligned with the operational behavior of the AI system. Changes in deployment context, system updates, or evolving user interactions may require adjustments to monitoring thresholds or signal interpretation.

Section C • 02 — Continuous Monitoring Feedback Loop

This section illustrates how monitoring signals are continuously collected, evaluated, and translated into operational responses throughout the lifecycle of a deployed AI system. Post-market monitoring is not a one-time activity; it is an ongoing feedback loop that enables providers to detect emerging risks, assess system performance, and apply corrective measures when necessary.

An effective monitoring framework connects operational signals, risk evaluation processes, and corrective actions in a continuous cycle. This ensures that the AI system remains aligned with regulatory expectations and continues to operate safely within its intended deployment environment.

AI System Monitoring Feedback Loop



The monitoring feedback loop illustrates how operational signals from deployed AI systems are continuously evaluated and translated into corrective actions. By maintaining this lifecycle, providers can detect emerging risks, update system controls, and ensure ongoing compliance with regulatory monitoring obligations.

Section C • 03 — Monitoring Documentation and Evidence

This section outlines the documentation and operational evidence that should be maintained to demonstrate the effective operation of the monitoring framework. Maintaining well-structured monitoring records enables providers to verify that monitoring processes are functioning as intended and that identified risks are appropriately addressed.

Monitoring documentation should capture system observations, evaluation outcomes, corrective actions, and governance decisions made throughout the lifecycle of the deployed AI system. These records support internal accountability and provide traceability during regulatory review or compliance audits.

Documentation Type	Description	Responsible Team
Monitoring Reports	**Periodic reports summarizing monitoring results, system performance indicators, and operational observations**	**ML Operations Team**
Drift Analysis Records	**Documentation of detected data drift, investigation findings, and evaluation outcomes**	**Data Science Team**
Incident Investigation Logs	**Records of operational incidents, root-cause analysis, and resolution actions**	**Engineering / Risk Teams**
Corrective Action Records	**Documentation of remediation steps taken to address identified system risks**	**Responsible AI / Governance Team**
User Feedback Records	**Logs of complaints, feedback, and reported anomalies from users or deployers**	**Product / Support Teams**
Security Monitoring Logs	**Records of suspicious activity, misuse attempts, and security investigations**	**Security / Risk Team**

Evidence Retention Guidance

Monitoring documentation should be retained in accordance with organizational record-keeping policies and regulatory requirements. Maintaining structured monitoring evidence ensures that providers can demonstrate the effectiveness of their monitoring framework and respond efficiently to regulatory inquiries or compliance assessments.

Section D — Metrics and Performance Thresholds

This section establishes the quantitative metrics used to evaluate the operational performance of the AI system and defines the thresholds that determine when corrective intervention may be required. Clear performance metrics allow providers to interpret monitoring signals consistently and assess whether the system continues to operate within acceptable parameters.

Performance thresholds should reflect the system's intended purpose, deployment context, and associated risk level. When monitoring results exceed defined tolerance limits, appropriate investigation or remediation actions should be initiated to maintain system reliability and regulatory compliance.

Metric Category	Performance Metric	Monitoring Method	Threshold Condition
Model Performance	Prediction accuracy and reliability	Automated model evaluation pipelines	Accuracy falls below defined performance baseline
Data Integrity	Input data quality and distribution stability	Statistical drift detection tools	Drift score exceeds defined tolerance level
Operational Reliability	System uptime, latency, and error rates	System monitoring dashboards and logs	Downtime or error rates exceed operational tolerance
Fairness and Bias	Disparity metrics across demographic groups	Fairness evaluation tools and bias testing	Fairness disparity exceeds acceptable threshold
User Impact	Volume and severity of user complaints	Feedback channels and support ticket analysis	Significant increase in negative user reports
Security Integrity	Detection of adversarial inputs or misuse	Security monitoring systems and anomaly detection	Confirmed misuse event or abnormal activity pattern

Performance Threshold Guidance

Threshold values should be reviewed periodically to ensure they remain aligned with the operational characteristics of the deployed AI system. Changes in data distributions, user interactions, or system updates may require adjustments to monitoring thresholds to maintain accurate risk detection.

Section D • 01 — Performance Monitoring Indicators

This section defines the key operational indicators used to track AI system performance during real-world deployment. Monitoring indicators translate system behavior into measurable signals that allow teams to assess whether the AI system continues to operate within expected performance boundaries.

