# AI GOVERNANCE DESK

# Human Oversight Protocol Template for High-Risk AI Systems

*Supporting Implementation of Article 14 EU Artificial Intelligence Act (Regulation EU 2024/1689)*

# Document Overview

## Purpose of the Template

This document provides a structured template for designing and documenting human oversight mechanisms for high-risk artificial intelligence systems. The template supports organizations that must operationalize human supervision requirements within AI-enabled decision processes.

Rather than presenting theoretical guidance, the document provides a practical governance framework that organizations can adapt to their operational environment. Each section is designed to help governance teams define oversight responsibilities, intervention points, monitoring mechanisms, and escalation pathways in a consistent and auditable manner.

## Regulatory Context

The template aligns with Article 14 of the European Union Artificial Intelligence Act (Regulation EU 2024/1689), which requires that high-risk AI systems be designed and deployed with effective human oversight mechanisms. The regulation emphasizes the ability of natural persons to understand system behavior, detect anomalies, and intervene when necessary to prevent risks to health, safety, and fundamental rights.

Human oversight is increasingly recognized as a central element of responsible AI governance. Organizations deploying high-risk AI systems must demonstrate that oversight mechanisms are not merely symbolic but capable of influencing system outcomes when risks emerge.

## Scope of Application

This template is intended for use in governance programs responsible for the deployment or supervision of high-risk AI systems. It may be applied across sectors including healthcare, financial services, public administration, industrial operations, and other environments where AI systems influence consequential decisions.

The template focuses specifically on the operational design of oversight frameworks. It does not replace broader AI governance policies, risk management systems, or compliance programs, but rather complements those mechanisms by providing a structured format for documenting human supervision procedures.

## Intended Users

This document is intended for professionals responsible for designing, supervising, or auditing AI governance programs. Typical users include AI governance teams, compliance officers, risk managers, machine learning operations teams, internal auditors, and regulatory oversight bodies.

The template is particularly relevant for organizations implementing governance frameworks aligned with the EU Artificial Intelligence Act or similar regulatory expectations concerning human supervision of automated decision systems.

## How to Use This Template

Organizations should complete each section of this template using information specific to the AI system under review. The document is intended to support internal governance documentation and may also serve as supporting evidence during regulatory assessments or internal audits.

Governance teams should review the completed template alongside existing AI risk management documentation, system impact assessments, and monitoring procedures. The template may be updated periodically as system behavior, deployment context, or regulatory expectations evolve.

Where appropriate, organizations may expand the sections of the template to reflect sector-specific oversight requirements or internal governance policies.

# AI System Identification

*This section documents the core identification details of the AI system subject to oversight. Organizations should complete the fields below to clearly define the system being evaluated within the human oversight framework.*

**AI System Name**

_____

**AI System Provider / Developer**

_____

**Deployment Organization**

_____

**System Purpose**

_____

**Operational Environment**

_____

**Date of Oversight Review**

_____

**Responsible Department**

_____

**Primary Oversight Contact**

_____

## Guidance Not

The information captured in this section ensures that the oversight protocol is clearly linked to a specific AI system deployment. Accurate system identification helps governance teams track oversight activities, maintain audit records, and align documentation with regulatory compliance requirements.

# AI Risk Classification

*This section records the regulatory risk classification of the AI system under review. Under the EU Artificial Intelligence Act, AI systems are categorized according to the level of risk they pose to individuals and society. Accurate classification is essential because oversight obligations and compliance requirements vary depending on the system's risk category.*

**EU AI Act Risk Category**
□ Prohibited AI System

□ High-Risk AI System

□ Limited Risk AI System

□ Minimal / No Risk AI System

**Potential Impact Domains**
□ Health and Safety

□ Fundamental Rights

□ Financial Impact

□ Access to Public Services

□ Employment or Workforce Decisions

□ Law Enforcement / Public Administration

Applicable Annex III Category (if High-Risk)
_____

**Risk Severity Assessment**
□ Low Impact

□ Moderate Impact

□ Significant Impact

□ Critical Impact

**Guidance Note**
Risk classification determines the level of regulatory obligations applied to an AI system. Systems classified as high-risk under the EU AI Act require formal risk management processes, human oversight mechanisms, and ongoing monitoring. Governance teams should ensure that classification decisions are documented and periodically reviewed.

