AI Operations Handbook

Operatives AI Governance Handbook für Finanzinstitute

Dokumenttyp: Operatives AI Governance Handbook für Finanzinstitute

Version: V2.0 · Status: Published Version · Datum: 12.07.2026

Owner: Martin Bischoff · 4T2 Solutions GmbH

Public · Frei verfügbares Rahmenwerk

Dokumentkontrolle

Feld	Wert
Dokumentname	AI Operations Handbook
Version	V2.0
Status	Published Version
Vertraulichkeit	Public · Frei verfügbares Rahmenwerk
Owner	Martin Bischoff
Review-Zweck	Publizierte Version

Inhaltsverzeichnis

1. Zweck, Zielgruppe und Verwendung

Zweck

Das Operations Handbook für Artificial Intelligence (AI) übersetzt das verbindliche Entscheidungsmodell des **AI Governance Framework for Financial Institutions** in ausführbare Workflows. Es legt fest, wann ein Workflow startet, wer ihn führt, wie die Entscheidung zustande kommt und welche Evidence abgelegt wird.[1]

Zielgruppe

Das Handbook richtet sich an AI Owner, Fachbereiche, System Owner, operative Kontrollfunktionen sowie Projekt-, Plattform- und Beschaffungsteams. Sie verwenden es, wenn ein AI Use Case erfasst, klassifiziert, freigegeben, betrieben, revalidiert oder stillgelegt wird.

Beantwortete Managementfrage

Wie werden die im AI Governance Framework for Financial Institutions verlangten Entscheidungen im Tagesgeschäft verlässlich vorbereitet, ausgeführt und übergeben?

Beziehung zur Dokumentenfamilie

Das AI Governance Framework for Financial Institutions definiert Rollen, Entscheidungswege und den AI Governance Lifecycle. Der AI Control Standard bestimmt die prüfbaren Safeguards und erforderlichen Evidence. Die AI Security Baseline legt die technischen Mindestanforderungen fest. Das Handbook verbindet diese Vorgaben durch operative Workflows und eindeutige Handoffs.

Erwartete Ergebnisse und Abgrenzung

Die Anwendung des Handbooks erzeugt nachvollziehbare Entscheidungen, gepflegte Registereinträge, auffindbare Evidence und einen klaren Handoff an den nächsten Workflow. Es wird nicht verwendet, um den AI Risk Appetite festzulegen, Safeguards neu zu definieren oder technische Mindestanforderungen zu ersetzen.

Methodische Grundlage

Erklärungen und Leserführung folgen Digital.gov und der 4T2 Professional Prose. Workflows verwenden die chronologische Prozesslogik von Digital.gov und offene Muster der U.S. Cybersecurity and Infrastructure Security Agency (CISA) für Trigger, Rollen, koordinierte Aktionen, Entscheidungen, Eskalationen und Records. Die methodische Nutzung begründet keine CISA-Konformität.

---

1 Ein Workflow ist hier eine wiederholbare operative Abfolge mit Trigger, Owner, Input, Ablauf, Entscheidung, Ergebnis, Evidence und Handoff. Er ersetzt keine fachliche oder rechtliche Einzelfallentscheidung.

2. Rollen, Handoffs und Arbeitsprinzipien

Operative Verantwortung entsteht dort, wo ein Arbeitsschritt ein eindeutiges Ergebnis und einen verlässlichen Empfänger hat. Die Rollenübersicht ordnet deshalb nicht nur Aufgaben zu, sondern schafft die Grundlage für vollständige Handoffs zwischen den beteiligten Funktionen.

Rolle	Operative Aufgabe
Geschäftsleitung	AI Risk Appetite und wesentliche Eskalationen als Managemententscheide behandeln
AI Owner	AI Use Case führen, Zweck erklären, Freigaben vorbereiten
System Owner / IT Operations	Betrieb, Integration und Change koordinieren
Fachbereich	Prozesswirkung, Nutzergruppe und fachliche Kontrolle beschreiben
CISO	Security Review und technische Freigabefähigkeit unterstützen
Compliance / Legal	AI-Act-Rolle und Rechtsrisiken prüfen; eine erforderliche Grundrechte-Folgenabschätzung (FRIA) führen und zur Entscheidung bringen
Datenschutz	Datenschutz-Folgenabschätzung (DSFA), Rechtsgrundlage und Betroffenenrisiken prüfen; die DSFA-Schnittstelle zur FRIA verantworten
Risk Management	Risikoappetit, Risikoprofil und Modellrisiko einordnen
Data Owner	Datenquelle, Qualität und Nutzungserlaubnis bestätigen
Enterprise Architecture	Zielarchitektur, Plattformstrategie und Integrationsentscheide einordnen
Einkauf / Auslagerungsmanagement	Bezug zum Digital Operational Resilience Act (DORA), Supplier, Vertrag und Exit steuern
Interne Revision	Design und Wirksamkeit unabhängig prüfen, ohne operative Freigaben zu erteilen

Jeder Workflow endet mit einem dokumentierten Ergebnis, einer auffindbaren Evidence und einem Handoff. Ohne eindeutigen Handoff ist der Workflow nicht abgeschlossen.

Bei einer FRIA führt Compliance / Legal den Workflow. Der AI Owner beschreibt Zweck und fachliche Wirkung; Fachbereich, Risk Management, System Owner, CISO und Datenschutz liefern die für ihren Verantwortungsbereich erforderlichen Beiträge. Die FRIA bleibt eine eigenständige Grundrechte-Folgenabschätzung und wird mit einer erforderlichen DSFA verknüpft, aber nicht gleichgesetzt.

3. Workflow-Grundmuster

Alle Workflows folgen demselben Muster.

Das Muster ist kein Formularzwang. Es ist eine kurze Vollständigkeitsprüfung für die operative Arbeit: Ein Team muss wissen, warum es startet, wer führt, was entschieden wird und wohin das Ergebnis geht. Felder dürfen in bestehenden Tools und Prozessen geführt werden, solange Entscheidung und Evidence eindeutig auffindbar bleiben.