These indicators provide early visibility into performance degradation, operational anomalies, or unexpected system behavior. Continuous observation of these indicators enables organizations to detect emerging risks and respond before issues escalate into operational or compliance concerns.

Indicator Category	Monitoring Indicator	Measurement Method	Responsible Team
Model Performance	Prediction accuracy trends, confidence levels	Automated model evaluation pipelines	ML Operations Team
System Reliability	Error rates, latency levels, uptime monitoring	Infrastructure monitoring tools and system logs	Engineering / Infrastructure Team
Data Stability	Input feature distribution and drift indicators	Statistical drift detection tools	Data Science Team
Fairness Monitoring	Bias metrics across demographic groups	Fairness evaluation frameworks and model audits	Responsible AI / Compliance Team
User Interaction Signals	User feedback patterns and complaint frequency	Feedback analysis and support ticket review	Product Governance Team
Security Monitoring	Suspicious usage patterns or adversarial inputs	Security monitoring tools and anomaly detection	Security / Risk Team

Indicator Interpretation Guidance

Monitoring indicators should be evaluated collectively rather than in isolation. Changes in one signal may reflect broader shifts in system behavior or operational context. Regular review of monitoring indicators ensures that organizations maintain visibility into emerging performance issues and can initiate investigation or remediation when necessary.

Section D • 02 — Risk Threshold Escalation Criteria

This section defines the escalation criteria used when monitoring indicators exceed defined performance thresholds. Escalation criteria ensure that monitoring outputs translate into timely investigation, governance review, or corrective action when operational risks emerge.

Clear escalation procedures help organizations respond consistently to abnormal system behavior and ensure that performance deviations are assessed before they affect system reliability, user safety, or regulatory compliance.

Escalation actions should be proportionate to the severity of the monitoring signal and aligned with the operational risk profile of the deployed AI system.

Monitoring Indicator	Threshold Trigger	Escalation Action	Responsible Team
Model Accuracy	Accuracy drops below defined performance baseline	Initiate model performance investigation and validation review	ML Operations Team
Prediction Distribution	Significant deviation from expected prediction distribution	Conduct model drift analysis and evaluate need for recalibration	Data Science Team
System Reliability	Error rate or service downtime exceeds operational tolerance	Initiate infrastructure diagnostics and system remediation	Engineering / Infrastructure Team
Fairness Metrics	Bias indicators exceed acceptable disparity thresholds	Escalate to Responsible AI governance review	Responsible AI / Compliance Team
User Complaint Signals	Rapid increase in user complaints or negative feedback	Initiate product review and incident assessment	Product Governance Team
Security Monitoring	Suspicious activity or adversarial interaction detected	Escalate to security response and risk management procedures	Security / Risk Team

Escalation Governance Guidance

Escalation thresholds should be reviewed periodically to ensure that monitoring triggers remain aligned with the operational characteristics of the deployed AI system. Organizations should ensure that escalation procedures are clearly connected to incident management processes, corrective action frameworks, and regulatory reporting obligations where applicable.

Section D • 03 — Corrective Response and Remediation Actions

This section outlines the corrective response procedures that should be initiated when monitoring indicators exceed defined thresholds and escalation criteria are triggered. Corrective actions ensure that identified risks are investigated, mitigated, and resolved in a structured and timely manner.

Effective remediation processes help organizations restore system reliability, maintain safe operation of AI systems, and demonstrate accountability in responding to operational risks. Corrective responses should be documented and integrated into ongoing monitoring and system improvement processes.

Corrective measures may include technical remediation, model retraining, system configuration updates, or governance review depending on the nature and severity of the identified issue.

Risk Event	Investigation Action	Corrective Response	Responsible Team
Model Performance Degradation	Conduct model performance analysis and validation testing	Retrain model, recalibrate parameters, or adjust deployment configuration	ML Operations Team
Data Drift Detection	Investigate input data distribution and feature drift patterns	Update training datasets or adjust preprocessing pipelines	Data Science Team
Operational System Failure	Diagnose infrastructure errors or system interruptions	Restore service availability and implement system reliability improvements	Engineering / Infrastructure Team
Fairness or Bias Deviation	Review fairness metrics and conduct bias evaluation	Adjust model training data or introduce fairness mitigation techniques	Responsible AI / Compliance Team
User Impact Escalation	Analyze complaint patterns and operational feedback	Implement product adjustments or revise user interaction workflows	Product Governance Team
Security or Misuse Event	Investigate suspicious activity and conduct security analysis	Deploy security patches, block malicious usage, or strengthen access controls	Security / Risk Team

Corrective Action Documentation Guidance

All corrective responses should be documented to ensure traceability and accountability. Documentation should capture the triggering event, investigation findings, corrective measures taken, and verification of system stability following remediation. Maintaining clear remediation records supports regulatory review and continuous improvement of the monitoring framework.

