AI Glossary for regulated organisations

372 public entries • updated 10.11.2026

allclouds.pl | Definitions, regulations and related concepts

A-BCP-01

AI Service Continuity & DR Plan

CDF artefact (phases F1.5/F6) of the CBC mechanism - the business continuity plan for the AI system required by Article 21(2)(c) of NIS2/uKSC. Feeds the AIMS Evidence Package and the uKSC evidence package (artefacts K4/K8). Introduced in CDF 1.5.0.

CDF methodology

See also: AIMS Evidence Package, NIS2/uKSC, AIMS

Online entry

A-F2-16

Service Fallback Specification

CDF artefact (phases F2 and F4) of control PAG-2 - a specification of the alternative route for contacting a member of staff in processes where AI interacts with citizens. Covers a hand-over-to-human function, a channel independent of the AI system and a route for lodging objections. Maintained as a section of the SA-XAI Documentation. Introduced in 1.6.0.

CDF methodology

See also: SA-XAI, PAG-2

Online entry

A-GOV-01

AI Justification Card

CDF artefact (phase F0) of control PAG-1 - a documented answer to the four Stage 0 questions of the MC Guide to AI, together with a GO / NO-GO / REDESIGN decision and approval by the Business Owner. Enters the Evidence Book as evidence of due diligence in the choice of technology. Introduced in 1.6.0.

CDF methodology

See also: Evidence Book, PAG-1

Online entry

A-GOV-02

Institutional AI Use Policy

CDF artefact (phase F2) of control PAG-3 - rules for the use of AI tools by staff, a catalogue of prohibited data (personal data and identifiers, special categories of data, classified information, internal official documents not intended for publication), the approval procedure for new tools, and information obligations. Introduced in 1.6.0.

CDF methodology

See also: PAG-3

Online entry

A-GOV-03

Approved AI Tools Register

CDF artefact (phases F2 and F6) of control PAG-3 - a list of AI tools approved for official use, with the basis for approval, the scope of permitted data, information on whether data are used to train models for the benefit of other customers, the business owner and the review date. Introduced in 1.6.0.

CDF methodology

See also: PAG-3

Online entry

A-HDP-01

Health Data Protection & EHDS Assessment

CDF artefact (phase F1.5) of the HDC mechanism (control HDC-1) - an assessment of health data protection and of compliance with the EHDS and Article 9 GDPR. Required for deployments with the HEALTH tag active. Introduced in CDF 1.5.0.

CDF methodology

See also: HEALTH (ACE tag), HDC-1, EHDS (Reg. 2025/327), RODO

Online entry

A-MDR-01

Medical Device AI Conformity Dossier

CDF artefact (phase F1.5) of the HDC mechanism (control HDC-2) - a conformity dossier for an AI medical device (MDR 2017/745 / IVDR 2017/746), generated where the AI system qualifies as medical device software. Introduced in CDF 1.5.0.

CDF methodology

See also: HDC-2, IVDR (Reg. 2017/746)

Online entry

A-MON-01

Post-Deployment Monitoring Checklist

CDF artefact generated in F5 and maintained in F6, based on the NIST AI 800-4 taxonomy (CAISI, March 2026). Defines 6 NIST-aligned monitoring categories: (1) Functionality - whether the system operates as intended, (2) Operational - whether the infrastructure sustains a consistent level of service, (3) Human Factors - the quality of human-AI interaction (per NIST: user intent and perception, dark patterns, feedback loops; in CDF additionally automation bias, skill degradation and overtrust), (4) Security - protection against attacks (OWASP ASI, prompt injection), (5) Compliance - regulatory compliance (AI Act, NIS2, DORA), (6) Large-Scale Impacts - positive societal and environmental effects. Required for LOA ≥ L2. For each category it specifies metrics, measurement frequency, escalation thresholds and the owner. Introduced in CDF 1.5.0.

CDF methodology

See also: NIST AI 800-4, AI Act, OWASP, DORA, NIST

Online entry

A-PLD-01

Product Liability Evidence Dossier

CDF artefact (phases F1.5/F2/F6) of the LER mechanism - an evidence readiness dossier containing a map of roles (manufacturer / importer / distributor / substantial modifier), a register of substantial modifications (LER-2), an index of evidence subject to disclosure (Article 9 of the PLD 2024/2853) with a trade secret protection clause, and documentation of the adequacy of product safety (Article 7(2)(f)). Feeds the Evidence Book (EB-4). Introduced in CDF 1.5.0.

CDF methodology

See also: Evidence Book, LER-2

Online entry

A-SSI-01

AI Supervisory Authorities Map

Identification of the competent supervisory authority (the Commission, KNF, a sectoral regulator) for a given AI deployment in the territory of the Republic of Poland. Covers the mapping of Articles 5-47 of the Act on Artificial Intelligence Systems (supervisory authority and Chapter 2) onto the client's organisational structure, and the identification of information and registration obligations towards the competent authorities. Mandatory artefact of phase F0/F1 in the GOV.PL variant.

CDF methodology

Online entry

A-SSI-02

24h Incident Reporting Procedure (Artefact Catalogue) - serious incident reporting procedure

Workflow for reporting serious incidents to the Commission in accordance with Article 73 of the AI Act (15 days as a rule; 10 days in the event of a person's death; 2 days in the event of a widespread infringement or a critical infrastructure incident); separately covers an early warning within ≤ 24 h to the competent CSIRT where the event constitutes a NIS2/uKSC incident. The Act on Artificial Intelligence Systems does not establish a separate Polish 24h reporting channel; the “24h” designation in the catalogue name refers to the NIS2/uKSC regime and to the internal CDF standard (preparation of the notification to the Commission within ≤ 24 h). Defines qualification criteria, a notification template, internal and external escalation (the Commission, CSIRT GOV/MON/NASK) and a status register with a monitoring dashboard. Phases F3/F5, tag GEO:PL. Introduced in CDF 1.5.0.

CDF methodology

See also: NIS2/uKSC, AI Act, NASK

Online entry

A-SSI-03

Inspection Readiness Checklist

Checklist of the organisation's readiness for an inspection by the Commission (Chapter 3, Articles 48-57), with notice given 7 days before the inspection. Covers the completeness of technical documentation in Polish, access to documents, systems and cloud computing (Article 52), designation of a contact person, and the availability of system logs and the Agent Registry. Takes into account the immediate enforceability of decisions (Article 108). Phase F4.

CDF methodology

See also: Agent Registry

Online entry

A-SSI-04

Individual Opinion Template

Application to the Commission for an individual opinion on the application of the AI Act to a specific AI deployment (Articles 8-18). The fee of PLN 150 follows from Article 11; the time limit is 30 days, or 60 days in a particularly complex case (Article 12), and the absence of an opinion is deemed an opinion consistent with the applicant's position. The opinion is binding within the scope of the case (Article 13) and, once anonymised, is published in the BIP (Article 17). Phase F1/F6.

CDF methodology

See also: AI Act

Online entry

A-SSI-05

Inspection Handling Procedure

Full workflow for handling an inspection by the Commission (Articles 48-57): 7 days' notice → provision of documentation and infrastructure → inspection report → right to lodge objections → post-inspection recommendations → recommendation implementation plan → implementation report. Recommendations set, as a rule, time limits of no less than 30 days (Article 57); in the event of an immediate risk the Commission may order the cessation of use or the withdrawal of the system (Article 63) and give its decision immediate enforceability (Article 108). Phase F5.

CDF methodology

Online entry

A-SSI-06

Sandbox Application Template

Application for admission to the AI regulatory sandbox operated by the Commission (Chapter 7, Articles 91-103). Participation lasts 6-12 months and is awarded by way of a competition; it is free of charge for SMEs. The participant submits an annual report (Article 98) and, within 90 days of confirmation of participation, may apply for an individual opinion (Article 101). Phase F0/F2.

CDF methodology

Online entry

A-SSI-07

SSI Fines and Sanctions Matrix

Risk matrix of administrative fines and criminal sanctions under the Act on Artificial Intelligence Systems (Articles 104-114). The amounts of the fines follow from Article 99 of the AI Act, and their equivalent in Polish zloty is calculated at the NBP exchange rate of 28 January (Article 104(4)). Covers the 20-70% / 30-90% settlement (Articles 70 and 84), the 10-50% reduction (Article 107) and the penal provisions of Articles 112-113. Phase F1.

CDF methodology

See also: AI Act

Online entry

Acceptance

Acceptance

Formal confirmation by the Client that the deployment meets the criteria defined in the Acceptance Criteria Checklist (F0-AC-01). Acceptance takes place after Phase F5 (Scaling and Industrialisation), on the basis of verification of all acceptance criteria - both the 6 minimum criteria recommended by CDF (section G.9) and the Client's own criteria. The acceptance protocol constitutes the formal closure of the deployment phase and a condition for the transition to F6 (CogOps).

Deployment and governance

Online entry

Acceptance Criteria Checklist (F0-AC-01)

Acceptance Criteria Checklist

Phase F0 artefact defining the formal criteria that must be met for the Client to accept the outcome of the deployment. Contains the 6 minimum criteria recommended by CDF (section G.9 of the Evidence Book): the complete set of mandatory artefacts from the ACE profile, an AI Act Readiness Score at the target level (recommendation ≥ 90%), an approved ASIA Report and SoA, a completed Human Competence Gate, an agreed and signed Cognitive SLA together with a transition plan to F6 CogOps, as well as the Client's own criteria. Constitutes an annex to the deployment agreement. Identifier: F0-AC-01.

CDF methodology

See also: AIMS Evidence Package, Agent Coordination, Cognitive SLA, AIMS

Online entry

Accountability Matrix

Accountability Matrix per LOA

A table assigning accountability for the decisions of the AI system to specific organisational roles according to the agent's level of autonomy (LOA L0-L4). For L0-L1, full accountability lies with the operator / deployer; for L2, accountability is shared (deployer + provider); for L3-L4, accountability shifts to the organisation (the management board), with a mandatory audit and a full Evidence Book package. In decision-making processes of the GOV profile the maximum level is L2 (CV-12). See Annex B, Table 62 in the Methodology.

CDF methodology

Online entry

ACE (Adaptive Configuration Engine)

Adaptive Configuration Engine

A dynamic configuration mechanism built into CDF which activates the appropriate subset of phases, controls, artefacts and annexes on the basis of the organisation's profile and the selected compliance requirements. Operates in Self-Service mode (Configuration Questionnaire) or Guided mode (F0). Introduced in CDF 1.4.4; described in the section “Adaptive Configuration Engine (ACE)” of the Methodology.

CDF methodology

See also: Configuration Questionnaire

Online entry

ACE Configuration Profile

ACE Configuration Profile

The output document of ACE specifying the active tags, the selected reference profile, the active tiers of CDF mechanisms (Cognitive SLA, HCG, F6) and the Personalised Compliance Matrix. Generated in F0, versioned as ACE-[PROFILE]-v[N].[M].

CDF methodology

See also: Cognitive SLA

Online entry

ACE Profile Matrix

ACE Profile Matrix

Annex E-ACE: a matrix of 77 compliance requirements × 11 reference profiles, with a REQUIRED / RECOMMENDED / AVAILABLE assignment per requirement and profile.

CDF methodology

Online entry

ACE Profile Version Record

ACE Profile Version Record

A formal, immutable record of each version of the organisation's configuration profile. Contains the version, date, author, rationale for the change and the REDUCTION flag (in the case of a Scope Reduction). Schema: ACE-[PROFILE]-v[N].[M].

CDF methodology

See also: Scope Reduction, REDUCTION (flag)

Online entry

ACE Reconfiguration Log

ACE Reconfiguration Log

CDF artefact (F0-F6) documenting every change to the organisation's configuration profile: version before/after, date, rationale, author, REDUCTION flag.

CDF methodology

See also: REDUCTION (flag)

Online entry

Act on Artificial Intelligence Systems (SSI)

Act of 3 July 2026 on Artificial Intelligence Systems (Ustawa o systemach sztucznej inteligencji)

Journal of Laws (Dz. U.) 2026, item 1003 (published 27.07.2026). The national act ensuring the application of the AI Act: 127 articles in 10 chapters, amending 10 other acts. It regulates the organisation of market surveillance (the Commission for the Development and Security of Artificial Intelligence), individual opinions, inspections and proceedings, the settlement on extraordinary mitigation of sanctions, notified bodies, the regulatory sandbox, and administrative fines and penal provisions. Entry into force: 11.08.2026 (Article 125(4) - 28.07.2026); Articles 8-18 and Chapters 3-5, 8 and 9 - 28.10.2026 (Article 127). In CDF it is addressed by Annex H (SSI supplement), artefacts A-SSI-01 to A-SSI-07 and items SSI-1 to SSI-7 of Matrix E.1.

Regulations and standards

AI Act

See also: AI Act

Online entry

Where we cover this: Act on AI systems

Where we cover this: Knowledge hub

AGENT (ACE tag)

ACE configuration tag

ACE tag activated where the deployment involves AI agents (single or multi-agent). Enables the Agent Governance, agent identity, security and agent lifecycle sections.

CDF methodology

Online entry

Agent (AI)

Autonomous AI Agent

An AI program capable of independently taking decisions and performing actions in a digital or physical environment in order to accomplish a specific business or operational task.

AI fundamentals

Online entry

Agent Coordination

Agent Coordination

A metric measuring the effectiveness of cooperation between AI agents in a multi-agent environment. Defined as the percentage of multi-agent tasks completed without escalation to a human. CDF baseline target: ≥ 85%. The metric belongs to Cognitive SLA Tier 2 (6 metrics). Measured in Phase F4 (Cognitive Sprint) and monitored in Phase F6 (CogOps). See Table 14 in the Methodology.

CDF methodology

See also: Cognitive SLA Tier, Cognitive Sprint, Cognitive SLA, CogOps

Online entry

Agent Identity Schema

Agent Identity Schema (CDF, based on NIST NCCoE)

An identity schema for AI agents. A CDF construct of its own, developing the identification and authentication pillars of the NIST NCCoE concept paper “Accelerating the Adoption of Software and AI Agent Identity and Authorization” (5.02.2026). It is not a quotation from the NIST publication. Control T-011, phase F2, artefact A-F2-05 Agent Registry.

CDF methodology

See also: Agent Registry, NIST

Online entry

Agent Kill-Switch

Agent Emergency Shutdown Procedure

A mechanism for the immediate hardware- or software-based halting of a single agent or of an entire agent swarm, with cascading notification of dependent nodes and automatic switch-over to manual verification. A mandatory element of Agent Governance from Phase 2 onwards.

AI fundamentals

Online entry

Agent Lifecycle Management (ALM)

Agent Lifecycle Management

The six-stage agent management model in CDF: Design → Build → Test → Deploy → Monitor → Optimize/Retire. Also comprises the Agent Retirement Protocol, which ensures the safe retirement of an agent, a check of dependencies and the transfer of operational and business knowledge. Carried out in Phase 6 of CDF. See also ALM (Agent Lifecycle Management).

CDF methodology

See also: ALM (Agent Lifecycle Management), Agent Retirement Protocol

Online entry

Agent Readiness Audit

AI Agent Readiness Audit

An assessment of the organisation's maturity for the deployment of autonomous AI agents, covering data, processes, competences, governance, psychological readiness and the ability to supervise agents safely in the working environment. Carried out in Phase 0 of CDF.

CDF methodology

Online entry

Agent Registry

AI Agent Register

A central register of all agents in the system, mandatory from Phase 2 onwards, recording their role, permissions, level of autonomy, owner, dependencies, token budgets, the Delegated By field, Kill-Switch Authority and audit history. The foundation of the Agent Governance Model and of the auditability of the multi-agent system.

CDF methodology

Online entry

Agent Retirement Protocol

Agent Retirement Protocol

A formal Phase 6 procedure of CDF defining the safe withdrawal of an AI agent from operation. Comprises: (1) archiving of the agent's memory and decision history, (2) revocation of permissions in the Agent Registry, (3) a dependency check - whether other agents or processes rely on the agent being retired, (4) transfer of operational knowledge to a successor or to a human team, (5) verification that there are no active MCP subscribers, (6) a final report setting out the reasons and an impact analysis.

CDF methodology

See also: Agent Registry

Online entry

Agent Threat Model

Agent Threat Model

A personalised model of agentic threats based on CoSAI, OWASP ASI and CSA ATF. Filtered through the ACE profile. See Annex B.

CDF methodology

See also: OWASP

Online entry

Agentic loop

A way of working in which an AI agent chooses its next actions based on the task and the information available: it plans, retrieves knowledge, calls tools and checks the result until the task is done. The opposite of a flow of predefined steps (DAG). In regulated environments a human approves the agent's plan before it runs, and the run history records every step

AI fundamentals

AI Act · ISO/IEC 42001

See also: Agent (AI), Multi-agent, HITL, Agent Registry

Online entry

Where we cover this: SAIE Pantera

Agentic RAG

agentic search with follow-up queries

A search mode in which an AI agent judges whether the material it has gathered is enough to answer. When something is missing, it writes follow-up queries and searches the documents again in another round, then merges fragments from all rounds and removes duplicates. Diagnostics show every round, query and source, so the answer can be checked

AI fundamentals

AI Act · ISO/IEC 42001

See also: RAG, Agent (AI), Multi-agent, LLM

Online entry

Where we cover this: SAIE Pantera

AI

Artificial Intelligence

Artificial intelligence - computer systems capable of performing tasks that require human intelligence, such as reasoning, learning, classification, content generation, decision-making or contextual analysis.