Feld	Bedeutung
Trigger	Anlass, der den Workflow startet
Owner	führende Rolle
Input	erforderliche Informationen

Feld	Bedeutung
Ablauf	operative Schritte
Entscheidung	Entscheidung oder Routing
Ergebnis	dokumentiertes Ergebnis
Evidence	Nachweis für AI Control Standard und Prüfung
Handoff	nächster Workflow oder Zielrolle

Für jeden Workflow gilt eine gemeinsame Eskalationsregel: Fehlen Pflichtinputs, bleibt eine Entscheidung unklar oder wird ein Stop-Signal erkannt, dokumentiert der Owner den offenen Punkt und übergibt ihn an die zuständige Fach- oder Entscheidungsrolle. Der Workflow darf erst fortgesetzt werden, wenn die Eskalation entschieden oder ein zulässiger befristeter Pfad dokumentiert ist. Der Ausschlussstatus X erlaubt keinen befristeten Freigabepfad.

4. Orientierung: AI-Signal früh erfassen

Die Orientierung ist die leichteste operative Routine. Sie erfasst ein AI-Signal, bevor ein formaler Intake nötig ist.

Trigger, Owner und Input. Eine neue Idee, Marktbeobachtung, ein Fachbereichsimpuls, ein Tool-Fund oder Anbieterhinweis startet den Workflow. Der Ideengeber oder Fachbereich führt ihn.

Ablauf und Entscheidung. Der Owner hält Zweck, erwarteten Nutzen, betroffene Nutzergruppe sowie erkennbare Daten- oder Tool-Bezüge fest, markiert offensichtliche Stop-Signale und schlägt einen AI Owner vor. Danach wird entschieden, ob das Signal beobachtet, in die Portfolio-Sichtung übernommen oder direkt dem Intake zugeführt wird.

Ergebnis, Evidence und Handoff. Ergebnis und Evidence sind die AI Idea Note und die dokumentierten Stop-Signale. Der Handoff führt zur Portfolio-Steuerung oder zum Intake.

5. Portfolio-Steuerung: Sichtung und Priorisierung

Die Portfolio-Steuerung bündelt frühe Signale und bestimmt, welche Vorhaben in den Intake gelangen. Die Entscheidungslogik ist im AI Governance Framework for Financial Institutions definiert.

Trigger, Owner und Input. Eine neue AI Idea Note, die periodische Portfoliosichtung oder ein strategischer Bedarf startet den Workflow. Der AI Governance Lead oder Portfolio Owner führt ihn.

Ablauf und Entscheidung. Auf Grundlage von Nutzenannahme, groben Risikosignalen, Kapazität und strategischer Passung werden Vorhaben gebündelt, Dopplungen erkannt und priorisiert. Die Entscheidung lautet: Intake starten, zurückstellen, bündeln oder stoppen.

Ergebnis, Evidence und Handoff. Die Portfolio Steering Note dokumentiert Priorisierung, Entscheidung und Portfolio-Status. Freigegebene Kandidaten gehen in den Intake.

6. Intake: AI Use Cases sichtbar machen

Der formale Intake beginnt, sobald aus einem AI-Signal ein konkret prüfbarer AI Use Case, ein Tool- oder Pilotvorhaben oder ein Shadow-AI-Fall wird. Der Zweck ist nicht eine vollständige rechtliche Bewertung, sondern Owner-Zuordnung, Registererfassung und richtiges Routing.

Trigger, Owner und Input. Ein neuer AI Use Case, ein neues Tool, ein Pilot, ein Shadow-AI-Fund oder eine neue AI-Funktion startet den Intake. Der AI Owner oder anfragende Fachbereich führt ihn.

Ablauf und Entscheidung. Zweck, Nutzergruppe, Datenarten, Anbieter, grobe Architektur und erwarteter Nutzen werden erfasst. Der Workflow benennt einen vorläufigen Owner, prüft den Scope, kennzeichnet Shadow AI und bestimmt das nächste Assessment. Die Entscheidung unterscheidet zwischen Ausnahme, vereinfachter Behandlung und vollständiger Prüfung.

Ergebnis, Evidence und Handoff. Der AI Intake Record enthält den Shadow-AI-Vermerk und die Routing-Entscheidung. Der Handoff führt zur Klassifikation oder zum erforderlichen Supplier-, Datenschutz- oder Security Assessment.

7. Vorprüfung: Scope, AI-System, Rolle und Datenbezug

Die Vorprüfung klärt, ob die AI Governance greift und welche Rollen beteiligt werden. Sie vermeidet, dass ein Projekt zu spät erfährt, dass Rechts-, Daten- oder Supplier-Fragen entscheidend sind.

Trigger, Owner und Input. Eine prüfpflichtige Intake-Entscheidung startet die Vorprüfung. Compliance / Legal führt sie gemeinsam mit dem AI Owner.

Ablauf und Entscheidung. Intake Record, Systembeschreibung, Zweck, Nutzer, Datenarten, Rechtseinheit und Einsatzländer bilden den Input. Der Workflow prüft die Nähe zu einem AI-System und erfasst Provider-, Deployer-, Importeur-, Distributor- und Produktherstellerrollen. Rebranding, wesentliche Änderung und Zweckänderung werden als mögliche Art.-25-Rollenwechsel geprüft. Der Workflow markiert den Datenbezug, setzt erste Trigger und routet in die vollständige Klassifikation, die normale IT-Prüfung oder zum Stop.

Ergebnis, Evidence und Handoff. Das Scope and Role Assessment enthält Einstufungsnotiz, Anbieterinformationen und Rollenbewertung. Der Handoff führt zum Risikoprofil, Applicability Statement und den ausgelösten Fachworkflows.

8. Klassifikation und Risikoprofil

Die Klassifikation übersetzt den AI Use Case in eine Profilklasse. Die Profilklasse steuert die Kontrolltiefe im AI Control Standard und die technische Mindestlinie in der AI Security Baseline.

Trigger, Owner und Input. Eine abgeschlossene Vorprüfung oder die neue Nutzung einer bestehenden Plattform startet die Klassifikation. Der AI Owner führt sie und bindet Risk Management, Compliance, Datenschutz und Security gemäss den Triggern ein.