Section E — Monitoring Governance and Roles

This section defines the governance structure responsible for overseeing post-market monitoring activities. Effective governance ensures that monitoring outputs are properly reviewed, interpreted, and translated into operational decisions throughout the lifecycle of the deployed AI system.

Clear role allocation enables organizations to maintain accountability for monitoring processes, risk evaluation, escalation management, and corrective action implementation. Governance structures should ensure that monitoring responsibilities are distributed across technical, operational, and compliance functions.

Monitoring oversight should also include periodic review by responsible governance bodies to ensure that monitoring activities remain aligned with regulatory expectations and the operational risk profile of the AI system.

Governance Role	Primary Responsibility	Monitoring Function	Accountability Scope
ML Operations Team	Monitor model performance and operational indicators	Track prediction accuracy, confidence trends, and model reliability	Technical monitoring and system stability
Data Science Team	Analyze model behavior and data distribution patterns	Detect data drift, investigate anomalies, and evaluate model outputs	Model quality and data integrity
Engineering / Infrastructure Team	Maintain system availability and operational reliability	Monitor infrastructure health, uptime, and system logs	System reliability and service continuity
Responsible AI / Compliance Team	Oversee fairness, bias monitoring, and regulatory alignment	Review fairness metrics and evaluate compliance obligations	AI governance and regulatory compliance
Product Governance Team	Review user feedback and operational impact	Monitor complaint trends and user interaction signals	User impact and product oversight
Security / Risk Team	Detect security threats or system misuse	Monitor suspicious activities and adversarial interactions	System security and risk mitigation

Governance Oversight Guidance

Organizations should ensure that monitoring governance structures support cross-functional collaboration between technical, operational, and compliance teams. Effective governance oversight enables timely interpretation of monitoring outputs and ensures that escalation or remediation actions are coordinated across responsible teams.

Regular governance reviews help confirm that monitoring processes remain effective and aligned with evolving operational and regulatory expectations.

Section E • 01 — Monitoring Review and Oversight Process

This section defines how monitoring outputs are reviewed and interpreted by responsible governance teams. Structured review processes ensure that monitoring signals are evaluated consistently and that potential risks are assessed before they affect system reliability, safety, or regulatory compliance.

Regular oversight of monitoring outputs enables organizations to identify emerging patterns, validate the effectiveness of monitoring mechanisms, and determine whether escalation or corrective actions are required.

Monitoring review activities should be conducted at appropriate intervals based on the operational risk level of the AI system and the nature of the monitoring signals being evaluated.

Review Activity	Review Objective	Review Frequency	Responsible Governance Body
Operational Monitoring Review	Evaluate system performance indicators and operational signals	Weekly or continuous monitoring review	ML Operations Team
Data Monitoring Assessment	Assess data quality, distribution shifts, and drift indicators	Weekly or bi-weekly review	Data Science Team
System Reliability Review	Evaluate infrastructure stability, error rates, and system availability	Weekly review	Engineering / Infrastructure Team
Fairness and Compliance Review	Assess bias metrics and compliance with responsible AI requirements	Monthly review	Responsible AI / Compliance Committee
User Impact Assessment	Review complaint trends and operational feedback from users	Monthly review	Product Governance Team
Security Monitoring Review	Evaluate security alerts, misuse signals, and system vulnerabilities	Continuous monitoring with monthly review	Security / Risk Oversight Team

Monitoring Oversight Guidance

Monitoring review processes should involve collaboration between technical teams and governance bodies to ensure that monitoring outputs are interpreted within the broader operational and regulatory context. Structured review meetings and documented evaluation procedures help organizations maintain transparency, accountability, and effective risk management.

Regular oversight reviews also support continuous improvement of monitoring mechanisms and ensure that governance structures remain aligned with evolving system behavior and regulatory expectations.

Section E • 02 — Monitoring Reporting and Internal Communication

This section defines how monitoring outputs are communicated within the organization to ensure that relevant stakeholders are informed of system performance, operational risks, and monitoring findings. Clear internal reporting processes support transparency, accountability, and timely decision-making.