AI fundamentals

AI Act

See also: AI Act

Online entry

AI Act

EU AI Act (Reg. 2024/1689)

Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence, as amended by Regulation (EU) 2026/1744 (Digital Omnibus on AI). It classifies systems by level of risk and imposes obligations on providers and deployers, including obligations concerning risk management, logging, transparency, human oversight and technical documentation. Phased application: prohibited practices and AI literacy from 02.02.2025; GPAI models, governance and penalties from 02.08.2025; transparency obligations (Article 50) from 02.08.2026; the new prohibitions under Article 5 after a transitional period ending 02.12.2026; stand-alone high-risk systems under Annex III from 02.12.2027; systems embedded in products under Annex I from 02.08.2028.

Regulations and standards

Reg. 2026/1744

See also: Digital Omnibus (EU)

Online entry

Where we cover this: Act on AI systems

Where we cover this: AI use policy - template

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment

AI Act Readiness Score (ARS)

AI Act Readiness Score

A quantitative indicator (0-100%) of the organisation's readiness for compliance with the EU AI Act. Formula: ARS = Σ (weight × score) across 5 dimensions: Risk Classification, Technical Documentation, Human Oversight, Transparency, FRIA Readiness. Decision thresholds: ≥90% - full compliance, 70-89% - conditional compliance, <70% - deployment blocked. Generated in F0 and updated in F1.5. Formalised in CDF 1.4.4 (Z-003).

CDF methodology

See also: AI Act, FRIA

Online entry

AI Champion

AI Leader / AI Ambassador

An internal employee of the organisation trained as an expert in and advocate of AI deployments. Assists teams in the practical use of AI tools and acts as a bridge between the business, users and the transformation team.

Deployment and governance

Online entry

AI Champions Program

AI Leaders Programme

A programme for building internal leaders of AI transformation within the organisation, carried out in Phase 3 of CDF. Its aim is to create local ambassadors of change capable of supporting AI adoption, escalating problems and promoting sound practices in the use of cognitive systems.

Deployment and governance

Online entry

AI Concerns Feedback Channel

AI Concerns Reporting Channel

A formal mechanism enabling employees, end users, partners and third parties affected by the operation of an AI system to raise concerns, complaints and requests relating to decisions taken by AI systems. Required by ISO/IEC 42001 Annex A - A.3.3 (AI concerns reporting channel), with protection of reporting persons in accordance with Directive (EU) 2019/1937; supports the requirements of Article 14 of the AI Act (human oversight and the ability to intervene). In CDF it is implemented in Phase F6 (CogOps) through artefact A-F6-07 AI Concerns Channel Register (also designated F6-AFC-01 in the F6 section of the Methodology). Distinct from the citizen's objection route under control PAG-2.

Deployment and governance

AI Act · ISO/IEC 42001

See also: ISO/IEC 42001, AI Act

Online entry

AI Fatigue Index

AI Fatigue Index

An indicator introduced in Phase 5 which systematically measures the level of organisational fatigue resulting from the pace of AI deployments, change overload, an excess of initiatives or declining user engagement. Serves to prevent deployment stagnation and to pace the scale of transformation appropriately.

Deployment and governance

Online entry

AI gateway

brama AI

An intermediary layer between people and applications on one side and AI models on the other. All requests pass through a single point where the organisation enforces its rules: it masks sensitive data, blocks attacks, selects the model, keeps to cost limits and records who used what

Sovereignty and architecture

See also: Request routing, Jailbreak, Prompt Injection, Pseudonymisation, WORM log

Online entry

AI literacy (Art. 4 AI Act)

AI literacy

Skills, knowledge and understanding that allow AI systems to be used in an informed way, with awareness of their opportunities and limitations and of the risks they pose (Art. 3(56) AI Act). Article 4 of the AI Act, as amended by Regulation (EU) 2026/1744, requires providers and deployers to take measures to support a sufficient level of AI literacy among their staff, taking into account their knowledge, experience and the context of their work. The provision does not prescribe the form; in practice the measures are documented by the training programme, the list of participants and certificates

Regulations and standards

AI Act Art. 3(56), Art. 4 · Reg. 2026/1744

See also: AI Act, Digital Omnibus (EU)

Online entry

AI Medical Device (URPL)

Medical Device AI / URPL

A medical device whose safety component is an AI system or which is itself an AI system (MDR 2017/745, IVDR 2017/746). Subject to notification under Chapter III, Section 4 of the AI Act; the URPL cooperates with the notifying authority (Article 122 of the Act). Linked to the HDC mechanism and the HEALTH tag.

Regulations and standards

Act on AI Systems · MDR/IVDR

See also: IVDR (Reg. 2017/746)

Online entry

AI Model & Vendor Risk Assessment

AI Model & Vendor Risk Assessment

A comprehensive process for assessing the risk of AI models and their providers, carried out in Phase 1.5 of CDF before the target model is approved. Covers 6 criteria: (1) provider jurisdiction, (2) training data jurisdiction, (3) compliance disclosure, (4) vendor lock-in and migration (linked to VDP-1), (5) the provider's regulatory history, (6) continuity of access. Artefact A-F15-07 (Artefact Catalogue). The result is documented in Table 12 of the Methodology.

CDF methodology

Online entry

AI Readiness Scoring

AI Readiness Scoring

A key Phase 0 artefact quantifying the organisation's maturity for AI adoption across the dimensions of data, governance, competences and psychological readiness.

Deployment and governance

Online entry

AI Regulatory Sandbox

AI Regulatory Sandbox

A controlled environment for testing innovative AI systems under the supervision of the Commission (Chapter 7, Articles 91-103; the provisions apply from 11.08.2026). The sandbox is established by the Commission, which grants admission by way of a decision (Article 91(1)); the EU deadline for launching the national sandbox is 02.08.2027 (Article 57 of the AI Act as amended by Regulation (EU) 2026/1744). Participation lasts 6-12 months; selection takes place by competition, and participation by SMEs is free of charge. A participant submits an annual report (Article 98) and may, within 90 days of confirmation of participation, apply for an individual opinion (Article 101). The Act does not set a separate limit on the number of users.

Regulations and standards

AI Act

See also: AI Act

Online entry

Where we cover this: Act on AI systems

AI use policy

AI use policy

An organisation’s internal document setting out which AI tools may be used, which data must not be entered into them, who is responsible for the output and how AI-generated content is labelled. The basis for proving deployer obligations (AI Act Arts. 4 and 50) and a requirement of ISO/IEC 42001; also called AI usage rules

Deployment and governance

AI Act · ISO/IEC 42001 · Kodeks pracy

See also: Shadow AI, Deployer, AI Act, ISO/IEC 42001, A-GOV-02

Online entry

Where we cover this: AI use policy - template

Where we cover this: Shadow AI

Where we cover this: Act on AI systems - what you need to demonstrate

AI Vendor Diversification Strategy

AI Vendor Diversification Strategy

A strategy for minimising the risk of dependence on a single AI provider (VDP-1).

CDF methodology

Online entry

AIMS

AI Management System (ISO/IEC 42001)

The artificial intelligence management system defined in the ISO/IEC 42001:2023 standard. In CDF it constitutes one of the key points of reference for AI governance, alongside the EU AI Act and NIS2/uKSC. The CDF Methodology is designed to support organisations in building an AIMS and preparing for certification.

Regulations and standards

ISO/IEC 42001

See also: ISO/IEC 42001

Online entry

AIMS Evidence Package

AIMS Evidence Package

A body of evidence of compliance with ISO/IEC 42001:2023 generated and maintained within CDF (artefact A-F15-03). Comprises: the AI Policy, the AI Risk Register, the Statement of Applicability (SoA), the AI management plan, the management review report, internal audit records, the AI incident log and evidence of competence. Created in F1.5 (baseline), enriched in F2-F4, reviewed in F5 and F6 (quarterly). The lifecycle of the individual artefacts in the package is defined in Table 9 of the Methodology.

CDF methodology

See also: Compliance Readiness Report, Agent Registry, ASIA

Online entry

AIMS Lifecycle

AIMS Artefact Lifecycle

A table defining the lifecycle of the 12 key artefacts of the AIMS Evidence Package across CDF phases F0-F6: the moment of creation (Created), update (Updated), review (Reviewed) and the owner (Owner). Source: the Methodology, AIMS Evidence Package section. Introduced in v1.4.4.

CDF methodology

See also: AIMS Evidence Package, AIMS

Online entry

AIP

Agent Interaction Protocols

A set of protocols governing cooperation between AI agents in CDF. Comprises three patterns: Hierarchical (Supervisor-Worker, the default and safest pattern for critical processes, L0-L1), Collaborative (shared workspace, permitted exclusively for auxiliary processes, L1-L2) and Pipeline (sequential hand-over of results, deterministic and linear processes). Every machine-to-machine interaction is logged in the Immutable Audit Trail with a timestamp, initiator, token cost and outcome. See Annex B.

CDF methodology

See also: Immutable Audit Trail

Online entry

Air-gap

Network Isolation

The physical disconnection of an IT system from external networks, including the internet. It is the highest level of security for sovereign AI systems and a typical requirement for defence, classified or particularly critical environments.

Sovereignty and architecture

Online entry

Where we cover this: Bielik and PLLuM

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment

Air-Gapped Defense

Isolated Defence Architecture

The highest level of target deployment pattern in CDF, assuming full physical isolation of the AI environment, no internet connections and no operational dependencies on external services. Used for defence, classified information and selected national critical infrastructure systems.

Sovereignty and architecture

Online entry

ALM (Agent Lifecycle Management)

Agent Lifecycle Management

Management of the full lifecycle of an AI agent: from registration in the Agent Registry (F2), through operational monitoring (F4-F6), to retirement (Agent Retirement Protocol). See Agent Lifecycle Management (ALM).

CDF methodology

See also: Agent Lifecycle Management (ALM), Agent Retirement Protocol, Agent Registry

Online entry

API

Application Programming Interface

Application programming interface - a set of rules and methods enabling communication between different systems or software components. In the CDF context it requires assessment in terms of supply chain dependencies and integration security.

AI fundamentals

Online entry

ARS (AI Act Readiness Score)

AI Act Readiness Score

An indicator of the organisation's readiness to meet the requirements of the EU AI Act. Scale 0-100%. CDF target: ≥ 90%. See AI Act Readiness Score (ARS). See Table 19 in the Methodology.

CDF methodology

See also: AI Act Readiness Score (ARS), AI Act

Online entry

ASIA

AI System Impact Assessment

An assessment of the impact of an AI system carried out before deployment, covering an analysis of risks to fundamental rights, safety, the environment and society. In CDF it is initiated in Phase F1.5 (for profiles with the REGULATED tag) or activated by the ACE profile (RECOMMENDED for the remaining profiles). Updated in subsequent phases (F2, F5, F6). Maps onto the obligations under Article 9 and Article 27 of the EU AI Act and onto the FRIA requirements. For CSE-GOV and CSE-COM deployments involving regulated data, the report includes an extended sovereignty module.

CDF methodology

See also: REGULATED (ACE tag), AI Act, FRIA

Online entry

ATF (Agentic Trust Framework)

Agentic Trust Framework (open specification by MassiveScale.AI, published on the CSA blog)

An agentic maturity framework published on 2.02.2026 on the Cloud Security Alliance blog as an open specification (Creative Commons licence, canonical version in the massivescale-ai GitHub repository); author: Josh Woodruff, MassiveScale.AI. It is a guest post, not a formal CSA research publication. 4 maturity levels: Level 1 (Intern - observation, every action approved), Level 2 (Junior - recommends and executes upon approval), Level 3 (Senior - acts independently with ex-post notification), Level 4 (Principal - full autonomy within the limits of its mandate). Mapping to CDF LOA: L0-L1 (Intern), L2 (Junior), L3 (Senior), L4 (Principal). See Table 61 (ATF ↔ LOA Cross-Reference) in Annex B of the Methodology.

CDF methodology

Online entry

Autonomous Swarm

Autonomous Agent Swarm

A network of many cooperating AI agents operating without constant human supervision within defined boundaries of autonomy. In CDF used exclusively for non-critical processes or operational back-office functions, with mandatory Token Budget Governance and an Agent Kill-Switch.

AI fundamentals

Online entry

Autonomy Scale (L0-L4)

Five-level scale of AI agent autonomy (L0-L4)

The standard CDF model defining the scope of an agent's decision-making authority: L0 Human-only (the agent only advises; the human takes all decisions and actions), L1 Human-in-the-loop (the agent executes; the human approves every action), L2 Human-on-the-loop (the agent executes; the human supervises and may interrupt), L3 Human-over-the-loop (the agent is autonomous within a defined framework), L4 Full autonomy (non-critical back-office processes only).

AI fundamentals

Online entry

Backup 3-2-1

3-2-1 Backup Strategy

A backup strategy based on maintaining at least 3 copies of the data, on 2 different media, of which 1 is stored off-site. In CDF applied in Phase 1.5 as an element of the NIS2/uKSC requirements.

Sovereignty and architecture

Online entry

Bielik

Bielik

A Polish open language model by the SpeakLeash Foundation, trained on the ACK Cyfronet AGH supercomputers. A family from 1.5 to 11 billion parameters under Apache 2.0 (free commercial use); smaller versions run on a laptop, 11B on a single 24 GB card. In SAIE it is available through PROXY:AI like any global model

AI fundamentals

See also: PLLuM, LLM, Quantisation, On-premises / On-prem, RAG

Online entry

Where we cover this: Bielik and PLLuM

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment

Bounded Autonomy

Bounded Agent Autonomy

A CDF design principle under which every AI agent operates within strictly defined boundaries of permissions, token budget and decision-making scope. Autonomy boundaries are assigned on the basis of the Autonomy Scale (L0-L4) and are subject to continuous monitoring under the Agent SLA.

AI fundamentals

Online entry

Business Continuity

Business Continuity

The organisation's ability to maintain key business functions during and after an incident or disruption. In CDF addressed by the CBC mechanism (Cognitive Business Continuity, controls CBC-1..3, artefact A-BCP-01) required by Article 21(2)(c) of NIS2/uKSC, and at the agent layer by the Agent Kill-Switch and the Vendor Disruption Protocol (Annex B).

Sovereignty and architecture

Online entry

C-Suite

Management Board / Top Management

A collective term for the top management of the organisation (CEO, CTO, CIO, CFO, CISO). In CDF it takes part in the Executive Alignment Workshop (Phase 0) and in the validation of the North Star (Phase 1).

Deployment and governance

Online entry

CapEx

Capital Expenditure

Capital expenditure on the purchase or construction of fixed assets, including AI infrastructure (servers, GPUs, cooling, cabling). In CDF taken into account in the 3-5 year TCO Model designed in Phase 1.

Deployment and governance

See also: OpEx

Online entry

CBC

Cognitive Business Continuity

A business continuity mechanism for the AI system introducing the continuity and disaster recovery regime required by Article 21(2)(c) of NIS2/uKSC: a continuity and DR plan (BCP/DRP), RTO/RPO per system, 3-2-1 backups, controlled degradation modes, fallback to a sovereign model. Distinct from CBP (the Cognitive Digital Twin). Comprises controls CBC-1, CBC-2 and CBC-3. Phases F1/F1.5/F6. Artefact: A-BCP-01. Introduced in CDF 1.5.0.

CDF methodology

Online entry

CBC-1

Continuity & DR Plan

CDF control of the CBC mechanism: a business continuity and recovery plan (BCP/DRP) for AI services - RTO/RPO per system, 3-2-1 backups, controlled degradation modes, fallback to a sovereign model (linked to VDP-2). Knowledge domains KD5/KD11. Phases F1/F1.5/F6. Introduced in CDF 1.5.0.

CDF methodology

Online entry

CBC-2

Crisis Management & Comms

CDF control of the CBC mechanism: crisis management and communication procedures, escalation, and linkage with incident handling (24h/72h under NIS2/uKSC). Knowledge domains KD5/KD2. Phases F1.5/F6. Introduced in CDF 1.5.0.

CDF methodology

See also: NIS2/uKSC

Online entry

CBC-3

Continuity Testing

CDF control of the CBC mechanism: periodic recovery tests and keeping the business continuity plan up to date. Knowledge domains KD5/KD12. Phase F6. Introduced in CDF 1.5.0.

CDF methodology

Online entry

CBP

Cognitive Digital Twin / Cognitive Worker Twin

A faithful cognitive model of an employee of the organisation, encompassing explicit knowledge, tacit knowledge, interpretations, decision preferences and behavioural patterns. Serves as a layer of cognitive continuity and as the completion of the AI deployment to its full potential. Element K12 of the CDF ontology.

