

Das EU-KI-Gesetz mit aqua cloud

In 60 Tagen konform mit dem EU AI Act: Ihre QA-geführte Roadmap

Verantwortung	QA-Abteilung, in Zusammenarbeit mit Legal/Compliance, Engineering, Product und dem DSB.
Tool-Grundlage	aqua cloud (EU-Hosting, ISO 27001, DSGVO-konform by design, DORA-aligned) als einheitliche Testmanagement- und Nachweisplattform.
Zielgruppe	QA-Manager, CTOs, CPOs, Compliance-Verantwortliche, DSBs und Engineering-Manager in Organisationen, die Hochrisiko-KI-Systeme auf dem EU-Markt bereitstellen.

Zusammenfassung

Der EU AI Act ist am 1. August 2024 in Kraft getreten. Die Compliance-Anforderungen für Hochrisiko-KI-Systeme treten in Kürze in Kraft. Bußgelder erreichen bis zu 35 Mio. € oder 7% des weltweiten Jahresumsatzes für verbotene Praktiken sowie 15 Mio. € oder 3% bei Hochrisiko-Verstößen. Die Kapazitäten benannter Stellen sind schon jetzt knapp – Teams ohne strukturierten Nachweispfad verlieren wertvolle Zeit.

Die Roadmap führt eine QA-Abteilung in 60 Kalendertagen zur Audit-Bereitschaft – beginnend am ersten Tag nach dem aqua-Webinar. Voraussetzung ist, dass aqua cloud als Testmanagement-Plattform ausgewählt wurde. Im Fokus stehen die Einführung der Plattform, ihre Befüllung mit den richtigen Nachweisen und ein internes Probe-Audit vor der eigentlichen behördlichen Prüfung.

Vier Phasen, ein Ergebnis

- Phase 1 – Bestandsaufnahme & Ausrichtung (Tage 1–10):**
KI-System-Inventar, Klassifizierung nach Artikel 6 / Anhang III, Lückenanalyse gemäß Artikeln 9–15 und 17, Lenkungsausschuss eingesetzt, aqua-Mandant bereitgestellt.
- Phase 2 – aqua-Grundlage aufbauen (Tage 11–25):**
Testfälle, Rückverfolgbarkeitsmatrix aktiv, Defekt- und Freigabe-Workflows live, Jira / Jenkins / Azure DevOps integriert.
- Phase 3 – Nachweise erstellen (Tage 26–45):**
Testkampagnen für alle Pflichten aus Artikeln 9–15 durchführen.
Risikomanagement, Data Governance, technische Dokumentation, Protokollierung, Transparenz, menschliche Aufsicht sowie Genauigkeit/Robustheit erzeugen zeitgestempelte, nutzerzugeordnete Nachweise in aqua.
- Phase 4 – Probe-Audit & Go-Live (Tage 46–60):**
Technische Dokumentation aus aqua exportieren, internes Probe-Audit mit Rechtsberater durchführen, Mängel beheben, Slot bei der benannten Stelle buchen, Qualitätsmanagementsystem freigeben und kontinuierliches Monitoring aktivieren.

Warum 60 Tage mit aqua realistisch sind

Die meisten Teams verlieren Wochen damit, Nachweise aus Tabellen, Jira, E-Mails und geteilten Laufwerken zusammenzuführen. aqua bündelt diese Arbeit in einer einzigen unveränderlichen Kette – Anforderung → Testfall → Defekt → Behebung → Freigabe – mit einem Klick als audit-ready Bericht exportierbar. Die 60 Tage fließen in die Nachweiserbringung, nicht in die Nachweissuche.

Zeitplan auf einen Blick

Jede Phase endet an einem Samstag, sodass Teams einen Wochenend-Puffer vor dem nächsten Phasenstart haben. Der Zeitplan gilt ab dem vereinbarten Starttag.

Phase	Tage	Datum	Ergebnis
Phase 1	Tage 1–10	nach Vereinbarung	Scope bestätigt, Lücken kartiert, aqua Tenant live, Charter unterzeichnet.
Phase 2	Tage 11–25	nach Vereinbarung	aqua konfiguriert, Anforderungen importiert, AI Copilot generiert Testfälle, Workflows live.
Phase 3	Tage 26–45	nach Vereinbarung	Nachweise für Artikel 9–15 erstellt. Defekttrends, Freigaben, Data-Governance-Berichte – alles vorhanden.
Phase 4	Tage 46–60	nach Vereinbarung	Probe-Audit bestanden, Technische Dokumentation exportiert, Benannte Stelle gebucht, laufendes Monitoring aktiv.
Puffer	Tage 61–68	nach Vereinbarung	Abschließende Mängelbehebung. Letzte Chance, alle im Probe-Audit aufgedeckten Punkte vor dem Compliance-Stichtag zu beheben.