Monitoring reports should provide structured summaries of system performance indicators, detected anomalies, escalation events, and corrective actions taken during the monitoring period. These reports help governance teams evaluate whether monitoring activities remain effective and aligned with the operational risk profile of the AI system.

Effective communication channels ensure that monitoring insights are shared across technical, operational, and compliance teams so that emerging risks can be addressed promptly.

Reporting Activity	Reporting Objective	Reporting Frequency	Responsible Team
Operational Monitoring Report	Summarize system performance indicators and operational monitoring results	Weekly reporting	ML Operations Team
Data Monitoring Summary	Report data distribution trends, drift signals, and anomaly detection outcomes	Weekly or bi-weekly reporting	Data Science Team
Infrastructure Monitoring Report	Provide updates on system reliability, uptime, and operational incidents	Weekly reporting	Engineering / Infrastructure Team
Responsible AI Monitoring Report	Summarize fairness evaluations and compliance monitoring outcomes	Monthly reporting	Responsible AI / Compliance Team
User Impact Report	Document complaint patterns, user feedback trends, and operational concerns	Monthly reporting	Product Governance Team
Security Monitoring Report	Provide updates on security alerts, misuse detection, and risk mitigation actions	Continuous monitoring with monthly reporting	Security / Risk Team

Monitoring Communication Guidance

Organizations should ensure that monitoring findings are communicated clearly to relevant governance bodies and operational teams. Structured reporting mechanisms help ensure that monitoring insights translate into informed decision-making, effective risk management, and timely corrective action where necessary.

Transparent communication across technical and governance functions strengthens organizational accountability and supports continuous improvement of monitoring practices.