AI fundamentals

Online entry

CBP Fidelity Test

CBP Fidelity Test

A cognitive fidelity test (artefact A-CBP-05, F5/F6) verifying the extent to which the CBP in production faithfully reproduces the employee's way of thinking, interpreting and taking decisions. Its result is the Cognitive Fidelity Score (CFS), which determines the CFL level. Performed in F5 and periodically in F6.

CDF methodology

Online entry

CBP Monitoring Dashboard

CBP Monitoring Dashboard

An F5/F6 dashboard visualising CBP metrics and Human Factors Monitoring indicators (frequency of overrides of AI decisions, output validation time, escalation-to-human rate). Based on the NIST AI 800-4 taxonomy. Referenced in the section “NIST AI 800-4 Architectural Principles” of the Methodology; it has no separate entry in the CDF Artefact Catalogue.

CDF methodology

See also: NIST AI 800-4, NIST

Online entry

CBP Readiness Assessment

CBP Readiness Assessment

An F1 artefact (A-CBP-01, SCALE tag) assessing how much of the organisation's knowledge is explicit and how much is tacit, and where the cognitive gaps lie; the starting point for the CBP Capture Strategy (F2).

CDF methodology

Online entry

CBP Sync Protocol

CBP Synchronisation Protocol

A mechanism for continuously updating the Cognitive Digital Twin from new employee data. An artefact of Phase F6 (Operate) ensuring that the CBP remains current as the employee's knowledge and behaviour evolve.

CDF methodology

Online entry

CDF

Cognitive Deployment Framework

A universal methodological framework by allclouds.pl, agnostic with respect to IT systems and infrastructure, for the deployment of Enterprise Cognitive Systems (ECS). In the Client Success edition it is adapted to the public and regulated sectors. It covers the full cycle from cognitive reconnaissance and compliance through to deployment, scaling, governance and continuous optimisation. Versioning follows the [N].[M].[P] format (section “CDF Methodology Versioning”).

Deployment and governance

Online entry

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment

CDF Academy

CDF Academy

The CDF training programme (Phase 3) delivering a 40-hour certified training course with a module on designing interactions that minimise operators' cognitive load. The foundation for building internal AI competences and the AI Champions programme.

CDF methodology

Online entry

CDF Artefact Catalogue

CDF Artefact Catalogue

The single source of the list of CDF artefacts (Table 6 of the Methodology), introduced in 1.6.0. It consolidates the lists previously scattered across the phase lists, ACE artefacts, CBP artefacts, the SSI artefact register and the descriptions of the domain mechanisms. 94 items, each assigned a phase, activation tag, owner from the RACI matrix, carrier type and version of introduction. The number of artefacts active for a deployment follows from the ACE profile, not from the number of catalogue items.

CDF methodology

See also: RACI

Online entry

CDF Control Catalogue

CDF Control Catalogue

The single source of the list of CDF controls (Table 5 of the Methodology), introduced in 1.6.0. 34 controls in eight families: T (methodological controls), MCP (security of the agent tooling layer), VDP (vendor continuity), SAG (agent security), LER (evidence readiness), CBC (business continuity), HDC (health sector), PAG (public administration). Each control is assigned a knowledge domain, phases, an activation tag, a type and a related artefact.

CDF methodology

Online entry

CDF North Star

CDF North Star Document

A Phase 1 artefact bringing together the strategic objectives, KPIs and milestones of the AI programme.

CDF methodology

Online entry

CDF Platform

CDF Platform

A web application supporting the deployment of the CDF Methodology. It implements ACE (Adaptive Configuration Engine) as an interactive profile configurator and displays tags, the compliance matrix and artefacts. ACE is a logical module described in the section “Adaptive Configuration Engine (ACE)” of the Methodology; the CDF Platform is its technological implementation and the third element of the release triad.

Deployment and governance

Online entry

CDF Release Triad

CDF Release Triad

Three synchronised artefacts published in every CDF release: (1) the Methodology DOCX (PL), (2) the Glossary DOCX, (3) the web application. All three are continuously improved and must be consistent in every release. Source: the CDF release process. Introduced in v1.4.4.

CDF methodology

Online entry

CDF Risk Engine

Risk Management Engine

A technological solution deployed as the security foundation of the system, implementing continuous risk management procedures consistent with ISO/IEC 23894 and AI governance requirements.

CDF methodology

See also: ISO/IEC 23894

Online entry

CDF Scales and Taxonomies

CDF Scales and Taxonomies

Definitional block introduced in 1.6.0, the single source of the levels of the CDF scales: LOA (L0-L4), CFL (CFL-1 to CFL-5), ACE guardrails (BLOCKING, AUTO-CORRECT, ADVISORY), Cognitive SLA tiers, HCG tiers, F6 CogOps tiers, the cognitive degradation scale, Cognitive SLA escalation, AI sovereignty levels (Level 1-3) and compute sovereignty levels (S1-S4). The remaining sections of the Methodology refer to the level and do not repeat the definitions or the number of elements.

CDF methodology

See also: Cognitive SLA, CogOps

Online entry

CDF Source Taxonomy

CDF Source Taxonomy - classes W, M, N, D

Four-class classification of the sources of the CDF canon, introduced in 1.6.0. Class W: acts of generally applicable law, in force or within their transition period; mandatory requirements gated by phase, with the state of application shown in the Status column of Matrix E.1. Class M: documents of public authorities and regulators without binding force; enabled by default for the profiles covered, with any exclusion requiring justification in the Compliance Gap Analysis. Class N: technical norms and standards; a maturity framework with no presumption of conformity until cited in the Official Journal of the EU. Class D: research and empirical data; they feed the Evidence Book and calibrate the default values of ACE profiles.

CDF methodology

See also: Compliance Gap Analysis, Evidence Book

Online entry

Center of Excellence

Centre of Excellence

An internal organisational unit responsible for standardisation, scaling and knowledge management in the field of AI. In CDF, an element of the Phase 5 organisational model (Scaling and Industrialisation).

Deployment and governance

Online entry

CETS 225 (Council of Europe AI Convention)

Council of Europe Framework Convention on AI (CETS 225)

The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. Opened for signature on 5 September 2024 in Vilnius. The basis for signature by the European Union was Council Decision (EU) 2024/2218 of 28.08.2024; the Union deposited its instrument of approval on 15 May 2026. As at 12 September 2026 the Convention had not entered into force, because the threshold under Article 30(3) (five consents to be bound, including three Council of Europe member States) had not been reached. The Union's deposit does not count towards the threshold of three States. The relationship with the AI Act is described in section E.6 of Annex E.

Regulations and standards

Online entry

CFL

Cognitive Fidelity Levels

A five-level CBP maturity scale, independent of the LOA scale. It measures the fidelity of cognitive representation: CFL-1 Declarative Profile, CFL-2 Observational Profile, CFL-3 Interpretive Profile (CFS ≥ 60%), CFL-4 Predictive Profile (CFS ≥ 80%), CFL-5 Autonomous Profile (CFS ≥ 90%).

CDF methodology

Online entry

CFS

Cognitive Fidelity Score

A measure of the quality of cognitive representation on a scale of 0-100%. It determines the degree to which the Cognitive Digital Twin (CBP) faithfully represents the employee's way of thinking, interpreting and making decisions. Thresholds: CFL-3 ≥ 60%, CFL-4 ≥ 80%, CFL-5 ≥ 90%.

CDF methodology

Online entry

Chain of Custody

Chain of Custody

The complete accountability path from input data to the output decision of an AI system, covering every stage of transformation, enrichment and use. In CDF it is implemented through: Immutable Audit Trail (F6), Data Provenance Tracking (K3), Agent Identity Schema and Cognitive Observability. It differs from data lineage in scope - it covers not only the origin of data but also human decisions (who approved, on what basis) and agent decisions (which agent, with what prompt, in what role).

Sovereignty and architecture

Online entry

Change Management

Change Management

The process of systematically managing the organisation's passage through transformation - from planning, communication and training to adoption monitoring and counteracting resistance. In CDF it is carried out in Phase 3 with the mandatory involvement of the organisation's leaders.

Deployment and governance

Online entry

Chatbot

text conversation program

A program that holds a text conversation in a chat window, on a website or in an app. Modern chatbots use large language models, so they write fluently and can pass for a human. The provider must design the chatbot so that users know they are talking to AI

AI fundamentals

AI Act (Art. 50(1))

See also: LLM, Voicebot, Agent (AI)

Online entry

Where we cover this: TURING:AI game

CLASSIFIED (ACE tag)

ACE tag for classified deployments

An ACE tag applied in profiles covering systems that process classified information. It activates requirements relating to security accreditation (e.g. ABW), physical separation of infrastructure, personnel criteria and compliance with the provisions on the protection of classified information. Applies to the DEFENSE and SOV (Sovereign) profiles at the highest level of restrictiveness.

CDF methodology

See also: DEFENSE (ACE tag)

Online entry

Cognitive Circuit Breaker

Cognitive Circuit Breaker

A mechanism that automatically cuts an agent off from external systems after 3 consecutive failed cognitive quality verification tests. It prevents the propagation of erroneous decisions and serves as a safeguard for multi-agent environments.

CDF methodology

Online entry

Cognitive Degradation Monitoring

Cognitive Degradation Monitoring

A three-level scale for monitoring the reasoning quality of AI agents: Normal (operating within the norm), Degraded (reduced quality - intervention required), Critical (critical deviation - remediation procedures). Implemented in Phase 2, it generates alerts and triggers remediation procedures, and the results are presented on the CogOps dashboard. Note: the scale describes the operational states of an agent and is independent of the metric measurement scale (Cognitive SLA Tiers).

CDF methodology

See also: Cognitive SLA, CogOps

Online entry

Cognitive Map

Cognitive Map

A Phase 0 artefact: a visualisation of the organisation's processes, data, competences and decision areas from the perspective of the potential for AI deployment.

AI fundamentals

Online entry

Cognitive Observability

Cognitive Observability

The ability to monitor and log in detail AI reasoning paths, agent actions, the dependencies between them and the use of knowledge sources - enabling the decision-making process to be reconstructed after the fact. In CDF it forms part of Phase 6 (CogOps) and supports compliance, audit, troubleshooting and the optimisation of AI decision quality.

AI fundamentals

Online entry

Cognitive Quality Reports

Cognitive Quality Reports

Monthly reports generated in Phase 4 and subsequent phases, presenting Cognitive SLA metric results, reasoning quality trends, cognitive incidents and optimisation recommendations.

CDF methodology

See also: Cognitive SLA

Online entry

Cognitive SLA

Cognitive Service Level Agreement

A multi-layered system of reasoning quality metrics for AI systems used in CDF, going beyond traditional IT indicators (uptime, latency). It measures readiness, consistency, hallucination level, knowledge freshness, the effectiveness of agent coordination and the ability to mitigate errors rapidly. Breach procedure: Yellow (24h) → Orange (72h) → Red (7 days or hallucinations >5% in a critical process → Kill-Switch).

AI fundamentals

Online entry

Cognitive SLA Tier

Cognitive SLA Tier

The three-tier division of the Cognitive SLA mechanism (the CDF Scales and Taxonomies block): Tier 1 (CORE - 4 baseline metrics: System Availability, Reasoning Accuracy Rate, Hallucination Rate, Mitigation Response Time), Tier 2 (AGENT + PRODUCTION - +2 coordination metrics: Agent Coordination, Confidence Calibration; 6 metrics in total), Tier 3 (SCALE or SOVEREIGN - +Knowledge Freshness Index; 7 metrics in total + CogOps dashboards). Each tier is fully operational at its own level; subsequent tiers add metrics rather than replacing the previous ones.

CDF methodology

See also: Knowledge Freshness Index, Mitigation Response Time, Reasoning Accuracy Rate, Confidence Calibration, System Availability

Online entry

Cognitive Sprint

Cognitive Sprint

An iterative deployment cycle in the CDF Methodology, analogous to an Agile Sprint but focused on the rapid and controlled delivery of AI value under conditions of compliance, auditability and reasoning quality measurement. Carried out in CDF Phase 4.

Deployment and governance

Online entry

CogOps

Cognitive Operations

The operational phase of maintaining AI systems, covering monitoring, model optimisation, compliance, retraining, and the management of drift, knowledge freshness and performance degradation. It is the equivalent of a mature operating model for cognitive systems. In CDF it is carried out in Phase 6.

AI fundamentals

Online entry

Commission for the Development and Security of Artificial Intelligence (KRiBSI)

Commission for the Development and Security of Artificial Intelligence (Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji, KRiBSI)

The Commission for the Development and Security of Artificial Intelligence, hereinafter the Commission, is the central AI market surveillance authority and the single point of contact (Article 5). It is composed of: the Chair, 2 Deputy Chairs and 4 members designated by UOKiK, KNF, KRRiT and UKE - 7 persons in total (Article 19). The Chair is appointed for a 5-year term by the Sejm with the consent of the Senate (Article 28). Legal basis: the Act on Artificial Intelligence Systems of 3 July 2026 (Journal of Laws (Dz. U.) 2026, item 1003), in force since 11.08.2026; the provisions on inspections, proceedings, settlements and fines, and on individual opinions - from 28.10.2026.

Regulations and standards

AI Act

See also: AI Act

Online entry

Where we cover this: Act on AI systems

Where we cover this: Knowledge hub

Commission Office (support of KRiBSI)

Support of the Commission for the Development and Security of Artificial Intelligence

The Act does not create a separate office or a state legal person: administrative and clerical support for the Commission and its Chairperson is provided by the office serving the minister competent for digitalisation (Article 43). The maximum limit of expenditure from the state budget (Article 126) is set for the years 2026-2035: 2026 = PLN 9.30 million; 2027 = PLN 23.74 million; 2028 = PLN 24.17 million; 2029 = PLN 24.89 million; 2030 = PLN 25.63 million; rising thereafter to PLN 29.68 million in 2035. Proceeds from administrative fines constitute revenue of the state budget (Article 106).

Regulations and standards

See also: Act on Artificial Intelligence Systems (SSI)

Online entry

Compliance Gap Analysis

Compliance Gap Analysis

A process carried out in Phase 0 that diagnoses the organisation's shortfalls against the requirements of the EU AI Act, ISO standards, sectoral regulations and the model contract of the Ministry of Digital Affairs. It forms the basis of the remediation plan and further architectural decisions.

CDF methodology

See also: AI Act

Online entry

Compliance Readiness Report

Compliance Readiness Report

A key F1.5 artefact documenting the organisation's state of regulatory readiness.

CDF methodology

Online entry

Compliance Timeline Tracker

Compliance Timeline Tracker

An interactive view of regulatory deadlines (EU AI Act, CRA, NIS2/uKSC, CEN/CENELEC) integrated with the CDF Platform. It enables compliance deadlines to be tracked and provides automatic notifications.

CDF methodology

See also: CDF Platform, NIS2/uKSC, AI Act

Online entry

Compliance-First

Regulatory Compliance as a Priority

An approach in which legal, regulatory and audit requirements are treated as a precondition of AI deployment rather than as a subsequent stage. In CDF, compliance is designed in from the outset and closed out before acceptance of the solution.

Deployment and governance

Online entry

Confidence Calibration

Confidence Calibration

A Cognitive SLA metric (Table 14 of the Methodology) measuring the correlation between the declared confidence of an AI response and its correctness. Target: r ≥ 0.85. A Tier 2 metric.

AI fundamentals

Online entry

Configuration Questionnaire

ACE Configuration Questionnaire

An interactive ACE questionnaire (Table 25 of the Methodology) used to establish the organisation's configuration profile in Self-Service mode. Part I: 7 questions on the purpose of the deployment, AI types, sector (with sub-question 3a on determinative processes for the public and defence sectors, from 1.6.0), type of data, scale, location and compliance requirements; Part I-A: cross-validation (CV-00..CV-12, MV-01..MV-07); Part II: compliance selection (REQUIRED / RECOMMENDED / AVAILABLE).

CDF methodology

Online entry

Conformity Assessment

Conformity Assessment of an AI System

The process of formally verifying whether a high-risk AI system meets the requirements of the EU AI Act before being placed on the market (Article 43). CDF carries it out in phases F1.5 (Compliance-First Delivery, self-assessment) and F5 (Compliance Audit Report) - item 10 of Matrix E.1. Systems under Annex III are subject to the internal conformity assessment procedure or to assessment by a notified body; the obligations of Chapter III, Sections 1-3 apply to them from 02.12.2027, and to systems under Annex I from 02.08.2028 (Regulation (EU) 2026/1744).

Regulations and standards

AI Act

See also: AI Act

Online entry

Context window

okno kontekstowe

The amount of text, counted in tokens, that a model sees at once: the prompt, the conversation history and attached documents. Whatever falls outside the window the model “forgets”. That is why long conversations and large documents are split into parts, and when working on an organisation’s documents the model receives only the fragments needed for the answer

AI fundamentals

See also: Token, LLM, RAG

Online entry

Coordination Effectiveness

Coordination Effectiveness

A metric of the Agent SLA layer (Table 56 of the Methodology, Annex A) measuring the quality of collaboration between agents in carrying out complex end-to-end tasks.