Hinweis zur Kapazitätslage bei benannten Stellen

Derzeit sind erst wenige benannte Stellen vollständig für die AI-Act-Konformitätsbewertung designed, und die Kapazitäten sind knapp. Ab Tag 1 dieser Roadmap wird die Buchung des Bewertungsslots parallel zur internen Arbeit angegangen – nicht erst in Phase 4.

Phasenübersicht

PHASE 1

BESTANDSAUFNAHME & AUSRICHTUNG

Tage 1–10

Ziel Umfang bestätigen, jedes KI-System der Organisation klassifizieren (Eigenentwicklung, Einsatz oder Integration), Lücken zum EU AI Act identifizieren und Programminfrastruktur inkl. aqua-Mandant aufbauen. Phase 2 beginnt erst, wenn die Klassifizierung unterzeichnet und der Lenkungsausschuss zusammengekommen ist.



Week / Tage	Schwerpunkt	Wichtigste Aktivitäten
Woche 1 (Tage 1–5)	Inventarisierung und Klassifizierung	- ag 1: Lenkungsausschuss einsetzen (QA-Lead, CTO/Eng VP, Rechtsberater, Compliance, DSB, Product). Wöchentlichen Rhythmus festlegen. - Tag 1: Kontakt zu benannten Stellen aufnehmen. Kapazität ist der limitierende Faktor – nicht der Aufwand. - Tag 2–3: KI-System-Inventar erstellen. Jedes Modell, jede Entscheidungsebene, Empfehlungs-Engine, jeder Scoring-Algorithmus und jede in ein größeres Produkt eingebettete KI-Funktion einbeziehen. - Tag 3–4: Jedes System nach Artikel 6 / Anhang III klassifizieren. Als verboten, hochriskant, mit begrenztem Risiko oder mit minimalem Risiko kennzeichnen. - Tag 5: Entscheidung über den Programmumfang – welche Systeme in das 60-Tage-Programm fallen und welche zurückgestellt werden.
Woche 2 (Tage 6–10)	Lückenanalyse und Charter	- Tag 6–7: Lückenanalyse gegenüber den Artikeln 9, 10, 11, 12, 13, 14, 15 und 17 durchführen. Aktuelle Nachweisquellen, Format und Verantwortlichen für jede Pflicht dokumentieren. - Tag 7: Anforderung zur Bereitstellung des aqua-Mandanten einreichen. EU-Rechenzentrumsauswahl und ISO 27001 / DORA-Referenzen für interne Sicherheitsprüfung bestätigen. - Day 8: Programm-Charta entwerfen. Umfang, RACI, Entscheidungsrechte und Budgetrahmen definieren. - Tag 9: Rechtsberater prüft die Lückenanalyse. Pflichten, die Legal vs. QA verantwortet, kennzeichnen. - Tag 10: Lenkungsausschuss erteilt Freigabe. Phase 1 abgeschlossen.

Abschlusskriterien

- ✓ Jedes relevante KI-System ist klassifiziert und von der Rechtsabteilung (Legal) freigegeben.
- ✓ Die Gap-Analyse wurde vom Lenkungsausschuss genehmigt und enthält für jede identifizierte Lücke eine verantwortliche Person.
- ✓ Der aqua-Tenant ist live und über die EU-spezifische URL erreichbar.
- ✓ Der Kontakt zur Benannten Stelle wurde erfolgreich hergestellt und ein Zeitfenster für die Bewertung vereinbart.

aqua cloud Aktivitäten in dieser Phase

- aqua cloud Tenant in einem EU-Rechenzentrum bereitstellen.
- ISO 27001-Zertifizierung und Trust-Center-Referenzen mit InfoSec bestätigen.
- Für jedes einbezogene KI-System ein Projekt anlegen. Projektbezeichnung soll der Inventar-ID entsprechen.
- SSO-Integrationsplan (Azure AD / Okta) aufsetzen, damit Identity Governance zu Beginn von Phase 2 bereitsteht.
- Bestehende Tools (Jira, Confluence, Excel, Azure DevOps) identifizieren, die Anforderungen und Test-Artefakte enthalten – das sind die Import-Quellen für Phase 2.

Ergebnisse

- KI-System-Inventar (mit Klassifizierung nach Artikel 6 / Anhang III und Risikostufe).
- Lückenanalysebericht (eine Zeile pro Artikel, aktueller Nachweis, Zielnachweis, Verantwortlicher, Aufwand).
- Programm-Charter und RACI.
- Auswahl benannter Stellen mit schriftlich bestätigten Kapazitäten.
- Bereitstellung des aqua-Tenants in der EU-Region, bereit für die Phase-2-Konfiguration.

Hauptverantwortliche

QA Manager (Programmleitung). Legal Counsel (Regulatorische Auslegung). DSB (Prüfung des Datenverarbeitungsumfangs). Engineering Manager (Systemerfassung & -inventarisierung).