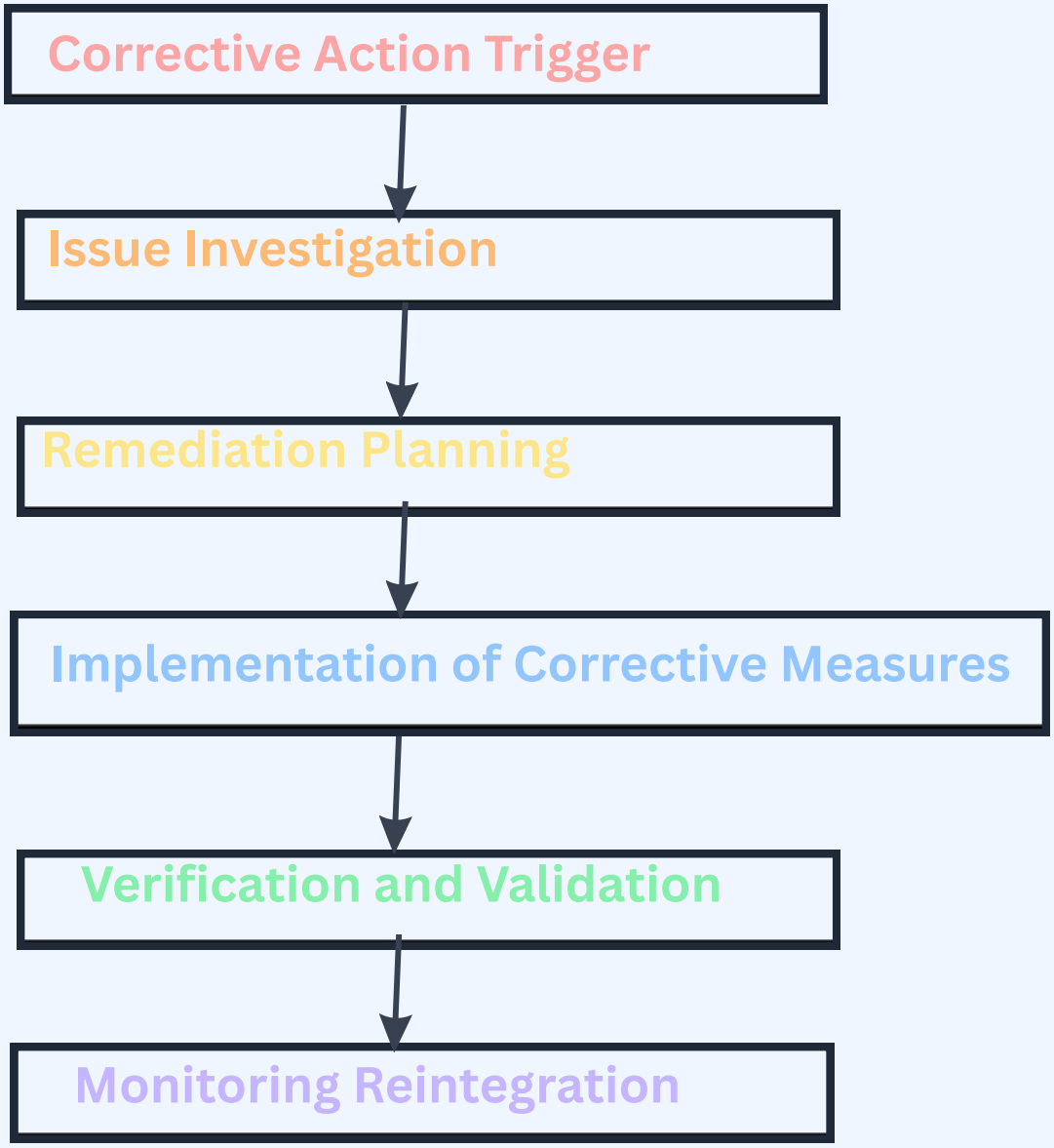
Section F — Corrective Action Framework

This section establishes the framework used to implement corrective actions when monitoring activities identify operational risks, performance degradation, or compliance concerns. The corrective action framework ensures that identified issues are addressed through structured investigation, remediation, and verification processes.

Corrective actions should be initiated when monitoring indicators exceed defined thresholds or when escalation procedures determine that system behavior requires intervention. A well-defined corrective action process helps organizations maintain system reliability, mitigate operational risks, and ensure continued alignment with regulatory requirements.

The framework should ensure that corrective actions are documented, validated, and integrated into ongoing monitoring activities to support continuous system improvement.

Corrective Action Lifecycle Diagram



The corrective action lifecycle ensures that monitoring signals are translated into structured operational responses. Each step of the corrective process contributes to identifying root causes, implementing remediation measures, and confirming that the AI system returns to acceptable performance conditions.

Integrating corrective responses back into monitoring activities ensures that system improvements are continuously evaluated and that similar risks are prevented in future system operations.

Corrective Action Governance Guidance

Organizations should ensure that corrective actions are coordinated across technical, operational, and governance teams. Clear documentation of corrective responses helps maintain traceability and supports regulatory review of post-market monitoring activities.

Corrective action procedures should also ensure that lessons learned from monitoring events contribute to improvements in system design, deployment practices, and risk management processes.