CDF methodology

Online entry

CORE (ACE tag)

ACE configuration tag

An ACE tag that is always active - the CDF core mandatory for every AI deployment regardless of the organisation's profile. It covers the fundamental phases, controls and artefacts.

CDF methodology

Online entry

Council attached to the Commission (SSI)

Council - Opinion-giving and Advisory Body of the Commission

An opinion-giving and advisory body operating alongside the Commission, referred to in the Act solely as the “Council”, comprising 9 to 15 members elected by the Commission for a 2-year term (Article 45). Candidates are nominated by, among others, the local government side of the Joint Commission of the Government and Local Government, the Commissioner for Human Rights (RPO), the Commissioner for Children's Rights (RPD), the Patients' Rights Ombudsman, the SME Ombudsman and the Chief Labour Inspector. The Council's opinions and positions are not binding on the Commission (Article 46). The Commission appoints and dismisses the Chair and the Deputy Chair of the Council (Article 47).

Regulations and standards

Online entry

CRA (Cyber Resilience Act)

Cyber Resilience Act - Regulation 2024/2847

Regulation (EU) 2024/2847 establishing mandatory cybersecurity requirements for products with digital elements. It covers: essential security requirements (Security by Design - Annex I), manufacturers' obligations (Article 13), reporting of actively exploited vulnerabilities and severe incidents within 24h/72h/14d (Article 14), SBOM (Software Bill of Materials), the classification of important and critical products (Articles 7-8, Annexes III-IV), and CE marking. Vulnerability reporting from 11.09.2026, full compliance from 11.12.2027. Fines: up to EUR 15 million or 2.5% of turnover. In CDF it is mapped in section D.2b and Matrix E.1.

Regulations and standards

See also: Vulnerability Disclosure, SBOM (Software Bill of Materials)

Online entry

Critical ICT Provider

Critical ICT Services Provider

An external ICT services provider designated jointly by the European Supervisory Authorities (EBA, ESMA, EIOPA) as critical for the financial sector (DORA, Articles 31-44). It is subject to direct oversight by the lead overseer and to resilience testing requirements. In CDF it is mapped to F1.5 and F6 - Critical Provider Oversight.

Regulations and standards

DORA

See also: DORA

Online entry

CRM

Customer Relationship Management

A system for managing customer relationships, for example Salesforce or Microsoft Dynamics. In CDF it appears as one of the typical integration systems in Phase 1.

Deployment and governance

Online entry

Cross-Validation Guardrail

ACE Cross-Validation Rule

An automatic rule checking the consistency of the ACE configuration (Table 26 of the Methodology). In 1.6.0, 13 rules CV-00 to CV-12 apply in a layered arrangement: Layer 0 - BLOCKING (CV-00: an attempt to disable REGULATED with FINANCE/GOV; CV-12: LOA > L2 in a GOV adjudicative process); Layer 1 - AUTO-CORRECT (CV-01 FINANCE→REGULATED, CV-02 GOV→REGULATED, CV-03 SOVEREIGN→REGULATED+GOV+CLASSIFIED, CV-04 multi-agent→AGENT, CV-10 HEALTH→REGULATED); Layer 1b - ADVISORY (CV-05 HCG-Full with REGULATED, CV-06 Tier 3 with SCALE/SOVEREIGN, CV-07 F6-Lite with PRODUCTION, CV-08 F6-Full with DEFENSE, CV-09 PLD exposure with fine-tuning, CV-11 special-category data with HEALTH); Layer 2 - substantive warnings MV-01 to MV-07 (ACE Consistency Rules, Table 27). Rule types are defined in the CDF Scales and Taxonomies block.

CDF methodology

See also: REGULATED (ACE tag), HCG-Full, FINANCE (ACE tag), SCALE (ACE tag)

Online entry

CV-12

Cross-Validation Rule 12 - LOA restriction in adjudicative processes

An ACE cross-validation rule of the BLOCKING type, introduced in 1.6.0. Declaring an adjudicative process in sub-question 3a of the Configuration Questionnaire together with the GOV tag blocks the assignment of an autonomy level above L2. From this release, validation Layer 0 comprises two rules: CV-00 and CV-12.

CDF methodology

See also: Cross-Validation Guardrail

Online entry

Cybersecurity Strategy of the Republic of Poland 2025-2029

National cybersecurity strategy

Strategic document adopted by the Council of Ministers on 10 March 2026, setting out 6 specific objectives strengthening the National Cybersecurity System. In section D.2a, CDF maps the Strategy's 7 initiatives onto knowledge domains K1-K11, phases F0-F6 and artefacts.

Regulations and standards

Online entry

Data Act (Reg. 2023/2854)

Data Act

Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data. It regulates access to data generated by products and services and switching between providers (interoperability, avoiding vendor lock-in). In CDF it is addressed in Annex E (VDP controls - provider switching). In force - applicable from 12 September 2025.

Regulations and standards

Online entry

Data Gravity

Data Gravity

The tendency of data to attract applications and services - the more data resides in one place, the harder it is to move and the greater its influence on the target architecture. A key concept in designing AI environments.

Sovereignty and architecture

Online entry

Data Gravity Assessment

Data Gravity Assessment

A Phase 0 process examining the characteristics and location of data in terms of their impact on the architecture of the AI deployment. It assesses volume, rate of change, integration requirements, latency, regulation, switching costs and the data lifecycle.

CDF methodology

Online entry

Data Gravity Index (DGI)

Data Gravity Index

A seven-dimensional measure of data gravity calculated in Phase 0 on the basis of the dimensions: Volume, Velocity, Latency, Integration, Regulation, Switching Cost and Lifecycle. The result helps determine whether a sovereign on-premises, hybrid sovereign-cloud or air-gapped defence architecture will be most suitable. See DGI.

CDF methodology

See also: Latency

Online entry

Data lake

jezioro danych

A repository in which an organisation stores raw data in many formats: tables, documents, logs, images. Unlike a data warehouse, the data does not have to be structured first, and analytics and AI models draw on it. Without data descriptions and access control a lake quickly turns into a “data swamp”

Sovereignty and architecture

See also: Data Gravity, Data Provenance Tracking, Training data

Online entry

Data Minimisation

Principle of data minimisation

A GDPR principle (Article 5(1)(c)) requiring that personal data be adequate, relevant and limited to what is necessary for the purposes of processing. In CDF it is implemented in F2 through the Data Governance Package and the Data Quality Certificate.

Regulations and standards

GDPR

See also: RODO

Online entry

Data Provenance Tracking

Data Provenance Tracking

A mechanism for recording the full path of data - from source, through transformations, to use in an AI agent's decision. Introduced in CDF 1.4.4 as an element of Phase 6 (F6 Operate), based on NIST recommendations on agentic AI. It ensures auditability, compliance with the AI Act and the ability to reconstruct the basis of every decision of the cognitive system.

Sovereignty and architecture

AI Act

See also: AI Act, Training data, Data lake

Online entry

Deepfake

synthetic media (deep fake)

A voice, image or recording generated or altered by AI so that it seems to show real statements or events. The AI Act requires such content to be disclosed as artificially generated or manipulated. In a phone call, a deepfake is most often the cloned voice of a relative or of a “bank employee”

AI fundamentals

AI Act (Art. 3(60), Art. 50(4))

See also: Voice cloning, Transparency Notice, Voicebot, Generative AI

Online entry

Where we cover this: TURING:AI game

DEFENSE (ACE tag)

DEFENSE

An ACE tag activated for the defence sector (Ministry of National Defence (MON), Armed Forces, critical infrastructure of the State). It enables the NATO PRU sections, K12 CBP, F6-Full and the retraining pipeline. Always activated together with the SOVEREIGN and GOV tags.

CDF methodology

See also: SOVEREIGN (ACE tag), NATO PRU, F6-Full

Online entry

Delegation Chain Protocol

Delegation Chain Protocol (CDF, based on NIST NCCoE)

A protocol for the chain of delegation between AI agents. A CDF construct of its own, developing the authorisation pillar of the NIST NCCoE concept paper (5.02.2026). It is not a quotation from the NIST publication. It covers the “On Behalf Of” scenario (delegation token: identity of the delegator, scope, validity period, escalation policy), the Agent → Sub-Agent chain with the Scope Narrowing principle, Human Identity Binding and cascading revocation of delegation. Control T-012 ext., phase F2; the full delegation chain is recorded in the Immutable Audit Trail (A-F6-05); in Matrix E.4 the artefact is designated as the Delegation Chain Log.

CDF methodology

See also: NIST

Online entry

Deployer

Entity deploying an AI system (deployer)

A natural or legal person, public authority, agency or other body using an AI system under its authority (Article 3, point 4 of the AI Act; in the Polish text of the Regulation “podmiot stosujący”). The deployer has the obligations set out in Article 26: use in accordance with the instructions, human oversight, monitoring, provision of information and retention of logs; for public bodies and selected sectors additionally an FRIA (Article 27). In CDF the deployer role is mapped to phases F2 and F6.

Regulations and standards

AI Act

See also: AI Act

Online entry

Where we cover this: Act on AI systems - what you need to demonstrate

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment

Deployment Pattern Library

Deployment Pattern Library

A catalogued collection of reusable, proven AI deployment patterns enabling the rapid and safe replication of successes in subsequent departments or organisational units. Built in Phase 5 of CDF.

Deployment and governance

Online entry

DevSecOps

Development, Security & Operations

An approach integrating security practices into software development and maintenance processes. In the CDF context it is applied to managing the lifecycle of AI components with security built in at every stage.

Sovereignty and architecture

Online entry

DGA

Data Governance Act (Reg. 2022/868)

Regulation (EU) 2022/868 of the European Parliament and of the Council on European data governance. It establishes a framework for the re-use of public sector data, data intermediation services and data altruism. In the CDF context it is relevant to Phase 1 (data architecture) and domain K11 (AI sovereignty, data localisation), particularly in public sector deployments that use administrative data.

Regulations and standards

Online entry

DGI

Data Gravity Index

Abbreviation of Data Gravity Index. See Data Gravity Index (DGI).

CDF methodology

See also: Data Gravity Index (DGI), Data Gravity

Online entry

Diarisation

Recognising in a recording who speaks and when: the transcript is divided into statements assigned to people, with the time of each

AI fundamentals

RODO

See also: LLM, Token, On-premises / On-prem

Online entry

Where we cover this: SAIE Pantera

Digital Omnibus (EU)

EU Digital Package Omnibus Regulation

Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards simplifying the implementation of harmonised rules on artificial intelligence. Published in the Official Journal of the EU on 24.07.2026, in force from 27.07.2026. Key changes: Chapter III, Sections 1-3 for Annex III (stand-alone high-risk systems) - applicable from 02.12.2027 instead of 02.08.2026; for Annex I (systems embedded in a product) - from 02.08.2028 instead of 02.08.2027; machine-readable marking of synthetic content (Article 50(2)) for systems placed on the market before 02.08.2026 - by 02.12.2026; operational national sandboxes (Article 57) - by 02.08.2027; new prohibitions in Article 5 (child sexual abuse material, non-consensual intimate imagery) with a transitional period until 02.12.2026; relaxation of the AI literacy obligation (Article 4); clarification of the concept of a safety component (Article 6). Status: in force.

Regulations and standards

AI Act · Reg. 2026/1744

See also: AI Act

Online entry

Digital Resilience Testing (TLPT)

Digital Resilience Testing

The operational resilience testing programme for financial entities required by DORA (Articles 24-27). It includes threat-led penetration testing (TLPT) at least once every 3 years. In CDF it is mapped to F4 and F6 - Digital Resilience Testing Programme (item 35 of Matrix E.1).

Regulations and standards

DORA

See also: DORA

Online entry

DoD (Definition of Done)

Definition of Done

A set of formal criteria that must be met for a CDF phase to be considered complete and for the transition to the next phase to take place. The DoD is specific to each phase F0-F6 and covers both artefacts and quality conditions. Source: the Methodology, section CDF Phase Entry and Exit Criteria. Introduced in v1.4.4.

Deployment and governance

Online entry

DORA

Digital Operational Resilience Act (Reg. 2022/2554)

European Union Regulation (2022/2554) on digital operational resilience for the financial sector. In CDF it is addressed through DORA ICT Risk Mapping (F1.5), the DORA Compliance Addendum (A-F15-08, FINANCE tag), requirements for ICT providers, and exit strategies and third-party risk management (Matrix E.1, Articles 5-44).

Regulations and standards

Online entry

DPIA (Data Protection Impact Assessment)

Data Protection Impact Assessment

A formal assessment of the impact of personal data processing operations on the rights and freedoms of natural persons, required by Article 35 GDPR. In CDF it is mandatory for the CBP (Cognitive Digital Twin), since it involves systematic profiling of employees using AI. Carried out in Phase F1.5 (Compliance-First Delivery). See section “Personal Data Protection in the CBP (GDPR/DPIA)” in the Methodology.

Regulations and standards

GDPR

See also: RODO

Online entry

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment - hallucination quiz

DPO / IOD (Data Protection Officer)

Data Protection Officer / Inspektor Ochrony Danych

A person designated under Article 37 GDPR, responsible for monitoring compliance of personal data processing, cooperating with the supervisory authority and advising on DPIAs. In CDF the DPO (IOD) role is mapped to the RACI Matrix (F1.5) with mandatory assignment in the compliance profile.

Regulations and standards

GDPR

See also: RODO

Online entry

Drift (Model Drift)

Model Drift

The gradual deterioration in the quality of an AI model's predictions over time, caused by changes in input data, the operating environment or user behaviour. It requires monitoring, re-evaluation and, at times, retraining.

AI fundamentals

Online entry

Dual-Orbit Sovereignty Matrix

Dual-Orbit Sovereignty Matrix

A tool for assessing the geopolitical risk of the AI stack. It identifies three provider orbits: US-orbit, CN-orbit, EU-sovereign. It assesses: model availability, sanctions risk, data residency, supply chain resilience, IP protection. See Annex F, section 2.9.

CDF methodology

Online entry

ECS

Enterprise Cognitive Systems

Enterprise-class cognitive systems - advanced AI platforms integrated with enterprise processes, supporting decision-making, automation, knowledge analysis and agentic work.

AI fundamentals

Online entry

EHDS (Reg. 2025/327)

European Health Data Space

Regulation (EU) 2025/327 establishing the European Health Data Space, regulating the primary and secondary use of health data and their interoperability. In CDF it is addressed by the HDC mechanism (control HDC-1, artefact A-HDP-01), activated by the HEALTH tag. Phased application: supervisory authorities from 26 March 2027, full functionality 2029/2031.

Regulations and standards

Online entry

EN 18286:2026

EN 18286:2026 - Artificial intelligence: Quality management system for EU AI Act regulatory purposes

The first European standard supporting implementation of the AI Act, published by CEN/CENELEC on 22.07.2026. It concerns the AI quality management system required by Article 17 of the AI Act. The standard has not been cited in the Official Journal of the EU, so its application does not confer a presumption of conformity. Item QMS-1 of Matrix E.1, coverage status PARTIAL. Source class: N.

Regulations and standards

AI Act

See also: AI Act

Online entry

Enterprise AI Catalog

AI Solutions Catalogue

An internal library of ready-made and validated AI use cases available for redeployment in different parts of the organisation. It supports scaling in Phase 5.

Deployment and governance

Online entry

Entry into Force of the SSI Act

Application timetable of the Act on Artificial Intelligence Systems

Article 127 of the Act: the core of the Act applies from 11.08.2026 (14 days after publication), Article 125(4) from 28.07.2026 (the day after publication), and Articles 8-18 (individual opinions) together with Chapters 3 (inspections), 4 (proceedings), 5 (settlement), 8 (administrative fines and penal provisions) and 9 (amendments to other provisions) from 28.10.2026 (3 months after publication). In CDF the date 28.10.2026 marks the threshold for activation of the full inspection and sanctions regime in profiles bearing the GEO:PL tag.

Regulations and standards

Act on AI Systems

Online entry

ERP

Enterprise Resource Planning

An enterprise resource planning system, for example SAP or Oracle. In CDF it is a typical integration system in the enterprise AI architecture.

Deployment and governance

Online entry

EU

European Union

The European Union - a supranational organisation that is the regulator of, among others, the EU AI Act, DORA, NIS2 and other frameworks affecting AI deployments in regulated sectors.

Regulations and standards

Online entry

EU Database (EU database for AI systems)

EU database for high-risk AI systems

A database maintained by the European Commission (Article 71 of the AI Act) in which high-risk AI systems are registered before being placed on the market or put into service (registration obligation - Article 49). Most entries are publicly accessible; entries relating to law enforcement and migration are held in a non-public section. In CDF it is carried out in phase F5 - EU Database Registration Process.