Ablauf und Entscheidung. Scope Assessment, Zweck, Datenarten, Prozesswirkung, Supplier und technische Rechte werden bewertet. Daraus folgen Profilklasse B, E, C oder H beziehungsweise der Ausschlussstatus X, die massgeblichen Trigger sowie der Bedarf an Management- oder Gremienentscheiden.

Ergebnis, Evidence und Handoff. Der Risk Profile Record dokumentiert die Begründung der Profilklasse, Trigger Matrix und Eskalationsnachweis. Der Handoff führt zum Applicability Statement sowie zur Betriebsfreigabe und Nutzungsfreigabe.

8a. AI-Act-Anwendbarkeit und Provider-Aktivierungsentscheid

Dieser Workflow begrenzt jede Vollständigkeitsfeststellung auf den konkreten Fall. Er verhindert zugleich, dass eine Eigenentwicklung oder wesentliche Änderung irrtümlich nur als Deployer-Nutzung freigegeben wird.

Trigger, Owner und Input. Jede formale Klassifikation sowie Eigen-/Auftragsentwicklung, Inbetriebnahme unter eigenem Namen oder eigener Marke, Rebranding, Zweckänderung und wesentliche Änderung starten den Workflow. Compliance / Legal führt ihn mit AI Owner und System Owner. Inputs sind Rechtseinheit, Länder, Systemversion, Zweck, Entwicklungs- und Marktmodell sowie die Annex- und Rolleninformationen.

Ablauf und Entscheidung. Der Workflow entscheidet Scope und Ausnahmen, jede Operatorrolle, Anhang-I-Relevanz und jede einschlägige Nummer von Anhang III. Das Art.-6-Abs.-3-Reasoning Sheet beurteilt, ob ein signifikantes Risiko für Gesundheit, Sicherheit oder Grundrechte besteht und ob das System den Entscheidungsausgang wesentlich beeinflusst. Es ordnet ausserdem den gesetzlichen Ausnahmetatbestand zu: enge Verfahrensaufgabe, Verbesserung eines menschlichen Ergebnisses, Muster- oder Abweichungserkennung ohne Ersatz oder Einfluss auf die menschliche Bewertung oder vorbereitende Aufgabe. Begründung und Registrierungsfolge werden genehmigt. Danach prüft der Workflow die unmittelbare Providerdefinition und einen Art.-25-Rollenwechsel. Der Entscheid lautet: Deployer-Pfad, Provider-Aktivierung oder spezialisiertes Handoff. Importeur-, Distributor-, Annex-I-Produkthersteller-, eigene GPAI-Modellprovider- und formelle Real-World-Testing-Signale führen zu Stop bis zum Spezialentscheid.

Ergebnis, Evidence und Handoff. Scope and Role Assessment, High-Risk Classification Record und Provider Activation Record aktualisieren das Requirements and Applicability Record. Ein positiver Providerentscheid aktiviert den Provider Compliance Plan und blockiert Betriebs- und Nutzungsfreigabe bis zu dessen Genehmigung. Der Plan weist die Deliverables aus Art. 9–21, 43, 47–49 und 72–73 sowie den einschlägigen Anhängen zu; das Handbook ersetzt kein allgemeines Herstellerhandbuch.

Eine Rückkehr in den Deployer-Pfad ist nur zulässig, wenn Legal / Compliance die Providerrolle begründet ausschliesst. Bei bestätigter Providerrolle ersetzt allein die Release-Entscheidung des Provider-Compliance-Prozesses den Stop; ein informeller Handoff oder ein unvollständiger Plan genügt nicht.

9. Assessment Workflows

Assessment Workflows werden nur gestartet, wenn Profilklasse oder Trigger sie auslösen.

Damit bleibt die Arbeitsweise proportional. Ein einfacher interner AI Use Case soll nicht durch Spezialassessments blockiert werden. Sobald Personenwirkung, kritische Prozesse, externe Anbieter oder erhöhte technische Rechte hinzukommen, sorgt das Routing dafür, dass die richtige Fachfunktion früh und mit einem klaren Entscheidungsauftrag beteiligt wird.

Assessment	Trigger	Ergebnis
Privacy Assessment	personenbezogene Daten, Art.-22-Nähe, DSFA-Signal	Privacy Assessment Record
Grundrechte-Folgenabschätzung (Fundamental Rights Impact Assessment, FRIA)	Art.-27-Trigger aufgrund Betreiberart oder Annex III № 5(b)/(c), sonst interner Fundamental-Rights-Trigger[2]	FRIA Record
Supplier Assessment	externe Leistung oder Modellanbieter	Supplier Assessment
Security Assessment	technische Plattform, Integration, RAG, Agent oder externe AI	Security Evidence Package
Model Risk Assessment	bankfachliche Modellwirkung	Model Risk Handoff
Architecture Assessment	neue Plattform oder wesentliche Integration	Architecture Decision
EU Database Registration Assessment	Annex-III-System, Providerstatus, Art.-6-Abs.-3-Ausnahme, öffentliche Deployerrolle oder Handeln im Auftrag einer öffentlichen Stelle	Registration Decision Record; bei Pflicht zusätzlich EU Database Registration Evidence

FRIA und EU-Datenbankregistrierung bleiben getrennte Entscheidungen. Ein FRIA-Trigger führt nicht automatisch zu einer Registrierungspflicht; umgekehrt ersetzt eine Registrierung keine FRIA-Prüfung.

9a. Grundrechte-Folgenabschätzung nach Art. 27

Die Grundrechte-Folgenabschätzung (Fundamental Rights Impact Assessment, FRIA) wird vor der ersten Nutzung abgeschlossen. Für Finanzinstitute sind insbesondere Kreditwürdigkeitsprüfung nach Anhang III № 5(b) sowie Risiko- und Preisbewertung in der Lebens- und Krankenversicherung nach № 5(c) relevant. Ein Hochrisikostatus allein löst die FRIA nicht pauschal aus.

Trigger, Owner und Input. Der bestätigte Art.-27-Trigger startet den Workflow. Compliance führt ihn mit AI Owner, Datenschutz, Risk Management und den betroffenen Fachfunktionen. Inputs sind Zweck und Prozess, Art.-13-Informationen, Personengruppen, Nutzungsdauer und -häufigkeit, Human Oversight, technische Wirkungs- und Monitoringdaten sowie eine vorhandene Datenschutz-Folgenabschätzung (DSFA).