**Risk Classification Justification**

_____

_____

_____

_____

# Oversight Model Selection

*This section documents the human oversight model applied to the AI system. Different operational environments require different forms of human supervision. Organizations should select the oversight model that best reflects how human decision-makers interact with the system during operation.*

**Selected Oversight Model**

☐ Human-in-the-Loop (HITL)

☐ Human-on-the-Loop (HOTL)

☐ Human-in-Command (HIC)

**Oversight Model Descriptions**

Human-in-the-Loop (HITL)
Human reviewers actively participate in the decision process and must approve or modify system outputs before actions are taken.

Human-on-the-Loop (HOTL)
The AI system operates autonomously under human supervision. Supervisors monitor system behavior and intervene when anomalies or risk signals appear.

Human-in-Command (HIC)
Human authorities retain ultimate decision authority over whether and how the AI system operates, including the ability to suspend or override system decisions.

**Oversight Model Justification**

_____

_____

_____

_____

**Primary Oversight Role**

_____

> **Guidance Note**
> The choice of oversight model should reflect the operational risk profile of the AI system and the level of human authority required during decision processes. High-risk systems often require direct human involvement or supervisory monitoring to ensure that automated outputs do not create unintended harm or regulatory violations.

# Human Oversight Roles and Responsibilities

*This section defines the human roles responsible for supervising the AI system and executing oversight procedures. Clear assignment of responsibilities ensures that governance teams understand who must review system outputs, monitor operational behavior, and intervene when necessary to prevent unintended risks.*

| Oversight Role | Primary Responsibility | Assigned Person / Department |
|---|---|---|
| Operational Reviewer | Evaluates AI system outputs during operational use and determines whether outputs require approval, modification, or escalation. | |
| Oversight Supervisor | Monitors overall system performance and reviews cases escalated by operational reviewers. | |
| AI Governance Lead | Maintains oversight policies and ensures alignment with organizational AI governance frameworks and regulatory obligations. | |
| Executive Authority | Retains final authority to suspend, modify, or terminate system deployment if governance risks are identified. | |

## Escalation Authority

_____

### Oversight Review Availability

☐ Continuous Monitoring

☐ Periodic Review

☐ Event-Triggered Oversight

> **Guidance Note**
> Effective oversight requires clearly defined human roles. Each role should have sufficient authority, training, and access to system information to intervene when risks are identified. Organizations should review oversight responsibilities periodically to ensure they remain appropriate as AI systems evolve.

# Human Oversight Intervention Points

*This section identifies the specific stages within the AI system workflow where human oversight must occur. Organizations should clearly define when human reviewers must evaluate system outputs, what conditions trigger intervention, and how decisions are approved, modified, or escalated. Documenting intervention points ensures that oversight mechanisms are operationally embedded within the system lifecycle rather than applied only after risks emerge.*

| Workflow Stage | Oversight Trigger | Human Action Required | Escalation Condition |
|---|---|---|---|
| Data Input Validation | Detection of missing, inconsistent, or anomalous input data | Reviewer verifies data quality before model processing | Escalate if data integrity cannot be verified |
| Model Output Generation | High-impact or high-risk decision output | Human reviewer evaluates the AI recommendation before operational use | Escalate if the output appears inconsistent with expected behavior |
| Decision Approval | AI output influences operational or regulatory decisions | Human reviewer approves, modifies, or rejects the recommendation | Escalate if uncertainty exists regarding risk implications |
| Exception Handling | Detection of anomalies, system errors, or unexpected outputs | Supervisor reviews incident and determines corrective action | Escalate to governance leadership if systemic risk is suspected |
| Post-Decision Monitoring | Evidence of outcome deviation or performance degradation | Oversight team reviews system behavior and validates decisions | Escalate if performance drift or governance violations occur |

# Human Override Authority

## Required Human Intervention Response Time

☐ Immediate (real-time oversight required)

☐ Same operational cycle

☐ Periodic review window

> ## Guidance Note
> Human intervention points should be clearly defined during system design and documented within operational procedures. Oversight mechanisms must enable reviewers to detect anomalies, interpret system outputs, and intervene effectively when automated decisions present potential risks to individuals, organizations, or regulatory compliance.