PHASE 2

AQUA-GRUNDLAGE AUFBAUEN

Tage 11–25

Ziel Konfiguration von aqua als zentrale Instanz („Single Source of Truth“) für alle AI-Act-Nachweise. Hierbei werden Anforderungen importiert, Testfälle mithilfe des AI Copilot generiert, eine Rückverfolgbarkeitsmatrix (Traceability Matrix) aufgebaut, Workflows für Defekte und Freigaben definiert sowie die Entwickler-Toolchain angebunden. Am Ende von Phase 2 ist Ihr Team in der Lage, eine vollständige Rückverfolgbarkeitsmatrix direkt auf Abruf zu erstellen.

Week / Tage	Schwerpunkt	Wichtigste Aktivitäten
Woche 3 (Tage 11–15)	Tenant-Setup, Struktur, Integrationen	• SSO, RBAC und Rollenmodell konfigurieren: QA Engineer, QA Lead, Compliance Reviewer, Genehmiger, Auditor (nur-lesend). • Projekthierarchie und Feldmodell anlegen: KI-System → Release → Anforderung → Testfall → Ausführung → Defekt → Freigabe. • Artikel 9–15 + 17 als benutzerdefinierte Risikoklassifizierungsfelder für Anforderungen und Testfälle hinzufügen. • Jira-, Jenkins- und Azure DevOps-Integrationen installieren. Bidirektionale Synchronisation anhand eines Pilotprojekts validieren. • Capture für nachweisqualitäts-gerechtes Fehlerreporting konfigurieren (Screenshots, Umgebung, Reproduktionsschritte, Zeitstempel).
Woche 4 (Tage 16–20)	Anforderungsimport + AI Copilot	• Anforderungen aus Jira, Confluence, Excel und bestehenden Anforderungsmanagement-Tools in aqua importieren. • Klassifizierung auf Artikel-Ebene für jede Anforderung vornehmen. Vorgesehenen Zweck, Risikostufe und betroffene Bevölkerungsgruppe kennzeichnen. • AI Copilot über jede in-scope Anforderung laufen lassen, um strukturierte Testfälle zu generieren (positiv, negativ, Grenzfall, adversarial). • Jeden generierten Testfall manuell prüfen. Der Copilot beschleunigt die Arbeit – er genehmigt sie nicht. • Jeden Testfall mit seiner Anforderung verknüpfen, sodass die Rückverfolgbarkeit von Anfang an gewährleistet ist.
Woche 5 (Tage 21–25)	Workflows, Freigaben und Schulung	• Defekt-Workflow mit Audit-Feldern konfigurieren: Ursache, Risikoauswirkung, Artikel-Referenz, Behebung und Verifikation. • Freigabe-Workflow für menschliche Aufsicht konfigurieren (Artikel 14): Testausführungsfreigabe, Release-Freigabe, Änderungsfreigabe – jeweils mit Zeitstempel und Nutzer erfasst. • Audit-ready Berichtsvorlagen einrichten, die die unter Anhang IV erwartete Struktur der Technischen Dokumentation widerspiegeln. • QA-Team in aqua schulen (Testfallerstellung, Ausführung, Defektverknüpfung, Freigabe, Berichtsexport). • Tag 25: Bereitschaftsreview mit dem Lenkungsausschuss. Phase 2 abgeschlossen.

Abschlusskriterien

- ✓ 100 % der In-Scope-Anforderungen sind korrekt klassifiziert in aqua hinterlegt.
- ✓ Jede Anforderung ist mit mindestens einem Testfall verknüpft.
- ✓ Die Rückverfolgbarkeitsmatrix lässt sich fehlerfrei und ohne manuelle Nachbearbeitung in die Formate PDF, DOCX und XLSX exportieren.
- ✓ Die bidirektionale Synchronisation von Defekten zwischen Jira und Azure DevOps läuft reibungslos.
- ✓ Das QA-Team hat die aqua-Schulung erfolgreich abgeschlossen und kann Release-Prozesse eigenständig von Anfang bis Ende durchführen.

aqua cloud Aktivitäten in dieser Phase

- AI Copilot aktivieren und auf den gesamten importierten Anforderungsrückstand anwenden.
- Kette Anforderung → Testfall → Ausführung → Defekt → Behebung → Freigabe in aqua definieren.
- Rückverfolgbarkeitsmatrix-Ansicht konfigurieren – das ist das erste Artefakt, das Auditoren anfordern.
- Jira und Azure DevOps verbinden, damit Engineering-Defekte automatisch in aqua zurückfließen.
- Berichtsvorlagen auf die AI-Act-Struktur der Technischen Dokumentation (Anhang IV) sperren, damit Exporte mit einem Klick audit-ready sind.

Ergebnisse

- Konfigurierter aqua Tenant mit SSO, RBAC, Projekten, Feldern und Workflows.
- Importierter Anforderungsrückstand, nach Artikel und Risikostufe gekennzeichnet.
- Generierte Testfallbibliothek (AI Copilot Output, manuell geprüft).
- Funktionierende Rückverfolgbarkeitsmatrix für mindestens ein in-scope KI-System.
- Geschultes QA-Team mit Zertifizierung für aqua-Workflows und Freigabeprozesse.