Ablauf und Entscheidung. Die FRIA beschreibt Prozess und Zweck, Dauer und Häufigkeit, betroffene Gruppen und die spezifischen Grundrechtsschäden. Sie beurteilt Oversight und Schutzmassnahmen einschliesslich Governance- und Beschwerdewegen. Eine frühere FRIA darf nur bei hinreichend ähnlicher Nutzung wiederverwendet werden. Änderungen oder Überalterung lösen eine Aktualisierung aus. Die DSFA kann verbunden werden, ersetzt die FRIA aber nicht.

Ergebnis, Evidence und Handoff. Das Approved FRIA Record enthält alle Pflichtfelder, Freigabe

2 Art. 27 AI Act regelt die Grundrechte-Folgenabschätzung für bestimmte Betreiber und bestimmte Hochrisiko-Anwendungen. Ein interner Fundamental-Rights-Check kann bewusst weiter gefasst sein, ist dann aber als interne Governance-Anforderung zu kennzeichnen.

und Änderungsdatum. Compliance übermittelt das Ergebnis mit dem vorgesehenen Template an die Marktüberwachungsbehörde, soweit keine gesetzliche Ausnahme greift, und legt Notification Evidence oder Ausnahmebegründung ab. Ohne Abschluss bleibt die Nutzungsfreigabe blockiert.

10. Betriebsfreigabe

Die Betriebsfreigabe entscheidet, ob Plattform, Modell oder technische Umgebung unter definierten Bedingungen betrieben werden kann. Sie entscheidet nicht, ob ein konkreter fachlicher AI Use Case erlaubt ist.

Trigger, Owner und Input. Der geplante technische Betrieb eines AI-Systems oder einer Plattform startet den Workflow. Der System Owner führt ihn mit CISO und IT Operations.

Ablauf und Entscheidung. Architektur, Supplier Assessment, Evidence aus der AI Security Baseline sowie Logging und Monitoring werden gegen die technische Mindestlinie geprüft. Offene Findings führen zu Betriebsauflagen oder einer Risk Acceptance. Die Entscheidung lautet: freigeben, einschränken, nachfordern oder ablehnen.

Ergebnis, Evidence und Handoff. Der Betriebsfreigabe-Record verweist auf Architekturdiagramm, Security-Evidence, Supplier-Freigabe und Monitoring-Nachweis. Der Handoff führt zur Nutzungsfreigabe, zum Monitoring und bei Änderungen zur Revalidierung.

11. Nutzungsfreigabe

Die Nutzungsfreigabe entscheidet über den konkreten AI Use Case. Sie prüft Zweck, Daten, Nutzergruppe, Output-Wirkung und Human Oversight.

Trigger, Owner und Input. Der beabsichtigte Einsatz von AI für einen konkreten fachlichen Zweck startet den Workflow. Der AI Owner führt ihn.

Ablauf und Entscheidung. Betriebsfreigabe, Risikoprofil, Datenarten, Nutzergruppe, Human Oversight und Transparenzbedarf bilden die Grundlage. Zweck und Datenfreigabe werden geprüft, die menschliche Aufsicht wird zugeordnet und Nutzungsbedingungen werden festgelegt. Die Entscheidung lautet: erlauben, einschränken, nachfordern oder ablehnen.

Ergebnis, Evidence und Handoff. Der Nutzungsfreigabe-Record verweist auf Freigabeprotokoll, Nutzungsbedingungen, Oversight-Nachweis und Revalidierungsdatum. Der Handoff führt in den produktiven Betrieb, das Monitoring, die erforderliche Schulung und die Evidenzablage.

11a. Betrieb als Hochrisiko-Deployer

Die Nutzungsfreigabe eines Hochrisiko-Systems aktiviert zusätzliche Betreiberpflichten. Sie werden als ein zusammenhängender Betriebsnachweis geführt und nicht auf allgemeine Freigabe-, Trainings- oder Incident-Unterlagen verteilt.

Trigger, Owner und Input. Eine bestätigte Hochrisiko-Deployerrolle startet den Workflow. Der AI Owner führt ihn mit System Owner, Data Owner, Human-Oversight-Rolle, Compliance, Datenschutz und Incident Management. Inputs sind Betriebsanleitung, Inputquellen, Oversight-Konzept, Monitoring, Logs und betroffene Personen- oder Beschäftigtengruppen.

Ablauf und Entscheidung. Das Team beschafft die aktuelle Betriebsanleitung des Providers, hält ihre Version fest und gleicht Nutzungsbedingungen und technische Konfiguration dagegen ab. Abweichungen werden nicht informell akzeptiert, sondern lösen eine Rollen- und Rechtsentscheidung aus. Danach prüft das Team kompetente und befugte Oversight-Personen, relevante und hinreichend repräsentative kontrollierbare Inputs sowie Monitoring und Stop. Automatisch erzeugte Logs unter der Kontrolle des Instituts werden mindestens sechs Monate oder nach einer längeren anwendbaren Regel aufbewahrt. Vor Arbeitsplatznutzung werden Arbeitnehmervertretung und betroffene Beschäftigte informiert. Bei einer einschlägigen Annex-III-Entscheidung wird die betroffene Person über den Einsatz informiert; die DSFA erhält die erforderlichen Informationen.

Ergebnis, Evidence und Handoff. Der High-Risk Deployer Operation Record verbindet Instruction Conformance, Oversight Assignment, Input Control, Monitoring, Retention, Workforce Information und Affected-Person Notice. Zwei Ereignispfade bleiben getrennt:

1. Hat das Institut Grund zur Annahme, dass die anleitungsgemässe Nutzung ein Risiko nach Art. 79 Abs. 1 erzeugen kann, setzt es die Nutzung unverzüglich aus. Es informiert ohne unangemessene Verzögerung den Provider oder Distributor und die zuständige Marktüberwachungsbehörde. Das Risk Suspension and Notification Record belegt Zeitpunkt, Entscheidung, technische Aussetzung und jede Mitteilung.
2. Bei einem schwerwiegenden Vorfall informiert Incident Management sofort zuerst den Provider. Danach informiert es den Importeur oder Distributor und die zuständige Marktüberwachungsbehörde. Ist der Provider nicht erreichbar, dokumentiert es Kontaktversuche und aktiviert den gesetzlichen Ersatzpfad. Das Serious Incident Notification Record hält Reihenfolge, Zeitpunkte, Adressaten und Evidence fest.