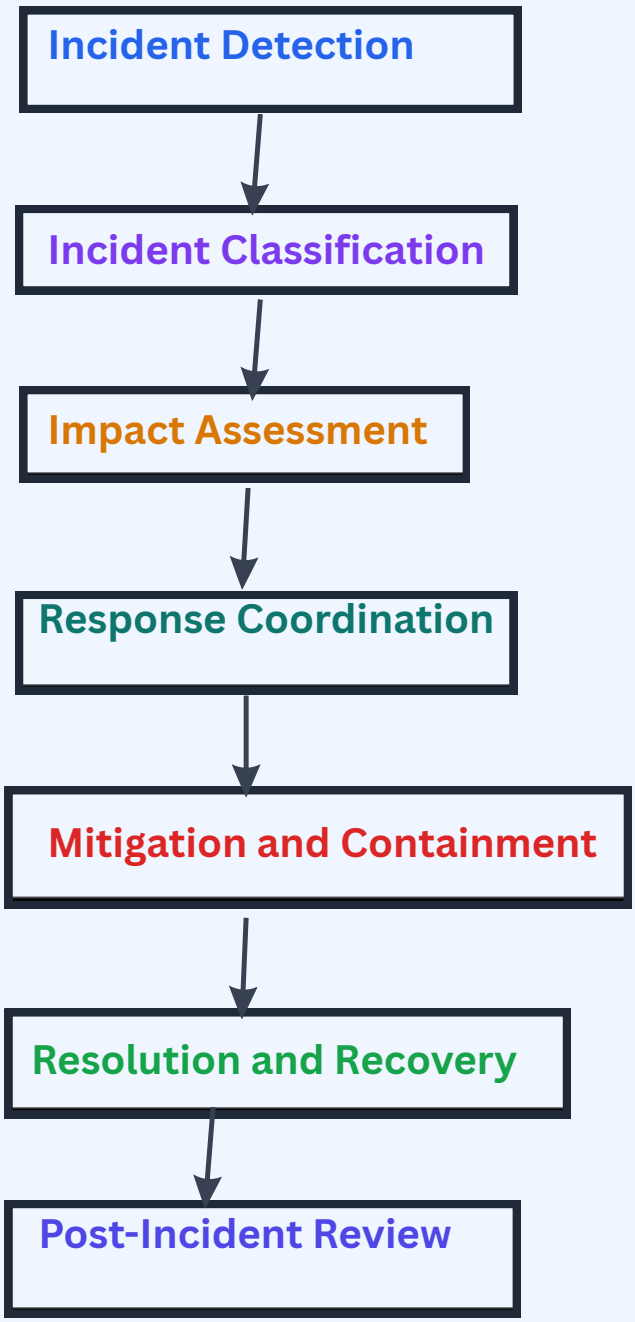
Section G — Incident Response Pipeline

This section defines the structured process used to respond to operational incidents detected through monitoring activities. An incident response pipeline ensures that system anomalies, operational failures, security threats, or unexpected AI behavior are investigated and addressed in a timely and controlled manner.

A clearly defined response pipeline enables organizations to detect incidents quickly, coordinate response actions across responsible teams, and minimize potential risks to system reliability, user safety, or regulatory compliance.

Incident response procedures should ensure that all incidents are documented, investigated, and resolved through a structured escalation and remediation workflow.

Incident Response Pipeline Diagram



Incident Response Governance Guidance

Organizations should ensure that incident response procedures clearly define roles, escalation pathways, and communication channels for managing operational events. Coordinated response actions across technical, operational, and governance teams help ensure that incidents are contained effectively and resolved without unnecessary delays.

Well-documented incident response processes support regulatory compliance and strengthen organizational resilience when responding to unexpected system behavior.

The incident response pipeline ensures that operational events detected through monitoring systems are handled through a structured response workflow. Each stage of the pipeline contributes to identifying the nature of the incident, coordinating response actions, and restoring normal system operation.

Following resolution, post-incident reviews help organizations analyze root causes, identify lessons learned, and strengthen monitoring and risk management practices to prevent similar incidents in the future.

Section H — Serious Incident Reporting

This section outlines the procedures for reporting serious incidents involving high-risk AI systems in accordance with Article 73 of the EU Artificial Intelligence Act. Serious incidents are events that may result in significant harm to individuals, operational disruptions, or violations of fundamental rights arising from the deployment or operation of an AI system.

Timely reporting of serious incidents ensures that competent authorities are informed of risks that may affect public safety, fundamental rights, or system reliability. Organizations deploying high-risk AI systems should ensure that clear procedures are established for identifying, documenting, and reporting such incidents.

Serious incident reporting procedures should be integrated into the broader monitoring and incident response framework to ensure that reportable events are escalated appropriately and communicated to regulatory authorities within required timeframes.

Incident Type	Description of Event	Reporting Requirement	Responsible Reporting Authority
Operational Safety Incident	AI system malfunction causing potential harm to individuals	Immediate internal escalation and regulatory notification	Responsible AI / Compliance Team
Fundamental Rights Impact	AI system behavior affecting individual rights or protections	Document incident and report to competent authority	Compliance and Legal Team
System Reliability Failure	Critical system failure affecting operational safety	Incident investigation and authority notification if required	Engineering / Infrastructure Team
Security Breach or Misuse	Unauthorized access or malicious use of the AI system	Report security incident and initiate risk mitigation	Security / Risk Team
Data Integrity Incident	Data corruption or manipulation affecting system outputs	Investigate impact and report if regulatory risk is identified	Data Governance Team

Serious Incident Reporting Guidance

Organizations should ensure that serious incidents are reported promptly in accordance with regulatory obligations. Incident reports should include a clear description of the event, the potential impact on individuals or system operations, and the corrective measures implemented to mitigate the identified risk.

Maintaining structured reporting procedures helps organizations demonstrate transparency and accountability in managing high-risk AI systems.