Hauptverantwortliche

QA-Manager (Konfigurations-Freigabe). QA Engineers (Anforderungsimport, Copilot-Review). Engineering Manager (Integrationsvalidierung). aqua-Administrator (technisches Setup).

PHASE 3

NACHWEISE ERSTELLEN

Tage 26–45

Ziel Testkampagnen durchführen, die die von jedem Artikel des EU AI Acts geforderten Nachweise generieren. Jede Testausführung hinterlässt einen zeitgestempelten, benutzerbezogenen Audit-Trail in aqua. Jeder Defekt ist transparent mit einer Anforderung und einer Behebung verknüpft. Jede Freigabe ist einer namentlich genannten, verantwortlichen Person zugeordnet. Genehmigungen über Slack oder andere Chat-Plattformen sind ausgeschlossen.

Week / Tage	Schwerpunkt	Wichtigste Aktivitäten
Woche 6 (Tage 26–30)	Artikel 9 (Risiko) und Artikel 10 (Data Governance)	• Artikel 9: Laufendes Risikomonitoring in aqua konfigurieren. Defekttrend-Berichte pro Release mit Schweregrad, Häufigkeit und Behebungszeit. • Artikel 9: Risikominderungsmaßnahmen für jedes klassifizierte Risiko dokumentieren; jede Maßnahme mit einem Testfall verknüpfen, der die Wirksamkeit belegt. • Artikel 10: Datenqualitäts- und Repräsentativitätsberichte für Trainings-, Validierungs- und Testdatensätze erstellen. Stichprobenmethodik und Bias-Prüfungen einschließen. • Artikel 10: Herkunft, Version und Zugriffskontrollen der Datensätze dokumentieren. Datensätze mit den Testausführungen verknüpfen, die sie genutzt haben. • Nachweispaket von Woche 6 mit DSB und Compliance freigeben.
Woche 7 (Tage 31–35)	Artikel 11 (Technische Dokumentation) und Artikel 12 (Protokollierung)	• Artikel 11: Bestätigen, dass die aqua-Berichtsvorlage Anhang IV exakt entspricht – Systembeschreibung, Designentscheidungen, Monitoring, Validierung, Genauigkeitskennzahlen, Aufsichtsmaßnahmen. • Artikel 11: Jeden Anhang-IV-Abschnitt aus aqua-Artefakten befüllen statt aus externen Dokumenten zu kopieren. • Artikel 12: Protokollierung konfigurieren, sodass jedes relevante Ereignis im Test-/Validierungslebenszyklus automatisch erfasst wird (wer, was, wann, Ergebnis). • Artikel 12: Bestätigen, dass die Log-Aufbewahrungsrichtlinie das AI-Act-Minimum und die Erwartungen der Branchenaufsicht erfüllt. • Halbphasenreview mit dem Rechtsberater.

Week / Tage	Schwerpunkt	Wichtigste Aktivitäten
Woche 8 (Tage 36–40)	Artikel 13 (Transparenz) und Artikel 14 (Menschliche Aufsicht)	• Artikel 13: Nutzerseitige Gebrauchsanweisungen erstellen, wobei die QA validiert, dass das tatsächliche Systemverhalten exakt mit dem dokumentierten Verhalten übereinstimmt. • Artikel 13: Jeden transparenzbezogenen Test wie Erklärungen, Konfidenzindikatoren und Output-Offenlegungen lückenlos in aqua protokollieren. • Artikel 14: Sicherstellen, dass jede Release-Freigabe zwingend eine namentlich genannte, verantwortliche Person mit der entsprechenden Rolle erfordert. • Artikel 14: Szenarien durchführen, in denen ein menschlicher Prüfer eine KI-Entscheidung überschreibt oder pausiert, und jedes Szenario als dokumentierte Testausführung erfassen. Das Freigabeprotokoll gründlich auf Releases prüfen, die ohne namentlich genannten Genehmiger freigegeben wurden, und etwaige Mängel umgehend beheben.
Woche 9 (Tage 41–45)	Artikel 15 (Genauigkeit, Robustheit, Cybersicherheit)	• Artikel 15: Genauigkeitstests gegen die definierten Kennzahlen und probabilistischen Schwellenwerte durchführen sowie Schwellenwert und Ergebnis für jede Kennzahl dokumentieren. • Artikel 15: Robustheitstests durchführen – einschließlich adversarialer Eingaben, Grenzfälle, Drift-Simulationen und Fallback-Verhalten. • Artikel 15: Cybersicherheitstests gemäß den NIS2-Anforderungen durchführen, sofern relevant, und die Pen-Test-Zusammenfassung in die aqua-Nachweiskette einbinden. Abschließende Regressionstests für jedes relevante KI-System durchführen und den unveränderlichen Nachweispfad für das Release final absichern. • Tag 45: Vollständigkeitsprüfung aller Nachweise gemeinsam mit der Rechts- und Compliance-Abteilung durchführen.