Regulations and standards

AI Act

See also: AI Act

Online entry

Where we cover this: Act on AI systems - AI Act classifier

Evidence Book

CDF Evidence Layer

Annex G of the CDF Methodology - an artefact supporting the evidence layer of the Methodology. It comprises: EB-1 Regulatory Mapping, EB-2 Case Studies, EB-3 Sample Deliverables, EB-4 Boundary Conditions of Claims, EB-5 Benchmarks and Metrics (including EB-5.2 NASK 2026 baseline) and G.9 Acceptance Criteria. Introduced in v1.4.4, developed in v1.4.4-r4, extended in 1.6.0.

Deployment and governance

Online entry

Evidence Readiness

Evidence Readiness

The organisation's ability to present - in the event of a product liability claim (PLD Directive 2024/2853) - a complete and credible body of evidence (Agent Registry, decision logs, model documentation, Evidence Book) serving as proof of due diligence that rebuts the presumptions of defectiveness and causal link (Article 10 PLD). Implemented through control LER-1. Introduced in CDF 1.5.0.

Deployment and governance

PLD 2024/2853

See also: PLD (Directive 2024/2853)

Online entry

Executive Alignment Workshop

Executive Alignment Workshop

A workshop for the C-Suite carried out in Phase 0, the aim of which is to align business priorities, expected outcomes and time horizons for the AI transformation programme.

Deployment and governance

Online entry

Exit Strategy

Exit Strategy

A plan for the emergency or planned termination of cooperation with an AI provider, covering the transfer of data, source code, documentation and operational knowledge. In CDF it is required in Phase 1.5 as an element of NIS2/uKSC and DORA compliance.

Deployment and governance

DORA

See also: DORA

Online entry

F6-AFC-01

AI Concerns Channel Register (catalogue designation A-F6-07)

The designation used in section F6 of the Methodology for the AI Concerns Feedback Channel Register artefact; in the CDF Artefact Catalogue this item has the identifier A-F6-07 (AI Concerns Channel Register, F6, CORE, owner CDF Lead, introduced in 1.5.0). It documents the channel configuration (form, e-mail, portal), the handling procedure, response SLA, escalation path, history of reports and actions taken. It fulfils the requirement of ISO/IEC 42001 Annex A - A.3.3; the results of the analysis of reports feed the Evidence Book and the periodic ASIA reviews.

CDF methodology

See also: AI Concerns Feedback Channel, AI Act

Online entry

F6-Full

Full mode of Phase 6

The extended mode of Phase 6 (CogOps) activated by the SCALE or DEFENSE tag (Table 38 of the Methodology): F6-Lite + Knowledge Graph Governance, retraining pipeline, industrialisation of CogOps and the Deployment Pattern Library. Profiles: DEFENSE, MULTI-JURIS.

CDF methodology

See also: Cognitive Degradation Monitoring, Knowledge Freshness Index, CogOps, SCALE (ACE tag)

Online entry

F6-Lite

Simplified mode of Phase 6

The basic mode of Phase 6 (CogOps) activated by the PRODUCTION tag (Table 38 of the Methodology): operational monitoring, alerts, compliance audit, periodic performance review. Sufficient for any production deployment without full scale. Profiles: STANDARD, STANDARD+AGENT, FINANCE, GOV, SOVEREIGN, ENTERPRISE, HEALTH.

CDF methodology

See also: Cognitive SLA Tier, Cognitive SLA, PRODUCTION (ACE tag), CogOps

Online entry

FINANCE (ACE tag)

ACE configuration tag

An ACE tag activated for the financial sector. It enables the DORA, ICT third-party risk and KNF-specific sections. It automatically enforces REGULATED (guardrail CV-01, AUTO-CORRECT); the absence of DORA in question 7 generates warning MV-01.

CDF methodology

See also: REGULATED (ACE tag), DORA

Online entry

Fine-tuning

Model fine-tuning

The process of further training a pre-trained AI model on a specific dataset in order to adapt it to a particular domain, style or type of task.

AI fundamentals

Online entry

FRIA

Fundamental Rights Impact Assessment

A fundamental rights impact assessment required by the EU AI Act (Article 27) for high-risk AI systems deployed by bodies governed by public law or by operators of public services. In CDF it is carried out as a component of ASIA in Phase F1.5.

Regulations and standards

AI Act

See also: AI Act

Online entry

Where we cover this: Act on AI systems - AI Act classifier

Fully On-Premises

Full on-premises deployment

A deployment pattern in which the entire core AI layer, data, logs, agent orchestration and integrations remain within the client's on-premises infrastructure. Applied where data sovereignty, operational control and the reduction of vendor risk are of key importance.

Sovereignty and architecture

Online entry

GDPR

General Data Protection Regulation (Reg. 2016/679)

The European Union's general regulation on the protection of personal data, directly applicable in all Member States since 25 May 2018. In Poland it operates under the name RODO; the national Act of 10 May 2018 on the Protection of Personal Data merely supplements it. In CDF it forms the foundation of the requirements governing the processing of personal data by AI systems. See RODO.

Regulations and standards

GDPR

See also: RODO

Online entry

Generative AI

AI generatywna

AI models that create new content: text, images, sound or code, based on a prompt and the patterns learned from their training data. Large language models are the best-known example. The AI Act requires providers of such systems to mark generated content in a machine-readable way, and in an organisation’s work a person checks the output, because a model can state something untrue with full confidence

AI fundamentals

AI Act (Art. 50(2))

See also: LLM, Hallucination, Training data, Deepfake

Online entry

GEO (ACE tag)

ACE location tag

The jurisdictional layer of ACE, operating independently of the sector tags. Variants: GEO:PL (Poland), GEO:EU (another EU/EEA country), GEO:MULTI (multi-jurisdictional), GEO:NON-EU (outside the EU).

CDF methodology

Online entry

Global Rollout

Global deployment / scaling

A process carried out in Phase 5, consisting in the replication of standardised AI agents, patterns and components across further departments, units or business areas.

CDF methodology

Online entry

GOV (ACE tag)

ACE configuration tag

An ACE tag activated for the public or defence sector. It enables sections specific to public administration, NATO PRU, the MC template and classified information. It automatically enforces REGULATED.

CDF methodology

See also: REGULATED (ACE tag), NATO PRU

Online entry

Governance Divergence Matrix

US-EU governance divergence matrix

A CDF analytical tool (Annex F, section 2.11, Table 84) comparing the EU and US regulatory approaches in the area of AI governance. It covers 8 areas: Safety Guardrails, Transparency / Disclosure, Data Ownership, Incident Reporting, Liability Model, Risk Classification, Bias / Fairness, Supply Chain Compliance. For each area it sets the requirements of the EU AI Act against clause GSAR 552.239-7001 (“American AI”, GSA 03/2026) and NIST AI RMF, and indicates the relevant CDF control and phase. General principle: “strictest applicable” - for deployments spanning both jurisdictions, the more restrictive requirements (EU) apply, with the divergence annotated in the SoA. See US-EU AI Governance Divergence.

CDF methodology

See also: Conformity Assessment, AI Act, NIST

Online entry

Groq 3 LPU

Groq 3 LPU / NVIDIA Groq 3 LPX

An inference accelerator based on Groq technology (LPU, used by NVIDIA under licence from Groq, Inc.), offered by NVIDIA as Groq 3 LPX - an extension of the Vera Rubin platform for interactive agentic inference; full production announced by NVIDIA on 24.08.2026 (according to NVIDIA, 4 times faster responsiveness in agentic tasks than the nearest alternative platform). In CDF it is included in the compute infrastructure benchmarks (Table 15 in the Methodology, where it still appears as a Groq product) as a reference for ultra-low-latency scenarios and K8 agentic workloads.

Sovereignty and architecture

Online entry

Ground Truth

Reference truth

A verified, correct state of knowledge or answer serving as the point of reference for measuring the accuracy of AI reasoning. Used in the definition of the Reasoning Accuracy Rate metric in the Cognitive SLA (Table 14 of the Methodology).

AI fundamentals

Online entry

Hallucination

Model hallucination

The phenomenon of an AI generating information that is untrue, unconfirmed or not grounded in credible sources. CDF assumes a very low tolerance for this phenomenon and, in critical processes, its active mitigation and continuous measurement.

AI fundamentals

Online entry

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment - hallucination quiz

Where we cover this: Knowledge hub

Hallucination Rate

Hallucination Rate

A Cognitive SLA metric (Table 14 of the Methodology) specifying the percentage of responses containing information unconfirmed by sources or contradicting the knowledge base. CDF targets: ≤ 2% for critical applications, ≤ 5% for standard ones; exceeding 5% in a critical process triggers a Red escalation (Agent Kill-Switch). A Tier 1 metric (baseline, required for all profiles).

AI fundamentals

Online entry

HCG

Human Competence Gate

Abbreviation of Human Competence Gate. See Human Competence Gate (HCG).

Deployment and governance

See also: Human Competence Gate (HCG)

Online entry

HCG Audit Log Specification

HCG Audit Log Specification

An F2 artefact defining the logging format for human-AI interactions within the Human Competence Gate.

CDF methodology

See also: Human Competence Gate (HCG)

Online entry

HCG Control Policy

HCG Control Policy

An F2 artefact defining the rules of human oversight of the AI system: who approves which decisions, and at what confidence threshold.

CDF methodology

Online entry

HCG-Full

Full Human Competence Gate mode

The extended HCG mode activated by the AGENT + REGULATED tags: full HCG matrix, a checkpoint per use case, a decision audit log, a register of control questions, escalation and periodic review.

CDF methodology

See also: REGULATED (ACE tag)

Online entry

HCG-Lite

Simplified Human Competence Gate mode

The basic HCG mode activated by the CORE tag: at least one human checkpoint per AI deployment, a go/no-go decision before production launch, and a clear definition of who is responsible for oversight.

CDF methodology

See also: CORE (ACE tag)

Online entry

HDC

Health-AI Compliance

The AI compliance mechanism for the health sector, embedding in the Methodology a regime activated upon entry into the medical market: EHDS (access to and secondary use of health data), MDR/IVDR (qualification of the AI system as medical device software, coupled with the high-risk pathway under Annex I of the AI Act) and Article 9 GDPR (special categories of data). Gated by the HEALTH tag. Comprises controls HDC-1 and HDC-2. Phases F1.5/F2. Artefacts: A-HDP-01, A-MDR-01. Introduced in CDF 1.5.0.

CDF methodology

See also: A-HDP-01, A-MDR-01, AI Act, HEALTH (ACE tag), HDC-1

Online entry

HDC-1

Health Data Governance

A CDF control of the HDC mechanism: processing of special categories of data (Article 9 GDPR), secondary use and interoperability in accordance with EHDS. An extension of the K3 Data Governance mechanism (the building block already exists - not a new mechanism). Knowledge domain KD3. Phases F1.5/F2. Artefact A-HDP-01. Introduced in CDF 1.5.0.

CDF methodology

See also: A-HDP-01, EHDS (Reg. 2025/327), RODO

Online entry

HDC-2

Medical Device AI Conformity

A CDF control of the HDC mechanism: assessment of the qualification of the AI system as medical device software (MDR 2017/745 / IVDR 2017/746) and coupling with the high-risk pathway under Annex I of the AI Act. A new control - CDF did not previously cover medical device conformity. Knowledge domain KD8. Phase F1.5. Artefact A-MDR-01. Introduced in CDF 1.5.0.

CDF methodology

See also: A-MDR-01, AI Act, IVDR (Reg. 2017/746)

Online entry

HEALTH (ACE tag)

HEALTH - ACE configuration tag

An ACE configuration tag activated when the deployment concerns the health sector (health data, AI medical device, EHDS). It enables the HDC mechanism (controls HDC-1/HDC-2) as well as cross-validation rules CV-10 (auto-activation of the REGULATED tag) and CV-11. Linked to the HEALTH reference profile. Introduced in CDF 1.5.0.

CDF methodology

See also: AGENT (ACE tag), CORE (ACE tag), FINANCE (ACE tag), GOV (ACE tag), PRODUCTION (ACE tag)

Online entry

HEALTH Profile

HEALTH Reference Profile

An ACE reference profile for healthcare entities and providers of medical AI. Archetype: health data, AI medical device, EHDS. Active tags: CORE + PRODUCTION + REGULATED + HEALTH + GEO:xx (+ AGENT where agents are present). Phases F0→F6-Lite, Cognitive SLA Tier 2, HCG-Full. The eleventh CDF reference profile. Profile card: Table 52 in the Methodology. Introduced in CDF 1.5.0.

CDF methodology

See also: Cognitive SLA Tier, Cognitive SLA, PRODUCTION (ACE tag), REGULATED (ACE tag), HCG-Full

Online entry

High-risk AI system

High-risk AI system

An AI system in a field listed in Annex III of the AI Act (recruitment, creditworthiness, access to public services, education, critical infrastructure, biometrics) that decides about people or materially influences a decision - unless it performs only a narrow procedural task (Art. 6(3)). Profiling of persons is always high-risk. Deployer obligations under Arts. 26 and 27 apply from 2.12.2027

Regulations and standards

AI Act

See also: Deployer, FRIA, EU Database (EU database for AI systems), Conformity Assessment, AI Act

Online entry

Where we cover this: Act on AI systems - AI Act classifier

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment

HITL

Human-in-the-Loop

A model of AI oversight in which a human participates in the decision-making process or is able to block, reverse or correct it. In CDF it is one of the fundamental governance and safety mechanisms.

AI fundamentals

AI Act

See also: AI Act

Online entry

HR

Human Resources

The area of human resources management. In CDF it appears both as a potential AI use case and as an example of a domain in which the level of sovereignty may be lower than in mission-critical systems.

Deployment and governance

Online entry

Human Competence Gate (HCG)

Verification of the decision-maker's competence before acceptance of an AI decision

A mechanism in which the AI system, before allowing a user to approve a decision, generates a context-dependent set of questions testing the user's understanding of the material facts, key consequences, and the limitations and exceptions relevant to the matter at hand. Failure to meet the defined correctness threshold blocks approval of the decision and may result in escalation or in the user being directed to additional training material. Implemented from Phase 2 of CDF onwards. The system generates 5-15 contextual Yes/No questions. See HCG.

Deployment and governance

Online entry

Human Factors Monitoring

Human Factors Monitoring

A category of post-deployment monitoring under NIST AI 800-4 (key question: is the system transparent to humans and of high quality). Within it NIST identifies: limited understanding of user intent and perception, dark interaction patterns (sycophancy, anthropomorphisation), human-system feedback loops, and the cost of collecting and evaluating user feedback. CDF extends this category with its own indicators: automation bias, skill degradation and overtrust (override frequency, output validation time, rate of escalation to a human). An element of F5/F6 CogOps.

Deployment and governance

See also: NIST AI 800-4, NIST

Online entry

Human Override

Human override

A mechanism enabling a human to halt, block, reverse or correct a decision taken by an AI system. In regulated sectors it constitutes a fundamental element of genuine human oversight.

AI fundamentals

Online entry

Hybrid Sovereign-Cloud

Hybrid sovereign architecture

A deployment pattern in which critical data, organisational memory, access control and key governance components remain under the organisation's control, while part of the computing capacity or of the models may operate in a trusted cloud environment.

Sovereignty and architecture

Online entry

ICT Security Addendum

ICT security addendum

A contractual supplement used in particular in the context of NIS2/uKSC, covering security clauses, the right of audit, incident management, backup, exit strategy and the assessment of ICT and AI providers. Implemented in Phase 1.5 of CDF.

CDF methodology

See also: NIS2/uKSC

Online entry

Immutable Audit Trail

Immutable event log

A system log whose entries cannot be deleted or altered without leaving a trace. In CDF it forms the foundation of automatic logging, auditability and the evidential value of the actions of AI and agents.

Sovereignty and architecture

AI Act

See also: AI Act

Online entry

Individual Opinion

Individual Opinion of the Commission

An interpretation by the Commission concerning the application of the AI Act or the Act to a specific AI system (Articles 8-18). The fee is PLN 150 (Article 11); the time limit is 30 days, or 60 days in a particularly complex case (Article 12). Failure to issue an opinion is deemed an opinion consistent with the applicant's position; the opinion is binding within the scope of the case (Article 13) and, once anonymised, is published in the Commission's Public Information Bulletin (BIP) (Article 17).

Regulations and standards

AI Act

See also: AI Act

Online entry

Inference

Model inference

The operational phase of an AI model in which it produces predictions, generates responses or recommendations on the basis of new input data.

AI fundamentals

Online entry

Innovation Plateau Diagnostic

Innovation plateau diagnostic

A CDF Phase 0 tool (artefact A-F0-07) diagnosing the Innovation Plateau - an organisational state in which investment in AI does not translate into business value. It identifies 5 types of plateau: (1) Pilot Purgatory, (2) Scale Paralysis, (3) Governance Gridlock, (4) Cultural Resistance, (5) Data Readiness. Each type has its own remediation plan in CDF.