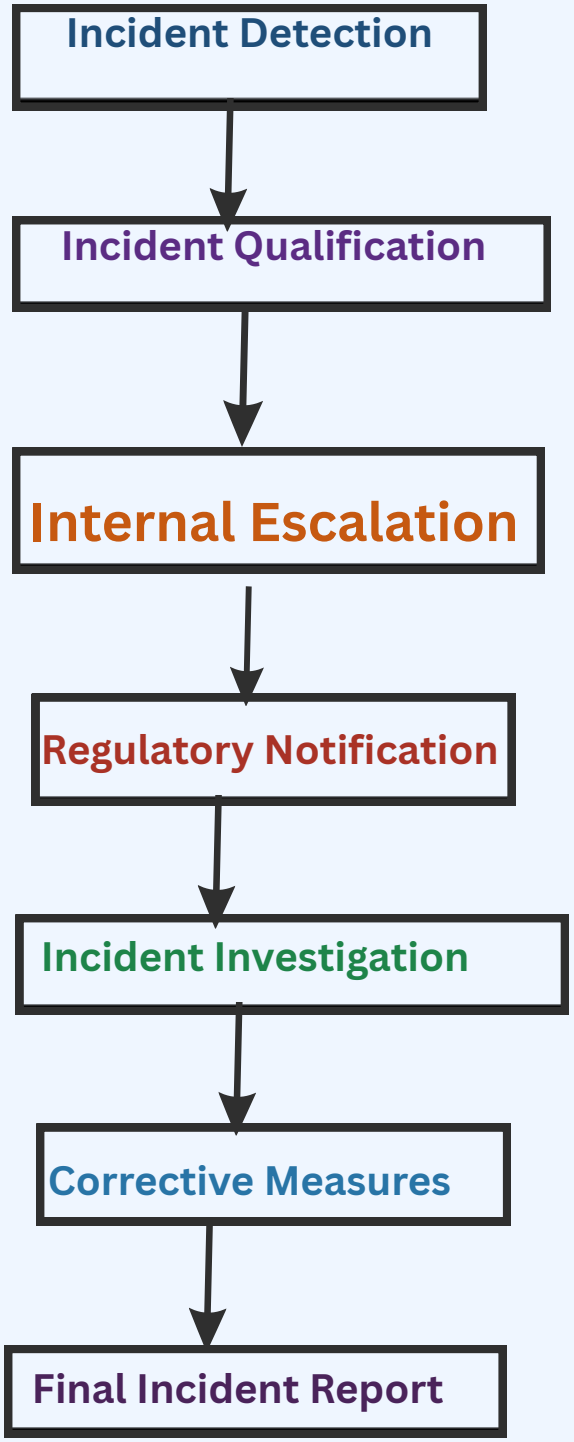
Section H • 01 — Serious Incident Reporting Workflow

This section describes the operational workflow used to report serious incidents involving high-risk AI systems in accordance with Article 73 of the EU Artificial Intelligence Act. The reporting workflow ensures that serious incidents are promptly identified, escalated internally, and communicated to competent authorities when regulatory reporting obligations are triggered.

A structured reporting process helps organizations ensure transparency, timely risk mitigation, and accountability when managing serious operational or safety incidents involving AI systems.

Organizations should integrate this reporting workflow with their monitoring, incident response, and governance structures to ensure that reportable incidents are handled consistently and documented appropriately.

Serious Incident Reporting Workflow



Serious Incident Workflow Guidance

Organizations should ensure that serious incident reporting workflows clearly define escalation thresholds, reporting responsibilities, and regulatory notification procedures. Establishing structured reporting processes helps ensure that serious operational events are addressed promptly and communicated to competent authorities where required.

Documented reporting workflows support regulatory transparency and help organizations maintain accountability when responding to incidents involving high-risk AI systems.

The serious incident reporting workflow illustrates how reportable operational events are identified, escalated internally, and communicated to competent authorities in accordance with regulatory obligations. Each stage of the workflow ensures that incidents are assessed, investigated, and documented in a structured and accountable manner.

Following resolution, organizations should produce a final incident report summarizing the event, investigation outcomes, corrective measures implemented, and lessons learned. Maintaining a structured reporting workflow supports regulatory transparency and helps organizations strengthen monitoring and risk management practices over time.

Section I — Evidence Pack and Audit Documentation

This section outlines the documentation and evidence records that organizations should maintain to demonstrate compliance with post-market monitoring obligations for high-risk AI systems. Maintaining a structured evidence pack ensures that monitoring activities, incident management procedures, and corrective actions can be verified during internal reviews or regulatory inspections.

An organized evidence pack enables organizations to demonstrate transparency, traceability, and accountability in the ongoing monitoring of deployed AI systems. Proper documentation supports regulatory oversight and helps organizations confirm that monitoring controls remain effective throughout the system lifecycle.

Organizations should ensure that monitoring records, incident documentation, governance decisions, and corrective action evidence are securely stored and accessible for audit or regulatory review when required.