Abschlusskriterien

- ✓ Jede Pflicht aus Artikeln 9–15 hat mindestens einen verknüpften, zeitgestempelten Nachweis in aqua.
- ✓ Kein Release im 60-Tage-Fenster wurde ohne namentlich genannten menschlichen Genehmiger freigegeben
- ✓ Anhang-IV-Technische Dokumentation exportiert aus aqua ohne manuelle Nachbearbeitung.
- ✓ Defekt-bis-Behebung-Kette ist für jedes in-scope Release lückenlos.

aqua cloud Aktivitäten in dieser Phase

- aquas Defekttrend-Tracking als Live-Risiko-Dashboard für Artikel 9 nutzen.
- Jede Testausführung über aqua laufen lassen, damit die Protokolle automatisch befüllt werden – ohne separate Logdateien.
- aqua Capture für jeden manuellen Fund nutzen, damit der Nachweis durch Screenshots und Zeitstempel lückenlos belegt ist.
- Jeden Datensatzeintrag direkt mit den Ausführungen und Anforderungen verknüpfen, die von ihm abhängen.
- Das Release sperren, sobald die Nachweise vollständig sind, um die Unveränderlichkeit der Kette abzusichern.

Ergebnisse

- Artikel-9-Risiko-Dashboard (live in aqua).
- Artikel-10-Data-Governance-Paket (Datensatz-Inventar, Qualitätsberichte, Bias-Prüfungen).
- Anhang-IV-Technische Dokumentation aus aqua-Artefakten befüllt.
- Artikel-12-Ereignisprotokolle für den gesamten Test-/Validierungslebenszyklus.
- Artikel-13-Validierungsbericht für Gebrauchsanweisungen.
- Artikel-14-Freigabeprotokoll mit namentlich genannten menschlichen Genehmigern.
- Artikel-15-Genauigkeits- und Robustheitstestergebnisse.

Hauptverantwortliche

QA Engineers (Ausführung). QA-Manager (Prüfung der Nachweisvollständigkeit). DSB (Freigabe von Artikel 10). Engineering Manager (Freigabe von Artikel 15). Legal Counsel (Prüfung von Artikel 11/13).

PHASE 4

PROBE-AUDIT UND GO-LIVE

Tage 46–60

Ziel Sämtliche Nachweise im Rahmen eines internen Probe-Audits gründlich überprüfen, bevor die offizielle regulatorische Prüfung erfolgt. Jegliche Schwachstellen oder Abweichungen, die dabei identifiziert werden, umgehend beheben. Den Audit-Termin bei der Benannten Stelle verbindlich bestätigen. Das Qualitätsmanagementsystem gemäß Artikel 17 freigeben und das kontinuierliche Monitoring aktivieren, damit die Compliance-Konformität sowohl am Stichtag als auch bei jedem zukünftigen Release lückenlos gewahrt bleibt.

Week / Tage	Schwerpunkt	Wichtigste Aktivitäten
Woche 10 (Tage 46–50)	Probe-Durchlauf und Probe-Audit	• Tag 46: Vollständige Technische Dokumentation direkt aus aqua generieren. Ein Klick, ganz ohne manuelle Zusammenführung. • Tag 47: Internes Probe-Audit durchführen – Rechtsberater und idealerweise ein externer Berater prüfen alle Nachweise auf Herz und Nieren, als wären sie der Regulator. • Tage 48–49: Jede gefundene Abweichung mit Schweregrad und entsprechendem Artikel-Bezug direkt in aqua katalogisieren. T • ag 50: Den Behebungsrückstand priorisieren und den Umfang strikt auf das eingrenzen, was innerhalb von fünf Arbeitstagen lösbar ist.
Woche 11 (Tage 51–55)	Behebungs-Sprint	• Fokussierten Behebungs-Sprint gegen den Probe-Audit-Rückstand durchführen. • Jeden Test erneut ausführen, der in Phase 3 mehrdeutige oder schwache Nachweise erzeugt hat. • Technische Dokumentation erneut exportieren und prüfen, dass jede Behebung in der Nachweiskette abgebildet ist. • Slot bei der benannten Stelle und finales Übergabeformat der Dokumente bestätigen. • Den Executive Sponsor (CTO/CPO) umfassend über verbleibende Restrisiken briefen und die vorgeschlagene Go-live-Entscheidung zur Freigabe vorlegen.
Woche 12 (Tage 56–60)	Go-live, Freigabe, kontinuierliches Monitoring	• Qualitätsmanagementsystem gemäß Artikel 17 prüfen und formal freigeben. • Finale Technische Dokumentation in vereinbartem Format an die benannte Stelle übergeben. • Kontinuierliches Monitoring aktivieren: geplante aqua-Berichte, Defekttrend-Alarme, Datensatz-Drift-Prüfungen, Re-Validierungs-Trigger bei Anforderungsänderungen. • Marktüberwachungsplan (Artikel 72) dokumentiert und einem namentlich genannten Verantwortlichen zugewiesen. • Tag 60: Go/No-go-Review. Programm wechselt vom Projekt- in den Betriebsmodus.