Legal / Compliance koordiniert begründete Behördenanfragen und legt die Zusammenarbeit als Evidence ab. Bestehende DORA-, Modellrisiko- oder andere Finanzaufsichts-Monitoring- und Dokumentationsevidence wird im Operation Record eindeutig den einschlägigen Art.-26- Pflichten zugeordnet. Eine sektorale Erfüllungsregel für Finanzdienstleistungen wird dokumentiert; sie hebt die übrigen Deployerpflichten nicht auf.

11b. Transparenz nach Art. 50

Art. 50 enthält unterschiedliche Pflichten für Provider und Deployer. Der Workflow hält Interaktionshinweise, Hinweise bei Emotionserkennung oder biometrischer Kategorisierung, Disclosure für Deepfakes und Texte von öffentlichem Interesse sowie technische Markierung auseinander.

Trigger, Owner und Input. Direkte Interaktion mit natürlichen Personen, Emotionserkennung, biometrische Kategorisierung oder synthetische Inhalte starten den Workflow. Der AI Owner führt ihn mit Legal / Compliance, Communications, Accessibility und System Owner.

Ablauf und Entscheidung. Das Team bestimmt Tatbestand, verpflichtete Rolle, Adressaten, Inhalt, Kanal und Zeitpunkt. Hinweise müssen klar, unterscheidbar, barrierefrei und spätestens bei erster Interaktion oder Exposition erfolgen. Deepfakes und AI-generierte oder manipulierte Texte von

öffentlichem Interesse werden offengelegt. Eine Ausnahme wegen menschlicher Prüfung und redaktioneller Verantwortung wird begründet. Bei eigener Providerrolle wird eine technisch machbare maschinenlesbare Markierung entworfen und auf Wirksamkeit, Interoperabilität, Robustheit und Zuverlässigkeit geprüft.

Ergebnis, Evidence und Handoff. Transparency Decision Record, Notice, Publication Record, Exception Record und gegebenenfalls Marking Detection Test werden vor Nutzung oder Veröffentlichung freigegeben und im AI Register referenziert.

11c. Erläuterungsanfragen nach Art. 86

Dieser Workflow gilt nur für eine qualifizierende Entscheidung auf Basis des Outputs eines erfassten Annex-III-Hochrisiko-Systems. Eine interne Service Level Agreement (SLA) steuert die Bearbeitung, wird aber nicht als gesetzliche AI-Act-Frist dargestellt.

Trigger, Owner und Input. Eine Anfrage oder ein erkennbarer Erläuterungsbedarf bei einer rechtlich oder ähnlich erheblich wirkenden, nachteiligen Entscheidung startet den Workflow. Der verantwortliche Kunden-, Kredit-, Versicherungs- oder HR-Prozess führt ihn mit Legal / Compliance und AI Owner.

Ablauf und Entscheidung. Legal / Compliance prüft Anhang-III-Bezug, Ausnahme für Anhang III № 2, Wirkung, Grundrechtsbezug und Subsidiarität zu einem anderweitigen Unionsrecht. Zusätzlich muss die Entscheidung Gesundheit, Sicherheit oder Grundrechte nachteilig berühren. Bei bestätigtem Anspruch bereitet der Process Owner eine klare und aussagekräftige Erläuterung zur Rolle des Systems und zu den Hauptelementen der Entscheidung vor. Fachfunktion und Legal / Compliance geben sie frei.

Ergebnis, Evidence und Handoff. Explanation Applicability Decision, freigegebene Antwort, Zustellnachweis und verwendete Entscheidungs-Evidence bilden den Explanation Response Record. Datenschutz- oder Beschwerdeprozesse bleiben verknüpft.

12. Beschaffung und Supplier Review

Supplier Review sorgt dafür, dass externe AI-Leistungen kontrollierbar bleiben. Er ersetzt nicht Einkauf, Datenschutz oder Auslagerungsmanagement. Er verbindet diese Funktionen.

Trigger, Owner und Input. Ein externer Anbieter, Software as a Service mit AI (SaaS-AI), General-Purpose AI (GPAI), ein Modelllieferant oder Unterauftragnehmer startet den Supplier Review. Einkauf / Auslagerungsmanagement führt ihn.

Ablauf und Entscheidung. Leistungsbeschreibung, Datenarten, Vertragsentwurf, Subdienstleister, Security-Evidence und Exit-Informationen werden geprüft. Der Workflow klärt den DORA-Bezug, startet den Datenschutz-Handoff, fordert Security-Nachweise an und bewertet den Exit. Die Entscheidung lautet: freigeben, Auflagen setzen, Risk Acceptance einholen oder ablehnen.

Ergebnis, Evidence und Handoff. Das Supplier Assessment verweist auf Supplier Record, Vertragscheck, Auftragsverarbeitungsvertrag (AVV), DORA-Check[3] und Exit-Plan. Der Handoff führt

3 DORA verlangt eine risikobasierte ICT-Drittparteiprüfung; bei Unterstützung kritischer oder wichtiger

zur Betriebsfreigabe, zum Datenschutz und zum Applicability Statement.

13. Datenschutz-, Legal-, Risk- und Security-Handoffs

Handoffs werden ausgelöst, wenn der Workflow eine Spezialentscheidung braucht. Das Handbook routet die Arbeit. Es ersetzt nicht das Fachurteil der Spezialfunktion.

Bei externer GPAI-Nutzung umfasst das Security-Handoff auch den Datenpfad vor dem Modell. Für Prompts, Dateianhänge, Quellcode und automatisch bereitgestellten Kontext wird festgelegt, welche Datenklassen zulässig sind und welcher Enforcement Point die Prüfung übernimmt. Blockierungen, Maskierungen, Umgehungsversuche und genehmigte Ausnahmen werden an AI Owner und Security weitergeleitet und als Evidence abgelegt.