Evidence Category	Documentation Description	Purpose of Evidence	Responsible Team
Monitoring Logs	Records of system monitoring outputs, alerts, and operational signals	Demonstrate ongoing system monitoring activities	ML Operations Team
Performance Evaluation Reports	Reports summarizing model performance metrics and monitoring indicators	Validate that the AI system operates within defined thresholds	Data Science Team
Incident Investigation Records	Documentation of incident investigations, root-cause analysis, and outcomes	Provide traceability of incident management processes	Engineering / Risk Team
Corrective Action Documentation	Records of remediation measures implemented after monitoring alerts	Demonstrate that identified risks were addressed	Responsible AI / Governance Team
User Feedback and Complaint Logs	Records of user complaints, feedback reports, and issue tracking	Monitor operational impact and user-reported concerns	Product Governance Team
Security Monitoring Reports	Logs of security alerts, misuse detection, and system vulnerability monitoring	Demonstrate system security oversight	Security / Risk Team

Evidence Retention and Audit Guidance

Organizations should maintain structured evidence records to support regulatory transparency and audit readiness. Monitoring logs, investigation reports, governance reviews, and corrective action documentation should be retained in accordance with organizational record-keeping policies and applicable regulatory requirements.

Maintaining a comprehensive evidence pack ensures that organizations can demonstrate compliance with post-market monitoring obligations and respond efficiently to regulatory inquiries or internal audits.

Appendix — Operational Templates

This appendix provides example operational templates that organizations may use to support post-market monitoring activities for high-risk AI systems. These templates illustrate how monitoring activities, incident reports, and corrective actions can be documented consistently within an organization.

Operational templates help ensure that monitoring information is captured in a structured manner, enabling organizations to maintain traceability, transparency, and audit readiness. Organizations may adapt these templates to align with their internal governance procedures and operational workflows.

Monitoring Log Record

Monitoring Date	Monitoring Indicator	Observation or Alert	Action Taken	Responsible Team
Example Entry	Model accuracy monitoring	Accuracy dropped below baseline threshold	Initiated investigation and model validation	ML Operations Team

Incident Report Record

Incident ID	Incident Description	Incident Impact	Investigation Outcome	Responsible Team
Example Entry	Unexpected system prediction anomaly	Potential operational disruption	Root cause identified and corrective action initiated	Engineering / Risk Team

Corrective Action Record

Issue Identified	Investigation Summary	Corrective Action Implemented	Verification Status	Responsible Team
Example Entry	Model drift detected	Data distribution change identified	Retrained model with updated dataset	Validation completed

Operational Template Usage Guidance

Organizations should adapt these operational templates to align with their internal monitoring and governance processes. Maintaining structured operational records supports transparency, traceability, and regulatory compliance when managing high-risk AI systems.

Consistent documentation practices help organizations demonstrate that monitoring activities, incident investigations, and corrective actions are performed in accordance with post-market monitoring requirements.

References and Disclaimer

References

This document references regulatory frameworks and governance principles associated with the ***European Union Artificial Intelligence Act (EU AI Act)*** and established practices for monitoring high-risk AI systems.

Key regulatory reference:

European Parliament and Council of the European Union.
Regulation (EU) on Artificial Intelligence
(Artificial Intelligence Act) establishing harmonized rules for artificial intelligence and amending certain Union legislative acts.

Organizations implementing post-market monitoring processes should review applicable regulatory requirements and adapt monitoring procedures to align with evolving regulatory expectations and operational risk profiles.

Additional guidance may also be informed by established risk management and AI governance practices used in responsible AI development and deployment.

Disclaimer

This document is provided as a general governance template intended to support organizations in structuring post-market monitoring activities for AI systems. The content is designed for informational and operational guidance purposes and should not be interpreted as legal advice.

Organizations are responsible for ensuring that their monitoring practices comply with applicable laws, regulatory requirements, and internal governance policies. The procedures and examples included in this template may be adapted to reflect the operational context, risk profile, and compliance obligations of the deploying organization.

Use of this document does not guarantee regulatory compliance and organizations should consult legal or regulatory experts where necessary when implementing AI governance frameworks.

About AI Governance Desk

AI Governance Desk provides clear, practical insights on AI governance, policy, ethics, regulation, and responsible AI for organizations, professionals, and decision-makers.

The platform focuses on translating complex regulatory and governance developments into actionable guidance that helps organizations understand and implement responsible AI practices. By bridging the gap between policy frameworks and operational implementation, AI Governance Desk supports organizations navigating the evolving landscape of AI governance and compliance.

AI Governance Desk publishes research, analysis, and governance resources that help professionals stay informed about developments in AI regulation, risk management, and responsible technology deployment.