Abschlusskriterien

- ✓ Sämtliche Befunde aus dem Probe-Audit sind vollständig behoben oder verfügen über eine unterzeichnete Freigabe der Rechtsabteilung.
- ✓ Die Benannte Stelle hat die finale Technische Dokumentation erhalten und das Bewertungsfenster ist verbindlich bestätigt.
- ✓ Das Qualitätsmanagementsystem gemäß Artikel 17 ist offiziell unterzeichnet.
- ✓ Das kontinuierliche Monitoring ist in aqua live geschaltet und einer namentlich genannten verantwortlichen Person zugewiesen.
- ✓ Die Pufferwoche (Tage 61–68) bleibt strikt für Last-Minute-Themen reserviert und wird nicht für neue Arbeiten genutzt.

aqua cloud Aktivitäten in dieser Phase

- Technische Dokumentation aus aqua für das Probe-Audit exportieren – Zeit messen; das ist Ihre echte Audit-Reaktionszeit.
- aquas Berichtsplanung nutzen, um den Monitoring-Rhythmus nach dem Compliance-Stichtag zu automatisieren (wöchentlicher Trendbericht, monatliches Compliance-Paket).
- Änderungsgetriebene Re-Validierung konfigurieren: Bei einer Anforderungsänderung markiert aqua jeden betroffenen Testfall.
- Auditierten Release in aqua sperren, damit die Nachweiskette ab dem Auditdatum unveränderlich ist.

Ergebnisse

- nterner Probe-Audit-Bericht mit katalogisierten und behobenen Befunden.
- Finale Technische Dokumentation an die benannte Stelle übergeben.
- Unterzeichnetes Qualitätsmanagementsystem gemäß Artikel 17.
- Kontinuierlicher Monitoring-Plan (Artikel 72) mit Verantwortlichem, Rhythmus und Auslösebedingungen.
- Go/No-go-Entscheidung dokumentiert und vom Executive Sponsor unterzeichnet.

Hauptverantwortliche

QA-Manager (Probe-Audit leiten). Rechtsberater (Regulatorperspektive). Externer Berater (unabhängige Prüfung). CTO/CPO (Go-live-Entscheidung).

EU-AI-Act-Pflicht

aqua cloud Workflow

Diese Tabelle legen Sie einem Auditor direkt am ersten Tag vor. Jede Pflicht ist mit einem einzigen, namentlich benannten Artefakt in aqua verknüpft. Kein Tool-Chaos, keine manuelle Zusammenführung.

EU-AI-Act-Artikel	Was der Regulator fordert	Wo es in aqua liegt
Art. 9 Risikomanagement	Kontinuierliches, lebenszyklusbasiertes Risikomanagementsystem mit dokumentierten Minderungsmaßnahmen.	Defekttrend-Dashboard, Änderungshistorie, risikoklassifizierte Anforderungen und Testfälle, Verknüpfungen Minderungsmaßnahme → Testfall.
Art. 10 Data Governance	Datenqualität, Repräsentativität, Herkunft für Trainings- und Testdaten.	Datensatzeinträge mit Ausführungen verknüpft, Qualitäts- und Bias-Prüfungsnachweise angehängt.
Art. 11 Technische Dokumentation	Anhang-IV-Technische Dokumentation zu Design, Validierung, Monitoring, Genauigkeit.	Ein-Klick-Export der Anhang-IV-Vorlage, befüllt aus Live-aqua-Artefakten.
Art. 12 Protokollierung (Logs)	Automatische Protokollierung relevanter Ereignisse über den Systemlebenszyklus.	aquas Audit-Trail erfasst jede Anforderung, Ausführung, jeden Defekt und jedes Freigabeereignis mit Zeitstempel und Nutzer.
Art. 13 Transparenz	Klare Gebrauchsanweisungen; Verhalten stimmt mit dokumentiertem Verhalten überein.	Transparenzbezogene Testausführungen protokolliert und mit der Version des Gebrauchsanweisungsdokuments verknüpft.
Art. 14 Menschliche Aufsicht	Nachweis, dass ein Mensch an entscheidenden Punkten eingebunden war.	Freigabe-Workflow: Jeder Release und jede Testausführung trägt einen namentlich genannten Genehmiger mit Zeitstempel – keine impliziten Genehmigungen.
Art. 15 Genauigkeit, Robustheit, Cybersicherheit	Leistung gegenüber definierten Kennzahlen und probabilistischen Schwellenwerten.	Genauigkeits-/Robustheitstestsuiten mit aufgezeichneten Kennzahlenschwellenwerten; Ergebnisse mit dem Release verknüpft.
Art. 17 Qualitätsmanagementsystem	Dokumentiertes QMS zu Design, Entwicklung, Testing, Monitoring.	aqua-Workflows bilden selbst das operative QMS; in Kombination mit dem Policy-Paket erfüllen sie Artikel 17.
Art. 43–49 Konformitätsbewertung	Externe Bewertung durch eine benannte Stelle, sofern vorgeschrieben.	Audit-ready Berichtspaket aus aqua exportiert und im vereinbarten Format an die benannte Stelle übergeben.
Art. 72 Marktüberwachung	Laufendes Monitoring der System-leistung nach dem Deployment.	Geplante aqua-Berichte, Defekttrend-Alarme, änderungsgetriebene Re-Validierungs-Trigger.