# Oversight Monitoring and Logging Mechanisms

*Effective human oversight requires continuous monitoring of AI system behavior and the ability to record oversight actions. This section documents the mechanisms used to monitor system activity, capture operational signals, and maintain logs of oversight decisions. Proper logging supports accountability, enables audit review, and allows organizations to detect anomalies or performance drift within deployed AI systems.*

| Monitoring Indicator | Detection Method | Oversight Response |
|---|---|---|
| Model Output Anomalies | Automated anomaly detection or manual review | Human reviewer investigates unexpected outputs |
| Performance Degradation | Performance monitoring dashboards | Oversight team evaluates model behavior and initiates review |
| Data Drift | Statistical monitoring tools | Review training data alignment and consider model retraining |
| Operational Incidents | System alerts or user reports | Supervisor investigates incident and records corrective action |
| Regulatory or Policy Violations | Compliance monitoring or audit review | Escalate to governance leadership for review |

## Oversight Logging Requirements

Oversight Activity Log Location

_____

Log Retention Period

_____

Responsible Logging Authority

_____

### Required Oversight Records

☐ Human review decisions

☐ System override actions

☐ Incident investigation reports

☐ Model performance monitoring reports

☐ Regulatory compliance documentation

---

## Guidance Note

Monitoring and logging mechanisms provide essential evidence that human oversight procedures are functioning effectively. Oversight logs should capture reviewer actions, system anomalies, and escalation events. Maintaining accurate records enables organizations to demonstrate compliance with regulatory obligations and supports continuous improvement of AI governance processes.

# Oversight Workflow

This section outlines the operational workflow for implementing human oversight across the AI system lifecycle. Establishing a structured oversight workflow ensures that governance teams understand when reviews must occur, which roles are responsible for intervention, and how oversight decisions are documented. A clearly defined workflow reduces operational risk and ensures that oversight procedures remain consistent throughout system deployment and monitoring.

| Workflow Phase | Oversight Activity | Responsible Role | Expected Outcome |
|---|---|---|---|
| Data Preparation | Validate training and input data integrity before model processing | Operational Reviewer | Data quality confirmed before model execution |
| Model Deployment | Review system readiness, risk classification, and oversight configuration | AI Governance Lead | Deployment approval granted with oversight controls |
| Operational Monitoring | Monitor AI outputs, anomaly alerts, and performance signals | Oversight Supervisor | Early detection of irregular system behavior |
| Incident Response | Investigate detected anomalies and determine corrective actions | AI Governance Lead | System risks mitigated and documented |
| Periodic Governance Review | Conduct scheduled oversight reviews and compliance validation | Executive Authority | Ongoing governance and regulatory compliance |

## Oversight Workflow Ownership

Workflow Owner

_____

Oversight Review Frequency

_____

Responsible Governance Team

_____

## Guidance Note

Human oversight workflows should be embedded directly into the operational lifecycle of AI systems rather than applied only during exceptional events. Clearly documented workflow stages ensure that reviewers know when intervention is required, which governance authority is responsible for decisions, and how oversight activities must be recorded for accountability and regulatory compliance.

# Escalation Protocol

*This section defines the escalation protocol for situations where human oversight identifies risks, anomalies, or compliance concerns during AI system operation. Escalation procedures ensure that oversight personnel can promptly report critical issues to appropriate governance authorities and that response actions are coordinated in a structured and accountable manner.*

| Escalation Level | Trigger Condition | Responsible Authority | Required Action |
|---|---|---|---|
| Level 1 — Operational Review | Minor anomalies or deviations detected in system outputs | Operational Reviewer | Investigate issue and document findings |
| Level 2 — Supervisory Escalation | Repeated anomalies or moderate risk indicators | Oversight Supervisor | Conduct system review and determine corrective actions |
| Level 3 — Governance Escalation | Significant risk to system integrity, compliance, or operational safety | AI Governance Lead | Initiate formal governance review and risk mitigation plan |
| Level 4 — Executive Intervention | Critical risk affecting regulatory compliance, safety, or system integrity | Executive Authority | Suspend or modify system deployment and initiate investigation |

## Escalation Communication Channels

Primary Escalation Contact

———————————————————

Secondary Governance Contact

———————————————————

Incident Reporting Channel

———————————————————

### Guidance Note
Escalation protocols must ensure that oversight personnel can rapidly communicate critical system issues to governance leadership. Clearly defined escalation levels reduce response delays and ensure that risks affecting safety, regulatory compliance, or operational integrity are addressed promptly and transparently.