Deployment and governance

Online entry

ISO/IEC 23894

ISO/IEC 23894:2023

A standard concerning risk management in AI systems. It provides guidance on the identification, assessment and mitigation of risks associated with the design, deployment and use of AI.

Regulations and standards

ISO/IEC 42001

See also: ISO/IEC 42001

Online entry

ISO/IEC 42001

ISO/IEC 42001:2023

A standard defining an artificial intelligence management system (AIMS) - a certifiable management system for organisations developing or deploying AI, with a catalogue of controls in Annex A.

Regulations and standards

See also: AIMS

Online entry

Where we cover this: AI use policy - template

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment - hallucination quiz

IVDR (Reg. 2017/746)

In Vitro Diagnostic Regulation

Regulation (EU) 2017/746 on in vitro diagnostic medical devices. It covers diagnostic software, including AI systems. In CDF it is addressed by control HDC-2 (artefact A-MDR-01), together with the MDR.

Regulations and standards

AI Act · MDR/IVDR

See also: AI Act

Online entry

J-curve of Productivity

Productivity J-curve

The phenomenon of a temporary decline in employee efficiency at the start of an AI deployment. CDF parameterisation: a dip of −10% to −30% over 3-9 months (F0- F3), an inflection point (F4), acceleration of +40-300% (F5-F6). ECS causal mechanisms: reaching critical mass of the KG, completion of Cognitive Succession, maturity of the Skill Partnership. In CDF this phenomenon is planned for and managed as an element of the ROI Baseline and the Scale Path Definition.

Deployment and governance

Online entry

Jailbreak

obejście zabezpieczeń modelu

An attempt to talk an AI model into breaking its rules, e.g. through role play, a “no limits mode” or an instruction hidden in a long text. The aim is an answer the model should not give, or disclosure of data. Unlike prompt injection, a jailbreak is usually typed in by the user. An organisation limits the risk with filters on the model’s input and output

AI fundamentals

See also: Prompt Injection, AI gateway, Hallucination

Online entry

Jurisdiction Compliance Card

Jurisdiction card

An ACE artefact generated in F0: a document describing the base law, national law, supervisory institutions, the timeline of requirements and the artefacts specific to the deployment location.

CDF methodology

Online entry

KG-RAG Integration Governance

KG-RAG integration governance

A set of rules (Phase 6 of CDF) ensuring that generative agents draw exclusively on current, validated sources in the knowledge graph. It comprises the Knowledge Freshness Monitoring and Knowledge Audit Trail mechanisms.

CDF methodology

See also: Knowledge Freshness Monitoring, Knowledge Audit Trail

Online entry

Kill/Pivot Criteria

Criteria for termination or change of direction

Pre-defined conditions under which an AI pilot should be terminated or redirected. An element of the Scale Path Definition. Note: to be distinguished from the Scale-or-Kill Gate - a mandatory binary decision point (Scale / Kill) that deliberately eliminates the “extend pilot” option, where “Kill” = a positive outcome (avoidance of a costly production investment).

Deployment and governance

Online entry

Knowledge Audit Trail

Knowledge base audit trail

A complete, immutable audit trail recording all changes to the organisation's knowledge base. It satisfies regulators' requirements regarding the transparency and inspectability of the AI system (Phase 6 of CDF).

CDF methodology

Online entry

Knowledge Curator

Knowledge curator

A dedicated organisational role responsible for the quality, currency, security and versioning of the knowledge graph. It manages Ontology Change Control and the knowledge freshness indicators. The role is introduced in Phase 6 of CDF.

CDF methodology

See also: Ontology Change Control

Online entry

Knowledge Debt Management

Knowledge debt management

The systematic identification and elimination of the organisation's information debt, comprising documentation gaps, data silos, outdated procedures and the dispersion of knowledge, which limit the effectiveness of AI systems. Carried out in Phase 6 of CDF.

AI fundamentals

Online entry

Knowledge Freshness Index

Knowledge freshness index

A measure used in the Cognitive SLA specifying what proportion of the knowledge base has been updated within a defined time window. A Tier 3 Cognitive SLA metric (active from the SOVEREIGN/SCALE profile). CDF target: ≥95% within a 7-day time window.

CDF methodology

See also: Cognitive SLA Tier, Cognitive SLA, SOVEREIGN (ACE tag), SCALE (ACE tag)

Online entry

Knowledge Freshness Monitoring

Knowledge Freshness Monitoring

An automatic F6 alerting system triggered when the knowledge staleness threshold in the Knowledge Graph or RAG is exceeded.

CDF methodology

See also: Knowledge Graph

Online entry

Knowledge Graph

Knowledge graph

A structured representation of organisational knowledge in the form of a graph of entities and relationships, forming the foundation of RAG systems in CDF. It is subject to strict Knowledge Graph Governance in Phase 6 (Knowledge Curator, Ontology Change Control, KG-RAG Integration Governance).

AI fundamentals

Online entry

KPI

Key Performance Indicator

Key performance indicator - a measurable gauge of the achievement of a business, operational or deployment objective.

Deployment and governance

Online entry

Latency

Latency

The time a system needs to respond or to perform an operation. In AI architecture it matters both at the infrastructure level and at the level of use.

AI fundamentals

Online entry

LER

Liability Evidence Readiness

A family of CDF mechanisms ensuring evidence readiness for product liability under Directive 2024/2853 (PLD), which makes software and AI systems products subject to no-fault liability. LER binds the existing evidential carriers (Agent Registry, Immutable Audit Trail, Evidence Book) into a regime enabling the rebuttal of the presumptions of defectiveness and causal link (Articles 9-10 PLD) and the fulfilment of the duty of disclosure of evidence. Comprises controls LER-1 and LER-2. Phases F1.5/F2/F6. Artefact: A-PLD-01. Introduced in CDF 1.5.0.

CDF methodology

See also: Immutable Audit Trail, Agent Registry, Evidence Book, A-PLD-01, LER-1

Online entry

LER-1

Product Liability Evidence Readiness

A CDF control of the LER mechanism: maintaining the complete body of evidence (model and data documentation, decision logs, Agent Registry, versioning, security tests) in a state enabling the rebuttal of the presumptions under Article 10 of PLD Directive 2024/2853 and the fulfilment of the duty of disclosure under Article 9, with protection of trade secrets. Knowledge domains KD8/KD6/KD3. Phases F1.5/F2/F6. Introduced in CDF 1.5.0.

CDF methodology

See also: Agent Registry

Online entry

LER-2

Substantial Modification Register

A CDF control of the LER mechanism: a register of substantial modifications (fine-tuning, continuous learning, updates) signalling the moment at which the deployer assumes the role of manufacturer (Article 8(2) of PLD Directive 2024/2853) and takes on liability. Knowledge domains KD1/KD4. Phases F2/F6. Introduced in CDF 1.5.0.

CDF methodology

Online entry

Liability Framework

AI legal liability framework

A structure defining the chain of legal liability for the decisions and actions of an AI system in a production environment. It covers three levels: the liability of the operator (deployer), of the provider, and of the organisation (the board) as the owner of the system. In CDF it is linked to the Accountability Matrix (per LOA, Annex B, Table 62) and to the LER mechanism (product liability under PLD 2024/2853), and mapped to the requirements of Articles 9, 25 and 26 of the EU AI Act.

Regulations and standards

AI Act

See also: AI Act

Online entry

LLM

Large Language Model

A large language model trained on very large bodies of text, capable of generating natural language, summarising, classifying, extracting information and supporting agents.

AI fundamentals

Online entry

Where we cover this: Bielik and PLLuM

LOA

Level of Autonomy

An abbreviation denoting the level of autonomy of an AI agent on the five-level CDF Autonomy Scale (L0-L4). See Autonomy Scale (L0-L4).

AI fundamentals

See also: Autonomy Scale (L0-L4)

Online entry

Machinery Regulation (Reg. 2023/1230)

Machinery Regulation

Regulation (EU) 2023/1230 on machinery, replacing Directive 2006/42/EC. It covers machinery with AI systems performing safety functions. Applicable from 20 January 2027; Regulation (EU) 2026/1744 changed the rules for classifying machinery with an AI component as high-risk systems and postponed the application of the Annex I obligations of the AI Act to 02.08.2028. Included in the Compliance Timeline Tracker (Table 20 of the Methodology).

Regulations and standards

AI Act

See also: AI Act

Online entry

Make-vs-Buy Decision Framework

Make vs Buy decision framework

A structured economic and operational assessment carried out in Phase 0, providing the rationale for choosing between building an AI solution in-house and purchasing ready-made components or services. It takes into account TCO, risk, time to deploy and vendor lock-in.

Deployment and governance

Online entry

Maturity Roadmap

Maturity Roadmap

ACE artefact generated in F0: a development path from the current profile to a higher one, with a timeline. For example, STARTER → STANDARD in 6 months.

Deployment and governance

Online entry

MC

Ministry of Digital Affairs

The Polish Ministry of Digital Affairs (Ministerstwo Cyfryzacji) - author of the draft model contractual clauses for public procurement of AI systems (ref. DPiS.WWKS.002.20.1.2026, letter of 16.02.2026; draft under consultation, recommended in CDF as the negotiation baseline, class M) and of the Guide to Artificial Intelligence for Public Administration (March 2026, class M, the basis of the PAG mechanism).

Regulations and standards

AI Act

See also: AI Act

Online entry

MC Guide to AI

Guide to Artificial Intelligence for Public Administration

A document of the Ministry of Digital Affairs of March 2026. A class M source in the CDF canon: without binding force, but setting the standard of conduct against which an institution is assessed by the supervisory authority and the auditor. An eight-stage deployment process from Stage 0 (necessity assessment) to Stage 7 (periodic review), a “do / don't” summary across six areas (in the Methodology: the matrix of prescriptions and prohibitions) and a six-point decision checklist for staff. Mapping to CDF phases and controls: Annex D.4. The basis for the PAG mechanism and the LOA ≤ L2 restriction.

Regulations and standards

Online entry

MCP

Model Context Protocol

An open protocol (Anthropic, 2024; specification version 2026-07-28) standardising communication between AI agents and external tools, data sources and services. In CDF it is subject to six security requirements, MCP-REQ-01 to MCP-REQ-06 (OAuth authentication, input validation, network isolation with TLS 1.3, monitoring and audit, protection against tool poisoning, least privilege), implemented through controls MCP-CTL-01 to MCP-CTL-06 (Control Catalogue, AGENT tag, artefact A-F2-08). See MCP Security.

AI fundamentals

Online entry

MCP Security

MCP Security Requirements (CDF's own interpretation)

Six security requirements for the Model Context Protocol layer, designated MCP-REQ-01 to MCP-REQ-06. The numbering and structure are CDF's own interpretation and do not originate from the MCP specification. Sources: the MCP specification version 2026-07-28 (the normative Authorization section: OAuth 2.1, RFC 6750, 8414, 8707, 9207, 9728, OIDC Discovery and Client ID Metadata Documents; dynamic client registration under RFC 7591 is marked as deprecated and retained solely for backward compatibility), the Security Best Practices document (in the docs/tutorials/security part of the specification) and the NSA AI Security Center Cybersecurity Information Sheet “Model Context Protocol (MCP): Security Design Considerations for AI-Driven Automation”, ver. 1.0, May 2026 (NSA announcement of 20.05.2026; document issued by the NSA alone, without CISA). Implemented through controls MCP-CTL-01 to MCP-CTL-06.

Sovereignty and architecture

See also: MCP

Online entry

MDR (Reg. 2017/745)

Medical Device Regulation

Regulation (EU) 2017/745 on medical devices. It covers software qualified as a medical device, including AI systems. In CDF it is coupled with the high-risk pathway under Annex I of the AI Act and addressed by control HDC-2 (artefact A-MDR-01).

Regulations and standards

AI Act · MDR/IVDR

See also: AI Act

Online entry

MEP

Mechanical, Electrical & Plumbing

The technical infrastructure of a building, comprising mechanical, electrical and plumbing installations. It is of key importance in the design of on-premises AI infrastructure and data centres.

Sovereignty and architecture

Online entry

MES

Manufacturing Execution System

A manufacturing execution system - software for managing production and operational processes at the execution level.

Deployment and governance

Online entry

MFA

Multi-Factor Authentication

Multi-factor authentication - an identity verification mechanism requiring at least two independent factors (e.g. a password plus a hardware token). In CDF it is required as an element of Zero Trust for access to AI systems and agent management consoles.

Sovereignty and architecture

Online entry

Minimum Sufficient Sovereignty (MSS)

Minimum Sufficient Sovereignty

A CDF design principle under which the level of isolation, localisation and control over an AI system is chosen so as to be sufficient to meet regulatory, security, business continuity and IP protection requirements, but no greater than necessary. It protects the organisation against both over-engineering and under-engineering of its AI architecture. See MSS (Minimum Sufficient Sovereignty).

Sovereignty and architecture

Online entry

Mitigation Response Time

Mitigation Response Time

A Cognitive SLA metric (Table 14 of the Methodology): the time from detection of a cognitive error to its correction. Targets: ≤ 15 min for critical errors, ≤ 4 h for standard errors. A Tier 1 metric.

CDF methodology

See also: Cognitive SLA

Online entry

Model Degradation

Model Degradation

A decline in the effectiveness and correctness of an AI model's operation in a production environment. In CDF, degradation is subject to systematic monitoring within CogOps and is treated on a par with drift as an operational risk.

AI fundamentals

Online entry

Model Selection Compliance Matrix

AI Model Selection Compliance Matrix

A CDF decision tool (Annex F, section 2.10, Table 83) supporting the selection of AI models. It scores each model across 6 dimensions on a 1-5 scale: Data Sovereignty, AI Act Compliance, Vendor Lock-in Risk, Censorship / Alignment Risk, Supply Chain Sanction Risk, Cost / TCO Transparency. The total score (6-30 points) classifies the model: 25-30 low risk, 18-24 acceptable with mitigation, 12-17 requires escalation to the board, below 12 unacceptable (blocked in F2); in the CSE-GOV variant the acceptance threshold is 20 points. Completed in F0 and updated in F2. Linked to the Dual-Orbit Sovereignty Matrix and the Vendor Disruption Protocol.

CDF methodology

See also: Dual-Orbit Sovereignty Matrix, SBOM (Software Bill of Materials)

Online entry

Model sycophancy

Model sycophancy

The tendency of a language model to agree with the user and confirm the assumption contained in the prompt instead of assessing the facts. The prompt “find irregularities” gets an answer full of irregularities, and “assume it is fine” gets a reassuring answer. It is reduced by prompts without an assumption: a request for facts, arguments for and against, and matters for a human to decide

AI fundamentals

M. Sharma et al., Towards Understanding Sycophancy in Language Models, ICLR 2024

See also: Hallucination, Human Factors Monitoring

Online entry

MSS (Minimum Sufficient Sovereignty)

Minimum Sufficient Sovereignty

Abbreviation of Minimum Sufficient Sovereignty. The minimum required level of AI sovereignty for a given profile, determined in F0 on the basis of the SLA-S. See Annex F. See Minimum Sufficient Sovereignty (MSS).

CDF methodology

See also: Minimum Sufficient Sovereignty (MSS), SLA-S

Online entry

Multi-agent

Multi-agent AI System

An architecture in which multiple autonomous agents cooperate to carry out more complex tasks or end-to-end processes.

AI fundamentals

Online entry

Multi-Jurisdiction Compliance Map

Multi-Jurisdiction Compliance Map

An ACE artefact generated in F0 for the GEO:MULTI profile: requirements per jurisdiction, regulatory conflicts, Cross-Border Data Transfer Assessment.

CDF methodology

Online entry

MVOrg / MVOp (formerly MVO)

Minimum Viable Organization (MVOrg) / Minimum Viable Operation (MVOp)

MVOrg (Minimum Viable Organization) - the minimum configuration of competences, governance and technical capabilities required before initiating an ECS deployment (including an Executive Sponsor, the Knowledge Curator role and the data inventory from F0). MVOp (Minimum Viable Operation) - the minimum operational version of a back-office process performed by a swarm of AI agents (Autonomous swarm, LOA L2-L3) in a controlled manner before full scaling; the third level of production deployment in Phase 4. The acronym MVO has been withdrawn from use owing to a semantic collision.

Deployment and governance

Online entry

MVP

Minimum Viable Product

A version of a product with the minimum set of features sufficient to validate an idea or a direction of development.

Deployment and governance

Online entry

Named Shortcut (ACE)

ACE Named Shortcut

An ACE reference profile (e.g. STARTER, FINANCE, SOVEREIGN) serving as a named shortcut for a typical combination of tags. A configuration starting point - the organisation may modify the tags independently of the profile selected.

CDF methodology

See also: SOVEREIGN (ACE tag), FINANCE (ACE tag)

Online entry

NASK

Research and Academic Computer Network (Naukowa i Akademicka Sieć Komputerowa)

A state research institute operating CSIRT NASK - one of the three national-level CSIRT teams (alongside CSIRT GOV and CSIRT MON) - and the operator of the S46 System. In the context of CDF and the uKSC/NIS2, the entity to which essential and important entities report cybersecurity incidents.