Handoff	Typischer Trigger	Ergebnis
Datenschutz	personenbezogene Daten oder DSFA-Signal[4]	Privacy Assessment
Legal / Compliance	AI-Act-Rolle, Art. 25, Art. 49, Art. 50, FRIA oder verbotene Praktik	Legal / Compliance Decision, gegebenenfalls Registration Decision Record
Risk Management	Profilklasse C oder H, Modellrisiko oder Risk Acceptance	Risk Decision
CISO / Security	technische Plattform, RAG, Agent, externe AI	Security Evidence Package
Enterprise Architecture	neue Plattform oder Integration	Architecture Decision

14. Pilot, Sandbox und Real-World Testing

Pilot und Sandbox sind begrenzte Lernräume. Sie sind keine produktive Nutzung ohne Governance.

Trigger, Owner und Input. Der geplante begrenzte Test eines AI Use Cases startet den Workflow. Der AI Owner führt ihn mit dem System Owner.

Ablauf und Entscheidung. Testzweck, Datenlimits, Nutzerkreis, Laufzeit, Monitoring und Abbruchkriterien werden festgelegt. Testdaten und Pilotgrenzen werden geprüft, das Monitoring wird aktiviert und die Abschlussentscheidung vorbereitet. Der Pilot wird gestartet, begrenzt, abgebrochen oder in den Freigabepfad überführt.

Vor Start entscheidet Legal / Compliance, ob es sich um einen normalen internen Pilot, eine regulatorische Sandbox oder formelles Real-World Testing nach Art. 60 AI Act handelt. Ein formelles Real-World-Testing-Signal aktiviert AI PAC-03 und blockiert den Test bis ein spezialisierter Plan mit Rechtsweg, Schutzvorkehrungen, Information oder Einwilligung, Meldung und Stop-Regeln genehmigt ist.

Ergebnis, Evidence und Handoff. Der Pilot Record verweist auf Pilotfreigabe, Testbericht und

---

Funktionen gelten insbesondere Art. 28-30.

4 Art. 35 DSGVO verlangt eine Datenschutz-Folgenabschätzung bei voraussichtlich hohem Risiko für die Rechte und Freiheiten natürlicher Personen.

Abschlussentscheidung. Der Handoff führt zur Betriebsfreigabe, Nutzungsfreigabe oder Stilllegung.

15. Produktiver Betrieb und Monitoring

Im produktiven Betrieb prüft der AI Owner, ob die Nutzung innerhalb der Freigabe bleibt. System Owner und Security liefern technische Signale.

Trigger, Owner und Input. Die Betriebsfreigabe und Nutzungsfreigabe starten den produktiven Betrieb. Der AI Owner führt die laufende Prüfung mit dem System Owner.

Ablauf und Entscheidung. Freigaben, Monitoring-Signale, Findings, Incidents und Nutzerfeedback werden geprüft. Findings werden weitergeleitet, Reporting Inputs bereitgestellt und Abweichungen eskaliert. Daraus folgt der Weiterbetrieb, eine Einschränkung, die Revalidierung oder der Incident Workflow.

Ergebnis, Evidence und Handoff. Die Operating Review Note verweist auf Monitoring Summary, Finding Log und Reporting Input. Der Handoff führt zur Revalidierung, zum Incident Workflow oder zum Management Reporting.

16. Revalidierung und Change Trigger

Revalidierung startet, wenn sich Risiko oder Wirkung ändern. Der Workflow entscheidet, ob Freigaben gültig bleiben.

Trigger, Owner und Input. Änderungen an Zweck, Daten, Modell, Prompt, Supplier, Tool-Rechten, Rechtslage oder Bedrohungslage starten die Revalidierung. Der AI Owner führt sie.

Ablauf und Entscheidung. Bestehende Freigaben, Änderungsbeschreibung, Monitoring-Signale, Findings und Supplier-Informationen werden ausgewertet. Der Owner identifiziert betroffene Entscheidungen, bindet die zuständigen Fachfunktionen ein und aktualisiert die Evidence. Die Freigabe wird bestätigt, eingeschränkt, erneuert oder entzogen.

Ergebnis, Evidence und Handoff. Der Revalidierungs-Record verweist auf Änderungsnachweis, aktualisierte Freigaben und eine aktualisierte Risk Acceptance. Der Handoff führt zum Applicability Statement, zur Betriebsfreigabe, Nutzungsfreigabe oder Stilllegung.

17. Incident Workflow und Eskalation

Incident Workflow verbindet schnelle Begrenzung, Beweissicherung und parallele Meldeprüfung.

Trigger, Owner und Input. Der Verdacht auf einen AI-bezogenen Sicherheits-, Datenschutz-, Modell-, Supplier- oder Nutzungsincident startet den Workflow. Incident Management führt ihn mit CISO und AI Owner.

Ablauf und Entscheidung. Meldung, System, AI Use Case, Zeitpunkt, Nutzer, Output, Logs und Anbieterinformationen bilden den Input. Das Team triagiert den Vorfall, begrenzt den Schaden, sichert Evidence und prüft Meldepflichten parallel. Es klassifiziert den Fall als Incident, Near Miss, Finding, Fehlalarm oder Stop.

Bei einem Hochrisiko-System entscheidet die Triage ausdrücklich zwischen dem Art.-79-Risikopfad nach AI DEP-04 und dem schwerwiegenden Vorfall nach AI DEP-09. Sie prüft Provider, Importeur,

Distributor und zuständige Marktüberwachungsbehörde als Adressaten und dokumentiert bei nicht erreichbarem Provider den gesetzlichen Ersatzpfad.

Ergebnis, Evidence und Handoff. Der AI Incident Triage Record verweist auf Incident Ticket, Zeitstempel, Meldeentscheid, Forensikpaket und Lessons Learned. Der Handoff führt zu den Forensik-Anforderungen der AI Security Baseline, den Incident Safeguards des AI Control Standard und zur Revalidierung.

Bei einer reinen Deployerrolle führt der Workflow die Meldekette nach Art. 26 aus. Bei bestätigter Providerrolle aktiviert er zusätzlich Post-Market Monitoring, die gesetzliche Meldeuhr und den Serious-Incident-Prozess aus dem Provider Compliance Plan. Beide Pfade werden im Meldeentscheid getrennt dokumentiert.