## Escalation Response Requirements
☐ Immediate escalation (critical system risk)

☐ Same operational cycle escalation

☐ Escalation within defined governance review window

# Monitoring and Review Metrics

*This section defines the metrics used to evaluate the effectiveness of human oversight within the AI system lifecycle. Monitoring and review indicators help governance teams measure system reliability, detect emerging risks, and assess whether oversight mechanisms are functioning as intended. Regular evaluation ensures that oversight procedures remain aligned with operational risks and regulatory expectations.*

| Monitoring Metric | Measurement Method | Review Frequency | Responsible Authority |
|---|---|---|---|
| Output anomaly rate | Monitoring system alerts and anomaly detection logs | Continuous monitoring | Oversight Supervisor |
| Model performance stability | Performance dashboards and system validation tests | Weekly review | Operational Reviewer |
| Data drift indicators | Statistical drift monitoring tools | Periodic review cycle | AI Governance Lead |
| Incident escalation frequency | Governance incident reports and escalation logs | Monthly governance review | **AI Governance Lead** |
| Regulatory compliance status | Internal audits and governance documentation review | Quarterly compliance review | Executive Authority |

## Oversight Review Reporting

Monitoring Dashboard Location
_____

Oversight Review Schedule
_____

Responsible Monitoring Team
_____

## Governance Performance Indicators

☐ Oversight anomaly detection effectiveness

☐ Oversight intervention response time

☐ Escalation response compliance

☐ Regulatory compliance review completion

## Guidance Note

Monitoring metrics help governance teams determine whether oversight mechanisms are effectively identifying risks and supporting responsible AI operation. Regular review of these metrics allows organizations to detect systemic issues early and continuously improve governance procedures.

# Oversight Logging Template

*This section provides a structured template for recording human oversight activities during the operation of AI systems. Oversight logs ensure that intervention decisions, system anomalies, and governance actions are documented in a consistent and auditable format. Maintaining accurate oversight records supports transparency, regulatory compliance, and continuous improvement of AI governance practices.*

| Log Date | System Event | Oversight Action | Responsible Reviewer | Escalation Status | Notes |
|----------|-------------|------------------|---------------------|-------------------|-------|
| [Date] | Output anomaly detected | Reviewed system output and validated data source | Operational Reviewer | No escalation | Issue resolved during review |
| [Date] | Model performance deviation | Initiated performance validation review | Oversight Supervisor | Escalated to governance review | Monitoring required |
| [Date] | Data drift detected | Requested model retraining review | AI Governance Lead | Governance escalation | Corrective action initiated |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Oversight Incident Documentation

Incident Description
_____

Oversight Decision Taken
_____

Corrective Action Implemented
_____

**Log Reviewed By**
_____

**Review Date**
_____

**Governance Approval**
_____

**Guidance Note**
Oversight logs provide a documented history of human review and intervention during AI system operation. Maintaining detailed records allows organizations to demonstrate accountability, support regulatory compliance reviews, and identify patterns that may require improvements to governance procedures.

# Training and Competency Requirements

*Effective human oversight requires that personnel responsible for supervising AI system operations possess appropriate training and domain knowledge. Organizations must ensure that oversight personnel understand system functionality, operational risks, and governance procedures. This section documents the training programs and competency requirements necessary for individuals responsible for executing oversight responsibilities.*

| Oversight Role | Required Knowledge and Skills | Recommended Training | Certification / Verification |
|---|---|---|---|
| Operational Reviewer | Understanding of system outputs, operational workflows, and anomaly detection | AI system operational training | Internal oversight competency assessment |
| Oversight Supervisor | Monitoring system performance, escalation procedures, and incident analysis | Governance oversight training program | Governance supervision certification |
| AI Governance Lead | AI governance frameworks, risk management, and regulatory compliance | AI governance and compliance training | Governance leadership certification |
| Executive Authority | Strategic oversight of AI governance and regulatory accountability | Executive AI governance briefing | Executive governance approval record |

## Oversight Training Program Documentation

Training Program Name

_____

Training Provider

_____

Training Completion Frequency

_____

Responsible Training Coordinator

_____

## Competency Verification

□ Oversight personnel training completion verified

□ Oversight competency assessment completed

□ Governance supervision training documented

□ Regulatory compliance training completed

---

**Guidance Note**
Human oversight personnel must possess sufficient technical understanding and governance awareness to effectively evaluate AI system outputs and intervene when necessary. Training programs should be regularly updated to reflect evolving system capabilities, regulatory requirements, and operational risks.