Regulations and standards

Online entry

NASK 2026 Study

AI in Public e-Administration - the Perspective of Officials and Institutions

Report by NASK-PIB of 17 March 2026. A class D source in the CDF canon: it does not create requirements, but provides an adoption baseline for the CSE-GOV variant (section D.5) and the boundary conditions for four solution concepts. The quantitative study is described by its authors as exploratory and pilot in nature, and the sample as non-representative; the values may be used as comparative material within the sample, not as population parameters or as the basis for contractual commitments (boundary condition EB-4).

Regulations and standards

See also: NASK

Online entry

NASK GOV Prerequisites

NASK GOV Prerequisites

A checklist of prerequisites for the CSE-GOV variant (artefact A-F0-11, tag GOV+GEO:PL, introduced in CDF 1.5.0), verified in F0 before the transition to F1. Based on the data of the NASK 2026 Study, it covers: the existence of internal AI deployment procedures, a staff training plan, the definition of the level of human oversight (LOA) and the availability of sovereign AI infrastructure (local models, PL/EU data residency). It complements the GOV Deployment Prerequisites (Annex D.3).

CDF methodology

See also: NASK

Online entry

NATO PRU

NATO Principles of Responsible Use of AI

The principles of responsible use of AI adopted by NATO, comprising: lawfulness, responsibility, explainability, reliability, governability and bias mitigation. In CDF, addressed for the defence sector through artefact A-F15-09 NATO PRU Compliance Addendum (tag DEFENSE).

Regulations and standards

Online entry

NGAC

Next Generation Access Control

A next-generation access control model, standardised as ANSI/INCITS 499 (NGAC-FA, functional architecture) and ANSI/INCITS 525 (NGAC-IRPAD, implementation requirements, protocols and API); compared with XACML in NIST SP 800-178. Based on attributes and policies, it enables dynamic management of AI agent permissions in a multi-agent environment. In CDF, applied as a recommendation for Phase 2 alongside SPIFFE/SPIRE and SCIM.

Sovereignty and architecture

See also: NIST

Online entry

NIS2/uKSC

NIS2 / National Cybersecurity System

Directive (EU) 2022/2555 (NIS2) and the amended Act on the National Cybersecurity System (uKSC) implementing it - cybersecurity regulations for essential and important entities. For ICT/AI providers (CDF): security clauses in contracts, right of audit, incident reporting within ≤24h, supply chain risk management. Implemented in Phase 1.5 as the ICT Security Addendum.

Regulations and standards

Online entry

NIST

National Institute of Standards and Technology

The US standards institute within the US Department of Commerce. In CDF, cited as the source of frameworks: NIST AI RMF (AI risk management), NIST SP 800-178 (comparison of XACML and NGAC), NIST AI 800-4 (CAISI, post-deployment monitoring), the NIST Cybersecurity Framework and NCCoE research on the security of AI agents.

Regulations and standards

Online entry

NIST AI 800-4

NIST AI 800-4 - Challenges to the Monitoring of Deployed AI Systems

A NIST report prepared by the Center for AI Standards and Innovation (CAISI), published in March 2026 (NIST announcement of 9.03.2026), analysing the barriers to monitoring AI systems after deployment. It defines six monitoring categories: Functionality, Operational, Human Factors, Security, Compliance, Large-Scale Impacts. The document does not set out normative requirements; CDF adopts its category taxonomy as the basis for artefact A-MON-01. Source class: N.

Regulations and standards

See also: NIST

Online entry

Non-repudiation

Non-repudiation

A property of a system guaranteeing that no participant (human or agent) can deny having performed or commissioned an operation. In CDF, required in Phase 6 (artefact A-F6-05 Immutable Audit Trail Specification, tag AGENT+REGULATED), an extension of the NIST NCCoE pillars. Implemented through cryptographically signed entries in the Immutable Audit Trail (agent key linked to the Agent Identity Schema), tamper-proof storage, Human Authorization Binding and external verifiability.

Sovereignty and architecture

Online entry

North Star

North Star / Strategic Goal

The overarching strategic goal of an AI project: one measurable business outcome + ≤5 KPIs + 90-day milestones + an investment envelope. It prevents fragmentation of the portfolio of AI initiatives. It serves as the evaluation framework for the Scale-or-Kill Gate. Delta vs. the North Star Metric (Ellis 2017): the dimension is enterprise transformation, not product growth.

Deployment and governance

Online entry

Notified Body (SSI)

Notified Body

A conformity assessment body notified under Chapter III, Section 4 of the AI Act; in Poland the notifying authority is the minister responsible for digital affairs (Articles 86-90 of the Act on Artificial Intelligence Systems), supported by the Polish Centre for Accreditation. Phase F1 (conformity assessment of high-risk systems).

Regulations and standards

AI Act · Act on AI Systems

See also: AI Act

Online entry

Notifying Authority (SSI)

Notifying Authority

The minister responsible for digital affairs - the authority notifying AI conformity assessment bodies (Article 86 of the Act on Artificial Intelligence Systems); the PCA co-develops the accreditation programme and informs the minister within 14 days of significant accreditation decisions.

Regulations and standards

AI Act

See also: AI Act

Online entry

Nudifier Application

Nudifier Application

An AI application generating nude images without the consent of the person depicted. Covered by the prohibition added to Article 5(1) of the EU AI Act by Regulation (EU) 2026/1744 as point (ba) (systems generating or manipulating realistic intimate images of an identifiable natural person without their consent) and point (bb) (child sexual abuse material within the meaning of Directive 2011/93/EU); for systems not intended for such purposes, adequate technical safeguards against misuse are required. The transitional period expires on 2 December 2026. In CDF, taken into account in the fines and sanctions matrix (SSI-7) and in the F2 prohibited practices module.

AI fundamentals

Online entry

OC

Civil Liability (Odpowiedzialność Cywilna)

Civil liability insurance. In the CDF context, it concerns policies covering damage related to the deployment of an AI system.

Regulations and standards

Online entry

On-premises / On-prem

On-premises Deployment

A deployment model in which the AI infrastructure runs at the physical location of the client or organisation, without dependence on the public cloud as the foundational layer.

Sovereignty and architecture

Online entry

Where we cover this: Bielik and PLLuM

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment

Ontology Change Control

Ontology Change Control

A rigorous procedure for managing changes to the knowledge graph ontology, covering versioning and approval of changes. Performed by the Knowledge Curator in CDF Phase 6, it ensures the consistency and integrity of the AI system's knowledge base.

CDF methodology

See also: Knowledge Curator

Online entry

OpEx

Operational Expenditure

Ongoing operational expenditure on maintaining and operating the AI system (energy, licences, support, retraining). In CDF, included in the 3-5 year TCO Model designed in Phase 1.

Deployment and governance

See also: CapEx

Online entry

Orchestration

Orchestration

The process of coordinating and managing the flow of tasks between multiple AI agents, systems or components in order to carry out a complex business process. In CDF, every orchestration is logged in the Immutable Audit Trail.

AI fundamentals

Online entry

Overfitting

przeuczenie

A situation in which a model has memorised its training data instead of learning general patterns from it. It shines on familiar examples and fails on new ones. That is why a model is tested on data it did not see in training, and the quality of its answers is measured continuously after deployment

AI fundamentals

See also: Training data, Fine-tuning, Drift (Model Drift)

Online entry

OWASP

Open Web Application Security Project

An international non-profit organisation publishing application security standards and threat lists. In CDF, the primary reference point for agent security is the OWASP Top 10 for Agentic Applications 2026 (ASI01-ASI10, full coverage in Annex B), complemented by the OWASP Top 10 for LLM Applications 2026 (the layer of LLM-based applications; the 2025 edition remains a historical reference).

Regulations and standards

Online entry

OWASP ASI Mapping Matrix

OWASP Agentic Security Initiative Mapping Matrix

A table mapping the 10 risks of the OWASP Top 10 for Agentic Applications 2026 (ASI01 Agent Goal Hijack, ASI02 Tool Misuse, ASI03 Identity & Privilege Abuse, ASI04 Agentic Supply Chain Vulnerabilities, ASI05 Unexpected Code Execution, ASI06 Memory & Context Poisoning, ASI07 Insecure Inter-Agent Communication, ASI08 Cascading Failures, ASI09 Human-Agent Trust Exploitation, ASI10 Rogue Agents) onto CDF controls, artefacts and phases. See Annex B, Table 58 (in Table 58 the name of ASI10 requires correction to Rogue Agents).

CDF methodology

See also: OWASP

Online entry

PAG

Public Administration Guardrails

A family of three CDF controls for public administration, introduced in 1.6.0 and gated by the GOV tag; the national module is activated by the GEO:PL tag. It comprises PAG-1 Necessity Gate, PAG-2 Human-Contact Fallback and PAG-3 Approved Tooling Register. All of the controls are blocking: non-fulfilment halts the passage of the phase gate. PAG is a control family, not a configuration tag.

CDF methodology

See also: PAG-1, PAG-2, PAG-3

Online entry

PAG-1

Necessity Gate

A CDF control (KD1, KD8; phase F0) of the PAG family. A gate assessing the justification for the use of AI, based on Stage 0 of the MC Guide to AI. Three-valued output: GO - justification accepted; NO-GO - the objective is achievable by simpler means, project closed in F0; REDESIGN - the scope requires redesign. The NO-GO variant is an equally valid outcome of phase F0. Artefact A-GOV-01. In profiles other than GOV the control is recommended, not mandatory.

CDF methodology

See also: A-GOV-01

Online entry

PAG-2

Human-Contact Fallback

A CDF control (KD9, KD7; phases F2 and F4) of the PAG family. Every process in which AI interacts with a citizen must provide an alternative service channel leading to a member of staff: a switch-to-human function at every point of interaction, a channel independent of the AI system maintained during declared hours, and a path for raising objections, separate from the F6 AI concerns reporting channel. The absence of a fallback path blocks the F4 exit gate. Artefact A-F2-16.

CDF methodology

See also: A-F2-16

Online entry

PAG-3

Approved Tooling Register

A CDF control (KD6, KD1; phases F2 and F6) of the PAG family. A register of AI tools approved for official use, together with an AI use policy. It differs from Shadow Agent Governance: SAG-4 detects unauthorised agents within the system architecture, whereas PAG-3 covers GenAI tools used by staff outside the deployment architecture. Both controls feed a joint review in F6. Artefacts A-GOV-02 and A-GOV-03.

CDF methodology

See also: SAG (Shadow Agent Governance), Shadow Agent Governance, A-GOV-02, A-GOV-03

Online entry

PageIndex

document structure index

An index that maps the structure of a long document as a tree: chapters, sections and fragments. Search follows this structure rather than only fragment similarity, so the model reaches the right chapter and can show where the answer comes from. Useful for manuals, standards, contracts and legal acts

AI fundamentals

See also: RAG, Agentic RAG, LLM

Online entry

Where we cover this: SAIE Pantera

PCOC (Joint Cybersecurity Operations Centre)

Joint Cybersecurity Operations Centre (Połączone Centrum Operacyjne Cyberbezpieczeństwa)

A format for the coordination and ongoing management of cybersecurity at national level, organised by the Ministry of Digital Affairs in cooperation with the Government Centre for Security (RCB) and provided for in the Cybersecurity Strategy of the Republic of Poland 2025-2029 as one of the lines of intervention (expansion of the acronym according to the Report of the Government Plenipotentiary for Cybersecurity). In phase F2/F3, CDF requires identification of the sectoral CSIRT and an incident reporting procedure consistent with the PCOC coordination model.

Regulations and standards

Online entry

Phase Gate

Phase Gate

A formal checkpoint at the transition between CDF phases (F0→F1→F1.5→F2→F3→F4→F5→F6). Each gate defines: Entry Criteria, required artefacts and exit criteria (Definition of Done). Passage requires approval by the Accountable person from the RACI matrix. Source: the Methodology, section "CDF Phase Entry and Exit Criteria". Introduced in v1.4.4.

Deployment and governance

See also: RACI

Online entry

Phase Rollback

Phase Rollback

A mechanism for returning to the previous CDF phase where the exit criteria (DoD) of the current phase are not met. A Phase Rollback requires a formal decision by the Accountable person and documentation of the reasons for the rollback. Source: the Methodology, section "CDF Phase Entry and Exit Criteria". Introduced in v1.4.4.

CDF methodology

Online entry

PKG

Personal Knowledge Graph

An employee's personal knowledge graph - a structured representation of the relationships between the concepts, documents, processes and contexts with which a given employee operates. A component of the Cognitive Digital Twin (CBP) architecture, alongside the Personal Language Model (PLM) and the Interpretive Profile (PI).

CDF methodology

See also: PLM, PLM (Personal Language Model)

Online entry

PLD (Directive 2024/2853)

Product Liability Directive

Directive (EU) 2024/2853 of the European Parliament and of the Council on liability for defective products, repealing Directive 85/374/EEC. It covers software and AI systems as products, introducing no-fault liability, an obligation to disclose evidence (Article 9) and presumptions of defectiveness and of causal link (Article 10). Transposition into Polish law by 9 December 2026. In CDF, addressed through the LER mechanism (artefact A-PLD-01).

Regulations and standards

PLD 2024/2853

Online entry

PLLuM

PLLuM

A family of Polish language models by the HIVE AI consortium led by NASK and funded by the Ministry of Digital Affairs; trained on official and legal texts (Monitor Polski, Journal of Laws, parliamentary transcripts). Sizes from 4 to 70 billion parameters, licence depending on the variant (Apache 2.0, Llama 3.3 or CC BY-NC). Since 31.12.2025 it powers the assistant in the mObywatel app

AI fundamentals

See also: Bielik, LLM, NASK, NASK 2026 Study, Quantisation

Online entry

Where we cover this: Bielik and PLLuM

PLM

Personal Language Model

Abbreviation of Personal Language Model. See PLM (Personal Language Model).

CDF methodology

See also: PLM (Personal Language Model)

Online entry

PLM (Personal Language Model)

Personal Language Model

An individually tuned language model forming a component of the CBP (Cognitive Digital Twin), alongside the Personal Knowledge Graph (PKG) and the Interpretive Profile (PI). The PLM is calibrated on the communication style, terminology and reasoning patterns of a specific employee. It requires a DPIA (Article 35 GDPR) owing to the processing of personal data. The PLM is calibrated exclusively on data related to the professional role - private data and special categories of data (Article 9 GDPR) are excluded. Introduced in CDF 1.4.4; described in section "K12: Cognitive Digital Twin (CBP)" of the Methodology. See PLM.

AI fundamentals

GDPR

See also: DPIA (Data Protection Impact Assessment), RODO

Online entry

Post-Deployment Monitoring

Post-Deployment Monitoring

The process of continuously monitoring an AI system after production launch, covering the 6 categories defined in NIST AI 800-4: functionality, operational performance, human factors, security, regulatory compliance and large-scale impacts. In CDF, carried out in phases F5 (Scaling) and F6 (CogOps) through cognitive oversight mechanisms.

Deployment and governance

AI Act

See also: NIST AI 800-4, AI Act, NIST

Online entry

Post-Quantum Cryptography

Cryptography resistant to quantum attacks

Cryptographic algorithms resistant to attacks using quantum computers. The Cybersecurity Strategy of the Republic of Poland 2025-2029 requires a cryptographic migration plan. In the Security Baseline (K8, F3/F4), CDF includes an assessment of the cryptographic readiness of AI systems.

Sovereignty and architecture

See also: NIST

Online entry

PRODUCTION (ACE tag)

ACE Configuration Tag

An ACE tag activated for production deployments or transformations. It enables the full phases F0-F4 (or F0-F5 with SCALE) and F6-Lite. It does NOT activate compliance requirements - only the full deployment flow.

CDF methodology

See also: F6-Lite, SCALE (ACE tag)

Online entry

Production Cost Model

Production Cost Model

A component of the Scale Path Definition setting out the full cost of moving from a pilot to a production environment. The CDF 380% heuristic: production costs amount on average to 380% of pilot costs, broken down into 5 components: Infrastructure 2.0×, Compliance 3.5×, CogOps Staffing 4.0×, KG Population 2.5×, Security Hardening 3.0×. It covers infrastructure, integrations, governance, maintenance, support and compliance.

Deployment and governance

Online entry

Prompt

Instruction / Query to AI

Input text passed to an LLM or AI agent in order to perform a task, obtain a response or trigger a procedure.

AI fundamentals

Online entry

Prompt Injection

Prompt Injection

An attack manipulating the input of an AI system (direct or indirect, through malicious instructions in data or in content from tools and sources); in the OWASP Top 10 for Agentic Applications 2026 covered by item ASI01 Agent Goal Hijack. In CDF, mitigation is an architectural requirement of the Cognitive Gateway (an input/output validation layer with logging of attack attempts, mandatory for LOA ≥ L2), addressed in the K8 Security Baseline, by control MCP-CTL-04 (MCP Input Validation) and by SAG-1 (Memory Poisoning Detection).