RACI

R = Responsible (Durchführung).

A = Accountable (Gesamtverantwortung).

C = Consulted (Einbezogen).

I = Informed (Informiert).

Arbeitsbereich	QA Mgr	CTO/CPO	Legal	Compliance	DSB	Eng Mgr	Produkt
Inventar und Klassifizierung des KI-Systems	R	A	C	C	C	R	C
Lückenanalyse (Artikel 9–15, 17)	R	I	A	R	C	C	I
aqua-Tenant-Konfiguration	A	I	I	I	C	R	I
Anforderungsimport & KI-Copilot	R	I	I	I	I	C	C
Testausführung & Nachweiserstellung	R	I	C	C	C	C	I
Artikel-10-Data-Governance-Nachweis	C	I	C	R	A	C	I
Artikel-14-Freigabe menschliche Aufsicht	R	I	C	C	I	A	C
Artikel 15: Genauigkeit & Robustheit	R	I	I	C	I	A	C
Probe-Audit	R	I	A	R	C	C	I
Engagement benannte Stelle	R	A	R	C	I	I	I
Artikel-17-QMS-Freigabe	C	A	R	R	C	C	I
Kontinuierliches Monitoring	A	I	C	C	C	R	I

KPI-Dashboard – Definition der Fertigstellung

Überwachen Sie diese Kennzahlen jeden Freitag im Lenkungsausschuss.
Sollte ein Indikator hinter seinem Phasenziel zurückbleiben, leiten Sie die Eskalation noch vor Montag ein.

KPI	Phase-1-Ziel	Phase-2-Ziel	Phase-3-Ziel	Phase-4-Ziel
KI-Systeme klassifiziert	100%	-	-	-
Anforderungen in aqua importiert	-	100%	-	-
Anforderungen mit verknüpftem Testfall	-	100%	100%	100%
Testausführungen in aqua protokolliert	-	≥30%	100%	100%
Releases mit namentlicher Freigabe	-	100%	100%	100%
Artikel 9–15 Nachweisvollständigkeit	-	≥40%	100%	100%
Befunde aus dem Probe-Audit vollständig behoben	-	-	-	100%
Kontinuierliches Monitoring in aqua aktiv	-	-	-	Yes

Risikoregister

Hauptrisiken für das 60-Tage-Fenster. Die verantwortliche Person prüft den Status wöchentlich im Defect-Tracker von aqua (verwenden Sie hierzu einen dedizierten Vorgangstyp „Programm-Risiko“).

Risiko	Wahrscheinlichkeit / Auswirkung	Minderungsmaßnahme	Verantwortung
Kapazitäten benannter Stellen erschöpft, bevor die Bewertung gebucht ist.	Hoch / Hoch	Buchungsgespräch ab Tag 1 parallel zur internen Arbeit führen. Zwei benannte Stellen auf die Shortlist, nicht nur eine.	QA Mgr
Klassifizierung nach Artikel 6 / Anhang III wird von Legal angefochten.	Mittel / Hoch	Rechtsberater unterzeichnet die Klassifizierung am Ende von Woche 2. Phase-2-Arbeit beginnt nicht für ein angefochtenes System.	Legal
Anforderungen in zu vielen Tools – lassen sich in aqua nicht abgleichen.	Mittel / Mittel	aquas Import-Assistenten für Jira/Confluence/ Excel in Woche 4 ausführen. Abgleich-Reviews an Tagen 17–19.	QA Mgr
Vom AI Copilot generierte Testfälle werden ohne menschliche Prüfung akzeptiert.	Mittel / Hoch	Review-Gate: Ein generierter Testfall gilt nicht als „genehmigt“, bis ein menschlicher QA Engineer ihn unterzeichnet. Durchgesetzt durch aqua-Workflow.	QA Mgr
Datensatzdokumentation für Artikel 10 liegt außerhalb der Reichweite des Datenteams.	Mittel / Hoch	DSB stößt in Woche 6 dazu. Datenteam ist ab Tag 1 im Lenkungsausschuss.	DSB
Freigaben finden auch nach Phase 2 weiterhin über Slack oder E-Mail statt.	Mittel / Hoch	Freigabefeld ist für Release-Issues Pflicht; aqua blockiert den Abschluss ohne es. Protokoll wöchentlich prüfen.	QA Mgr
Späte regulatorische Leitlinien ändern die Anforderungen.	Mittel / Mittel	Rechtsberater überwacht die Bulletins des EU-AI-Büros. Lenkungsausschuss prüft den Scope wöchentlich.	Legal
Engineering ist überlastet und entzieht QA die Testumgebungen	Mittel / Mittel	CTO-Sponsoring des Programms. Umgebungsverfügbarkeit ist ein KPI des Lenkungsausschusses.	CTO/CPO
Probe-Audit deckt Lücken in Woche 10 auf, die nicht in fünf Tagen behoben werden können.	Niedrig / Hoch	Vollständigkeitsprüfung der Nachweise an Tag 45 dient als Vor-Probe. Pufferwoche (Tage 61–68) ist in Reserve.	QA Mgr
Kontinuierliches Monitoring nach dem Compliance-Stichtag ist eingerichtet, aber niemand führt es durch.	Mittel / Hoch	Artikel-72-Verantwortlicher in Phase 4 benannt. Geplante aqua-Berichte + Bereitschaftsplan für Re-Validierungs-Trigger.	Eng Mgr