Bei AI-bezogenen Cybersecurity- oder IKT-Vorfällen gilt zusätzlich der bestehende DORA-konforme Incident- und Meldeprozess des Instituts. Er klassifiziert den Vorfall und steuert eine erforderliche externe Meldung; Datenschutz- und AI-Act-Meldepflichten werden parallel auf derselben abgestimmten Fakten- und Evidence-Basis geprüft.

18. Reporting-Zulieferung

Teams liefern Reporting Inputs. Die Managementinterpretation erfolgt gemäss dem AI Governance Framework for Financial Institutions.

Input	Quelle
Portfolio Status	AI Register und Portfolio Review
Kontrollstatus	Applicability Statement und Safeguard Testing
Incident Status	Incident Workflow
Supplier Findings	Supplier Review
Technical Findings	Evidence aus der AI Security Baseline
Risk Acceptance	Risk Acceptance Record

19. Stilllegung und Exit

Die Stilllegung schliesst Nutzung, Betrieb, Daten, Supplier und Evidence kontrolliert ab.

Trigger, Owner und Input. Das Ende eines AI Use Cases, der Ersatz eines Systems, ein Supplier Exit, ein nicht mehr akzeptiertes Risiko oder ein regulatorischer Stop startet den Workflow. Der AI Owner führt ihn mit dem System Owner.

Ablauf und Entscheidung. Aktive Freigaben, Datenbestände, Modelle, Prompts, Logs, Embeddings, Verträge und offene Findings werden erfasst. Nutzung und Zugriffe werden beendet, technische Löschung und Supplier Exit abgeschlossen sowie die Evidence archiviert. Die Entscheidung bestätigt die Stilllegung oder weist Restaufgaben aus.

Ergebnis, Evidence und Handoff. Der Stilllegungs-Record verweist auf Lösch- und Archivierungsnachweis, Zugriffsentzug und Supplier-Exit-Nachweis. Der Handoff führt zur Prüfung, zum Supplier Management und zu den Stilllegungsanforderungen der AI Security Baseline.

20. Evidence und Registerpflege

Evidence bleiben in ihrem fachlich führenden System und werden über eindeutige Referenzen mit dem AI Register verbunden. Dadurch können operative Teams und prüfende Funktionen eine Entscheidung nachvollziehen, ohne dieselben Daten mehrfach zu pflegen.

Register	Operative Pflege
AI Register	interne System- und Use-Case-ID, Zweck, Rechtseinheit, Operatorrollen, Einsatzländer, Profilklasse oder X, Owner, Status, Freigaben, AI-Act-Einstufung, Provider-Aktivierung, FRIA-/DSFA-, Art.-50-, Art.-86- und Registrierungstrigger, Registerreferenzen, Incidents und Revalidierung
AI Act Requirements and Applicability Register	atomare Pflicht, Artikel/Anhang, Rolle, Trigger, Fälligkeit, Owner, Control, Workflow, Evidence, Status, Quellen- und Reviewstand; konkretes Applicability Record je Rechtseinheit, Land, System und Version
AI Use Case Register	fachliche Nutzung und Nutzergruppe
Model Inventory	bankfachlich oder aufsichtlich relevante Modellreferenz, Validierung, Performance, Drift und Stilllegung
Data Catalogue	Datenquelle, Data Owner und Klassifikation
Supplier Register	Anbieter, Vertrag, DORA-Bezug und Exit
Configuration Management Database (CMDB)	technische Plattform, Schnittstellen und Betriebsverantwortung
DORA-Informationsregister	vertragliche Informations- und Kommunikationstechnologie-Service-Vereinbarung (ICT-Service-Vereinbarung), Rechtseinheit, Providerkette und Unterstützung kritischer oder wichtiger Funktionen
EU AI Database	externe gesetzliche Registrierung; Provider-URL, Registrierungs-ID, Status, Datum und Evidence werden im AI Register referenziert

Der AI Register Record enthält zusätzlich, soweit anwendbar, System-, Modell- und Versionsbezeichnung, Art.-5-Prüfung, Annex-I-Relevanz, Annex-III-Nummer, Begründung einer Art.-6-Abs.-3-Ausnahme, Art.-50-Trigger, technische Dokumentation, Betriebsanleitung, Konformitätserklärung, Zertifikat, Logging-Verantwortung, Aufbewahrungsregel, wesentliche Änderungen sowie Aussetzungs-, Rückruf-, Lösch- und Stilllegungsnachweise. Die Evidence bleibt im fachlich führenden System; das AI Register führt eindeutige Referenzen.

21. Formulare, Checklisten und Vorlagen

Templates setzen die Workflows in wiederverwendbare Arbeitsmittel um. Jedes Template führt zu einer Entscheidung, ordnet einen Owner zu, verweist auf Evidence und bestimmt den Handoff.

Template	Zugehöriger Workflow
AI Idea Note	Orientierung
Portfolio Steering Note	Portfolio-Steuerung
AI Intake Record	Intake
AI Register Record	Intake und Registerpflege
Scope and Role Assessment	Vorprüfung

Template	Zugehöriger Workflow
Risk Profile Record	Klassifikation
Annex III Decision Tree und Article 6(3) Reasoning Sheet	AI-Act-Applicability und Hochrisikoklassifikation
Requirements and Applicability Record	AI-Act-Anwendbarkeit und Provider-Aktivierungsentscheid
Provider Activation Record	AI-Act-Anwendbarkeit und Provider-Aktivierungsentscheid
Provider Compliance Plan	bestätigte Providerrolle
Specialist Handoff Closure	atypische Rolle oder formelles Real-World Testing
Approved FRIA Record	Grundrechte-Folgenabschätzung
High-Risk Deployer Operation Record	Betrieb als Hochrisiko-Deployer
Transparency Decision and Evidence Record	Transparenz nach Art. 50
Explanation Response Record	Erläuterungsanfragen nach Art. 86
Registration Decision Record	EU Database Registration Assessment
EU Database Registration Evidence	gesetzlich erforderliche EU-Datenbankregistrierung
Betriebsfreigabe-Record	Betriebsfreigabe
Nutzungsfreigabe-Record	Nutzungsfreigabe
Supplier Assessment	Beschaffung und Supplier Review
Revalidierungs-Record	Revalidierung
AI Incident Triage Record	Incident Workflow
Stilllegungs-Record	Stilllegung und Exit