# Governance Approval

*This section records the formal governance approval of the Human Oversight Protocol. Approval confirms that the oversight framework has been reviewed by responsible governance authorities and is authorized for operational use within the organization. Documenting approval ensures accountability and demonstrates that oversight procedures have been formally adopted within the organization's AI governance structure.*

| Governance Role | Name | Department | Signature / Approval |
|---|---|---|---|
| AI Governance Lead | | | |
| Oversight Supervisor | | | |
| Compliance Officer | | | |
| Executive Authority | | | |

## Approval Confirmation:

**Approval Date**

—————————————————————

**Effective Date of Protocol**

—————————————————————

**Next Scheduled Governance Review**

—————————————————————

*This Human Oversight Protocol is approved for implementation within the organization's AI governance framework. Governance authorities confirm that the procedures described in this document meet the organization's oversight, risk management, and regulatory compliance requirements.*

> **Guidance Note**
> Formal approval ensures that oversight procedures are recognized as part of the organization's governance framework. Governance approval also establishes accountability for maintaining and periodically reviewing the effectiveness of the oversight protocol.

# Version Control

*This section records the revision history of the Human Oversight Protocol. Maintaining version control ensures that updates to governance procedures are documented and approved. Tracking revisions helps organizations maintain transparency, ensure regulatory alignment, and preserve an auditable history of changes to oversight practices.*

| Version | Revision Date | Description of Changes | Updated By | Approval |
|---------|---------------|------------------------|------------|----------|
| 1.0 | | | | |
| 1.1 | | | | |
| 1.2 | | | | |
| | | | | |

## Document Control Information

**Document Owner**

——————————————————————

**Responsible Governance Department**

——————————————————————

**Next Scheduled Document Review**

——————————————————————

> ### Guidance Note
> Maintaining version control ensures that the Human Oversight Protocol remains current with evolving AI system capabilities, operational risks, and regulatory requirements. Governance teams should review this document periodically and update procedures whenever oversight practices or system deployments change.

## Version Update Approval

**Reviewed By**

——————————————————————

**Approval Date**

——————————————————————

**Authorized Governance Authority**

——————————————————————

# 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 governance and regulatory developments into actionable guidance that organizations can apply when designing, deploying, and supervising AI systems. By combining governance best practices with regulatory awareness, AI Governance Desk helps organizations build responsible AI frameworks that support transparency, accountability, and compliance.*

*Resources published through AI Governance Desk are intended to support governance teams, compliance professionals, technology leaders, and policy stakeholders seeking to strengthen oversight mechanisms in AI-enabled systems.*

# Professional Disclaimer

This Human Oversight Protocol Template is provided for informational and governance support purposes only. The content contained in this document does not constitute legal advice, regulatory advice, or professional compliance certification.

While this template reflects widely recognized AI governance principles and regulatory considerations, organizations should adapt the document to their specific operational environments, risk profiles, and applicable legal frameworks. Implementation of governance procedures should be conducted in consultation with qualified legal, compliance, and risk management professionals where appropriate.

AI Governance Desk makes no representations or warranties regarding the completeness, accuracy, or suitability of this document for any specific regulatory obligation or operational requirement. Organizations remain solely responsible for ensuring that their AI governance practices comply with applicable laws, regulations, and internal governance policies.

Use of this template does not guarantee regulatory compliance or certification under any jurisdiction, including but not limited to the European Union Artificial Intelligence Act or other emerging AI governance frameworks.

# Usage and Intellectual Property Notice

This document is an original resource developed by AI Governance Desk. The template may be used internally by organizations for governance documentation and oversight design.

Unauthorized redistribution, resale, or reproduction of this template without permission from AI Governance Desk is not permitted. Organizations and professionals may adapt the template for internal use, provided that the original attribution to AI Governance Desk is maintained.

For additional governance resources, insights, and updates on AI regulation and responsible AI practices,
visit: www.aigovernancedesk.com

Send message: contact@aigovernancesdesk.com

Prepared by AI Governance Desk
Responsible AI Governance Resources