Tag 61+ – Vom Projekt- in den Betriebsmodus

Compliance ist kein einmaliges Projekt. Der EU AI Act erfordert laufendes Monitoring und Re-Validierung bei Updates von KI-Systemen. Dieselben aqua-Workflows, die das Compliance-Nachweispaket erzeugt haben, laufen bei jedem folgenden Release.

Betriebsrhythmus

- Wöchentlich: Defekttrend-Review und Artikel-9-Risiko-Dashboard.
- Monatlich: Compliance-Paket-Export aus aqua, archiviert gegen die Version der Technischen Dokumentation.
- Pro Release: Kette Anforderung → Testfall → Defekt → Freigabe vor dem Deployment gesperrt.
- Pro Anforderungsänderung: aqua markiert betroffene Testfälle; Re-Validierung ist gezielt, kein Raten.
- Vierteljährlich: Artikel-17-QMS-Review mit Legal und Compliance.
- Jährlich: Artikel-72-Marktüberwachungsbericht und Datensatz-Drift-Bewertung.

The audit you don't see coming

Der Großteil der Durchsetzungsmaßnahmen trifft Systeme, die am ersten Tag compliant waren und danach abgedriftet sind. Kontinuierliches aqua-Reporting ist die günstigste Absicherung gegen diesen Drift.

Anhang A – aqua-Artefakt-Checkliste

Diese Liste als Audit-Paket-Manifest verwenden. Jeder Punkt ist aus aqua exportierbar.

- KI-System-Inventar mit Klassifizierung nach Artikel 6 / Anhang III.
- Anforderungsregister nach Artikel und Risikostufe gekennzeichnet.
- Testfallbibliothek (mit AI Copilot-Herkunftskennzeichnung, sofern zutreffend).
- Rückverfolgbarkeitsmatrix pro KI-System (Anforderung → Testfall → Ausführung → Defekt → Behebung → Freigabe).
- Defektregister mit Ursache, Artikel-Referenz und Behebung.
- Freigabeprotokoll mit namentlich genannten Genehmigern und Zeitstempeln.
- Datensatz-Inventar mit Ausführungen verknüpft (Artikel 10).
- Anhang-IV-Export der Technischen Dokumentation (Artikel 11).
- Ereignisprotokolle für den gesamten Lebenszyklus (Artikel 12).
- Genauigkeits- und Robustheitstestergebnisse (Artikel 15).
- Artikel-17-QMS-Dokumentenpaket.
- Marktüberwachungsplan (Artikel 72).

Anhang B – Referenzen

aqua cloud EU AI Act Webinar-Landingpage:	https://aqua-cloud.io/eu-ai-act-webinar/
aqua cloud Plattformübersicht:	https://aqua-cloud.io/
EU AI Act – Article 9 (Risiko Management System):	https://artificialintelligenceact.eu/article/9/
EU AI Act – Implementierungszeitplan:	https://artificialintelligenceact.eu/implementation-timeline/
Kapazitätskontext benannte Stellen:	https://eyreact.com/notified-bodies-ai-act/

AI-Act-Compliance-Walkthrough buchen (aqua): 

Nächster Schritt

Buchen Sie vor Tag 5 eine 30-minütige Compliance-Durchsprache (Walkthrough) mit aqua. Bringen Sie das KI-Systeminventar aus Phase 1 mit in den Termin, damit das Gespräch direkt an Ihrer spezifischen Situation ansetzt und nicht mit einer generischen Produkt-Demo startet.