22. Glossar

Die folgenden Kernbegriffe gelten in diesem Handbook eindeutig:

Begriff	Bedeutung
Trigger	dokumentierter Anlass, der einen Workflow startet
AI	Artificial Intelligence; in der Dokumentfamilie einheitlich verwendete Bezeichnung für künstliche Intelligenz.
Owner	Rolle, die den Workflow führt und sein Ergebnis verantwortet
Ergebnis	dokumentierter Abschluss eines Workflows
Evidence	auffindbarer Nachweis, der Entscheidung und Ausführung belegt
Handoff	dokumentierte Übergabe von Ergebnis und Verantwortung an den nächsten Workflow oder die nächste Rolle
Applicability Statement	Festlegung, welche Safeguards für einen AI Use Case gelten
Provider-Aktivierungsentscheid	Release-blockierender Entscheid über eine eigene Providerrolle und den erforderlichen Provider Compliance Plan; englische Record-Referenz: Provider Activation.
Requirements and Applicability Record	Fallbezogener Nachweis für Rechtseinheit, Land, Systemversion, Rolle, Risikoklasse, Trigger und anwendbare Pflichten.

Begriff	Bedeutung
Betriebsfreigabe	Freigabe des technischen Betriebs unter definierten Bedingungen
Nutzungsfreigabe	Freigabe eines konkreten AI Use Cases für Zweck, Daten und Nutzergruppe
Risk Acceptance	befristete, begründete und genehmigte Annahme eines Restrisikos durch die zuständige Entscheidungsrolle; mit Owner und Review-Datum dokumentiert
Revalidierung	erneute Bewertung nach einem relevanten Trigger oder einer wesentlichen Änderung
Stilllegung	kontrollierter Abschluss von Nutzung und Betrieb einschliesslich Daten, Zugriffe, Supplier und Evidence
Digital.gov Plain Language	Offene Methode der U.S. General Services Administration für verständliche Prozessinformation und chronologische Leserführung.
4T2 Professional Prose	4T2 Schreibmethode für klare fachliche Erklärungen zwischen operativen Schritten.
CISA Playbook Pattern	Offenes Muster der U.S. Cybersecurity and Infrastructure Security Agency für Rollen, Trigger, koordinierte Aktionen, Eskalationen und Records.
FRIA	Fundamental Rights Impact Assessment; Grundrechte-Folgenabschätzung nach Art. 27 AI Act bei bestätigtem Trigger.
DSFA	Datenschutz-Folgenabschätzung nach Art. 35 DSGVO bei voraussichtlich hohem Datenschutzrisiko.
DORA	Digital Operational Resilience Act; europäischer Rechtsrahmen für digitale operationale Resilienz im Finanzsektor.
GPAI	General-Purpose AI; vielseitig einsetzbares AI-Modell mit möglichen Downstream-Risiken.
SaaS	Software as a Service; extern betriebene Softwareleistung.
AVV	Auftragsverarbeitungsvertrag für die Verarbeitung personenbezogener Daten im Auftrag.
ICT	Information and Communication Technology; Informations- und Kommunikationstechnologie im DORA-Kontext.
CMDB	Configuration Management Database; Betriebsinventar für technische Konfigurationselemente und Beziehungen.
CISO	Chief Information Security Officer; Führungsrolle für Informationssicherheit und zugehörige Sicherheitsrisiken.

Weitere Governance-Begriffe sind im AI Governance Framework for Financial Institutions definiert. Der AI Control Standard definiert Safeguards und Prüfkonzepte; die AI Security Baseline führt die technischen Begriffe.

23. Quellen

Primärquellen, validiert am 12. Juli 2026:

- Digital.gov Plain Language Guide Series: https://digital.gov/guides/plain-language
- CISA Federal Government Cybersecurity Incident and Vulnerability Response Playbooks: https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

- Regulation (EU) 2024/1689 (AI Act), especially Articles 4-6, 25-27, 49, 50 and 71 as well as Annex VIII: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
- Council of the EU, final adoption of the Digital Omnibus on AI on 29 June 2026; publication, entry into force and workflow-effective dates remain under regulatory watch: https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/
- Regulation (EU) 2022/2554 (DORA), especially Articles 17-23 and 28-30, and Commission Implementing Regulation (EU) 2024/2956: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
- Regulation (EU) 2016/679 (GDPR), especially Articles 22, 28, 32 and 35: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
- BaFin MaRisk, Circular 06/2024 (BA), only where bank-specific governance, model-risk, interne Kontrollsysteme (IKS) oder Auslagerungstrigger betreffen: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2024/rs_06_2024_MaRisk_BA.html

Die Workflows operationalisieren das Entscheidungsmodell und routen Fachentscheide. Sie nehmen das rechtliche Ergebnis einer DSFA-, FRIA-, DORA- oder MaRisk-Prüfung nicht vorweg.

24. Haftungs- und Anwendungshinweis

Dieses Handbook wurde mit fachlicher Sorgfalt und gegen den angegebenen Rechtsstand erstellt. Eine Gewähr für Vollständigkeit, Fehlerfreiheit oder dauerhafte Aktualität wird nicht übernommen. Es ist weder Rechtsberatung noch regulatorische Freigabe, Zertifizierung oder Konformitätsbescheinigung.

Die Workflows müssen an Zuständigkeiten, Meldewege und Systeme des jeweiligen Instituts angepasst werden. Ihre Wirksamkeit entsteht erst durch genehmigte Records, tatsächliche Evidence und geprüfte Handoffs. Die Verantwortung bleibt beim anwendenden Institut.

Copyright und offene Lizenz

Transparenz zur Erstellung

Martin Bischoff erstellte dieses Dokument mit generativer AI-Unterstützung für Formulierung, Redaktion, grafische Gestaltung sowie die strukturierte Vollständigkeits- und Konsistenzprüfung. Auswahl, Bewertung und Freigabe erfolgten durch ihn. Dies ersetzt keine unabhängige Rechts-, Wirksamkeits- oder Konformitätsprüfung.