AI fundamentals

See also: OWASP, Jailbreak, AI gateway

Online entry

Where we cover this: AI use policy - template

Prompt Origin

Prompt Origin

Metadata on the source of a prompt: direct (user), template, agent, trigger. An element of Cognitive Observability in F6.

CDF methodology

See also: Cognitive Observability

Online entry

Proportionality (DORA)

Principle of Proportionality (DORA)

The principle of applying DORA requirements in proportion to the size, risk profile and the nature, scale and complexity of the financial entity's activities (Article 4). Microenterprises benefit from relief under Article 4; the simplified ICT risk management framework (Article 16) applies to specified categories of small entities, including small and non-interconnected investment firms and small payment institutions. In CDF, mapped to F1.5 - Simplified ICT Framework.

Regulations and standards

DORA

See also: DORA

Online entry

Protection of Classified Information (OIN)

Classification and Protection of Classified Information

Requirements arising from the Act of 5 August 2010 on the Protection of Classified Information, concerning classification levels (restricted / confidential / secret / top secret), personnel security clearances, accreditation of ICT systems and the conditions of processing. In CDF, mapped to F0 - GOV Deployment Prerequisites (classification document, ABW/SKW vetting).

Regulations and standards

Online entry

Pseudonymisation

Pseudonymisation of personal data

Processing personal data in such a way that it can no longer be attributed to a specific person without additional information, which is kept separately and protected (Art. 4(5) GDPR). Pseudonymised data is still personal data, unlike anonymised data. In work with AI this means, for example, replacing a name with the label [Applicant] before a document reaches the model, or masking the PESEL number on the AI gateway

Regulations and standards

GDPR Art. 4(5), Art. 25

See also: GDPR, AI gateway

Online entry

Psychological Readiness

Psychological Readiness

A dimension of organisational maturity assessed in Phase 0, relating to employee attitudes, the level of acceptance of change, resilience to cognitive stress and readiness to collaborate with AI.

Deployment and governance

Online entry

Psychological Safety Baseline Report

Psychological Safety Baseline Report

A Phase 3 artefact documenting the initial level of psychological safety of teams before the introduction of broad human-AI collaboration.

CDF methodology

Online entry

Psychological Safety Protocol

Psychological Safety Protocol

A set of measures implemented in Phase 3, comprising measurement of team psychological safety, countering the stigmatisation of AI users, change management interventions and monitoring of the entrenchment of suboptimal AI usage practices.

CDF methodology

Online entry

Quality Management System

AI Quality Management System

A system required by Article 17 of the AI Act for providers of high-risk AI systems. It comprises: a regulatory compliance strategy, design and development procedures, testing and validation procedures, data management, risk management and a post-market monitoring system. In CDF, mapped to F5 - AIMS Evidence Package and Quality Gate (item 11 of Matrix E.1). The supporting standard is EN 18286:2026 (item QMS-1 of Matrix E.1, without presumption of conformity).

Regulations and standards

AI Act · ISO/IEC 42001

See also: ISO/IEC 42001, AI Act

Online entry

Quantisation

Quantisation

Reducing the numeric precision of a model's weights (e.g. from 16 to 8 or 4 bits), so the model takes several times less GPU memory and runs faster at a small cost in quality. It decides whether an 11B model fits on a 24 GB card and a 70B model on a multi-card server

AI fundamentals

See also: LLM, Inference, Bielik, PLLuM, Sovereign Compute

Online entry

Where we cover this: Bielik and PLLuM

RACI

Responsibility Assignment Matrix

A matrix defining roles in each CDF phase (Table 16 of the Methodology): R (Responsible - performs), A (Accountable - approves), C (Consulted), I (Informed). It covers 8 roles: Sponsor / CEO, CDF Lead / AI Architect, Compliance Lead, Security Officer (K8), Data Steward (K3), Business Owner, Operations / CogOps Team, Agent Governance Lead (K8). In REGULATED profiles the Compliance Lead is Accountable in phases F1.5, F2 and F5; the Sponsor retains a right of veto in F0, F1 and F5. Artefact owners in the Artefact Catalogue derive from this matrix. Introduced in v1.4.4.

Deployment and governance

Online entry

RAG

Retrieval-Augmented Generation

An architecture combining a generative model with an external knowledge base, so that responses can be grounded in current and controlled sources, which limits hallucinations.

AI fundamentals

See also: Agentic RAG, PageIndex, Context window

Online entry

Where we cover this: Bielik and PLLuM

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment

RBAC

Role-Based Access Control

An access control model based on organisational roles. In CDF, used as the baseline mechanism for managing AI agent permissions, supplemented by NGAC and attribute-based policies in multi-agent environments.

Sovereignty and architecture

See also: NGAC

Online entry

Reasoning Accuracy Rate

Reasoning Accuracy Rate

The percentage of responses or decisions consistent with ground truth or with the expected state of domain knowledge. One of the core Cognitive SLA metrics.

AI fundamentals

Online entry

Records of Processing Activities (ROPA)

Records of Processing Activities

Records maintained by the data controller in accordance with Article 30 GDPR, documenting the purposes of processing, categories of data, recipients, transfers to third countries and envisaged time limits for erasure. In CDF, implemented in F2 through the Data Governance Package.

Regulations and standards

GDPR

See also: RODO

Online entry

Recovery Rate

Recovery Rate

A metric of the Agent SLA layer (Table 56 of the Methodology, Annex A) measuring an agent's ability to restore correct operation on its own after the detection of an error or cognitive incident, without human intervention.

CDF methodology

Online entry

REDUCTION (flag)

Scope Reduction Flag

A flag in the ACE Profile Version Record signalling that a profile change was a Scope Reduction. It requires written justification and verification of the regulatory floor.

CDF methodology

See also: ACE Profile Version Record, Scope Reduction

Online entry

REGULATED (ACE tag)

ACE Configuration Tag

An ACE tag activated for a regulated sector or where the deployment processes personal or operational data. It enables the compliance and audit sections and compliance-first delivery (Phase 1.5). Activated by sector, data or location.

CDF methodology

Online entry

Regulation (EU) 2026/1744

Digital Omnibus on AI

Regulation amending the AI Act (2024/1689) and Regulations (EU) 2018/1139 and (EU) 2023/1230. Published in the Official Journal of the EU on 24.07.2026, in force from 27.07.2026. The source of the applicable AI Act application dates used in CDF. See Digital Omnibus (EU).

Regulations and standards

AI Act

See also: Digital Omnibus (EU), AI Act

Online entry

Release Quality Gate

Release Quality Checklist

An 11-point quality control checklist that every CDF version must pass before publication. It covers: references, numbering, and the consistency of phases, artefacts, the glossary, annexes, dates, claims, scales, formatting and the release triad. Owner: Delivery Lead. Approval: Sponsor. Source: the Methodology, section "CDF Release Quality Checklist". Introduced in v1.4.4.

CDF methodology

Online entry

Request routing

kierowanie zapytań

Automatic choice of where a request goes: to which model, tool or person. The choice follows the organisation’s rules, e.g. sensitive data only to a local model, simple questions to a cheaper model, and unusual cases to an employee. This way the organisation combines data protection with cost control

Sovereignty and architecture

See also: AI gateway, LLM, Token Budget Governance

Online entry

Retraining

Retraining of a model

Updating an AI model on new data in order to improve its performance, adapt it to changes in the domain or limit drift.

AI fundamentals

Online entry

Reusable Asset Register

Reusable Asset Register

A collection of components, patterns, agents, templates and artefacts that can be safely reused in subsequent AI deployments within the organisation. An element of CDF Phase 5.

CDF methodology

Online entry

Right to Erasure

Right to Erasure / Right to Be Forgotten

The right of the data subject to request the erasure of their personal data (Article 17 GDPR). In CDF, implemented in F2 and F6 through Data Lifecycle Management - the mechanism for managing data retention and deletion in AI systems.

Regulations and standards

GDPR

See also: RODO

Online entry

RODO

General Data Protection Regulation (Polish designation)

The Polish designation of the General Data Protection Regulation (GDPR, Regulation 2016/679). In CDF it constitutes a key regulatory requirement concerning the processing of personal data by AI systems, including profiling, automated decision-making and data transfers. See GDPR.

Regulations and standards

See also: GDPR

Online entry

ROI

Return on Investment

Return on investment - a financial indicator measuring the profitability of a project by setting the benefits obtained against the costs incurred.

Deployment and governance

Online entry

ROI Baseline Report

ROI Baseline Report

Phase 0 artefact establishing the starting point for measuring business benefits, which also takes account of the effect of the productivity J-curve.

CDF methodology

Online entry

Root Cause Analysis

Root cause analysis

Systematic investigation of the causes of an incident or cognitive error in order to eliminate the source of the problem rather than merely its symptoms. In CDF it is required under the Orange escalation procedure (72h) within the Cognitive SLA.

AI fundamentals

Online entry

S46 System

S46 ICT system

The ICT system of the National Cybersecurity System (Article 46 of the uKSC), operated by NASK, used for reporting incidents and exchanging threat information and warnings between essential and important entities and CSIRT teams. In the K4/K8 artefacts, CDF requires reporting procedures consistent with the S46 format and integration with the sectoral CSIRT.

Regulations and standards

NIS2/uKSC

See also: NASK

Online entry

SA-XAI

Situation Awareness Explainable AI

CDF's proprietary approach to AI explainability, mapping system decisions onto the three levels of situation awareness in Endsley's model: perception, comprehension and projection (prediction of the future state). Applied in Phase 2 as an element of AI transparency measures, providing operators with the proper context for oversight.

Deployment and governance

Online entry

SAG (Shadow Agent Governance)

SAG control family - agent security (Shadow Agent Governance section)

Acronym of a family of five CDF controls (Control Catalogue, AGENT tag, introduced in 1.5.0) addressing threats specific to multi-agent systems: SAG-1 Memory Poisoning Detection, SAG-2 Cross-Session Hijacking Prevention, SAG-3 Confused Deputy Mitigation, SAG-4 Shadow Agent Detection Protocol, SAG-5 Agent Identity Audit. The controls apply from LOA ≥ L2. See Shadow Agent Governance.

CDF methodology

See also: Shadow Agent Governance

Online entry

SAVANT

SAVANT (product proper name)

SAVANT is the proper name of a product of allclouds.pl - a sovereign, enterprise-class cognitive system. It requires no acronym definition. Product page: www.savant-ai.app.

CDF methodology

Online entry

SBOM (Software Bill of Materials)

Software Bill of Materials

A formal inventory of all software components (libraries, AI models, APIs, frameworks) making up a digital product. Required by the CRA (Cyber Resilience Act) as a precondition for vulnerability monitoring. In CDF it is delivered through the Vendor AI Registry artefact (K2/K8), covering LLM models, embedding models, vector databases and other cognitive components. It enables tracing of the AI supply chain and a rapid response to CVEs affecting components.

Regulations and standards

CRA

See also: CRA (Cyber Resilience Act)

Online entry

SCALE (ACE tag)

ACE configuration tag

ACE tag activated for enterprise organisations (5000+ employees), transformations or multi-agent deployments. It enables the scaling, industrialisation, CBP, CogOps-Full and F6-Full sections.

CDF methodology

See also: F6-Full

Online entry

Scale Path Definition

Scale path definition

A mandatory CDF Phase 0 artefact specifying the pilot's exit criteria, the path to production deployment, the Production Cost Model and the kill/pivot criteria. Its purpose is to prevent the organisation from becoming stuck at the pilot stage.

CDF methodology

See also: Production Cost Model

Online entry

Scale-or-Kill Gate

Scale-or-Kill decision gate

A mandatory binary decision point at the end of an AI pilot, deliberately eliminating the “extend pilot” option. Two outcomes: Scale (transition to production) or Kill (termination). Kill = a positive result: avoidance of a costly production investment (the 380% heuristic). An original CDF concept [CDF-ORIGINAL]. To be distinguished from the Kill/Pivot Criteria (an element of the Scale Path Definition).

Deployment and governance

Online entry

SCIM

System for Cross-domain Identity Management

An open standard (RFC 7643/7644) automating the management of user and AI agent identities across systems. In CDF it is applied as a recommendation for the provisioning and deprovisioning of agents in the Agent Registry, ensuring identity consistency in a multi-agent environment.

Sovereignty and architecture

Online entry

Scope Reduction

Reduction of configuration scope

An ACE scenario in which the organisation deliberately limits the ambition of its deployment (for example, abandoning a transformation in favour of a pilot). It is subject to three requirements: a written justification, verification of the regulatory floor (REQUIRED requirements may not be disabled) and the REDUCTION flag in the version record.

Deployment and governance

Online entry

Security by Default

Security by default

A design principle under which secure settings, policies and restrictions are active by default rather than only after manual configuration.

Sovereignty and architecture

Online entry

Security by Design

Security by design

The principle of building security measures into an AI system from the very start of the project rather than only after deployment.

Sovereignty and architecture

CRA

See also: CRA (Cyber Resilience Act)

Online entry

Settlement with the Commission

Settlement with the Commission (administrative settlement)

The procedure governing the conditions for extraordinary mitigation of sanctions conducted by the Commission (Articles 70-85). A settlement may result in a reduction of 20-70%, and under the Article 84 procedure of 30-90%, subject to cooperation, remedying the harm and implementing corrective measures.

Regulations and standards

Online entry

Shadow Agent Governance

Governance of unauthorised agents

Section of Annex B defining the SAG control family (SAG-1 to SAG-5) for multi-agent systems, applicable from LOA ≥ L2: SAG-1 Memory Poisoning Detection (validation of agent memory integrity, hash checkpoint, rollback; F2/F6), SAG-2 Cross-Session Hijacking Prevention (isolation of session contexts per agent, token with TTL; F2/F6), SAG-3 Confused Deputy Mitigation (least privilege and explicit scope in the delegation token; F2), SAG-4 Shadow Agent Detection Protocol (inventory of agents against the Agent Registry, endpoint scanning, traffic monitoring, quarterly audit; F4/F6), SAG-5 Agent Identity Audit (periodic audit of agent identities and permissions; F6). It differs from PAG-3: SAG-4 detects unauthorised agents within the system architecture, whereas PAG-3 covers GenAI tools used by employees outside the deployment architecture. See Annex B in the Methodology.

AI fundamentals

See also: Shadow AI

Online entry

Shadow AI

Unauthorised use of AI

The phenomenon of unauthorised, unmanaged use of AI tools by the organisation's employees, outside the control of IT and governance. In CDF it is addressed as a risk in Phase 0 (diagnostics) and mitigated through the AI Champions Program, the CDF Academy and governance policies.

AI fundamentals

Online entry

Where we cover this: Shadow AI

Where we cover this: Act on AI systems - what you need to demonstrate

Where we cover this: AI use policy - template

SIEM

Security Information and Event Management

A security information and event management system aggregating logs and alerts from multiple sources in order to detect threats and incidents. In CDF it is integrated with the Immutable Audit Trail layer and with the monitoring of AI agents.

Sovereignty and architecture

Online entry

Single Agent

Single AI agent

An AI agent responsible for one discrete task, for example document classification, data extraction or the preparation of a recommendation.

AI fundamentals

See also: Agent (AI)

Online entry

Skill Partnership

Competence partnership

A collaboration model set out in matrix form in Phase 3, in which a human and an AI agent complement each other's competences and form a more effective working arrangement.

Deployment and governance

Online entry

SLA

Service Level Agreement

A service level agreement defining guaranteed operating parameters, such as availability, response time or quality of service.

Sovereignty and architecture

Online entry

SLA-S

Sovereignty Level Assessment

Abbreviation used for the sovereignty level assessment carried out in Phase 0, which serves to assign the appropriate AI deployment pattern to a given business area.

CDF methodology

Online entry

SoA

Statement of Applicability

Statement of applicability - a document specifying which controls and requirements of the standard (in CDF: the 38 controls of ISO/IEC 42001 Annex A) are included or excluded in the context of a specific deployment, together with the justification, the owner and the related artefacts. In CDF it is a Phase F1.5 artefact (A-F15-02, REGULATED tag), required for AIMS certification. See Statement of Applicability.

Regulations and standards

ISO/IEC 42001

See also: ISO/IEC 42001

Online entry

SOKiK (AI jurisdiction)

Court of Competition and Consumer Protection (Sąd Ochrony Konkurencji i Konsumentów)

The Regional Court in Warsaw - Court of Competition and Consumer Protection (SOKiK), competent to hear appeals against decisions and complaints against orders of the Commission (new Division IVfa of the Code of Civil Procedure, “Proceedings in matters concerning artificial intelligence”, Article 115 of the Act). Court fees: PLN 1000 (appeal, appeal on the merits, cassation appeal), PLN 500 (complaint) - Article 120.

Regulations and standards

Online entry

SOVEREIGN (ACE tag)

ACE configuration tag

ACE tag activated for deployments involving classified information or critical infrastructure. It enables the full sovereignty sections: air-gap, EuroHPC, Hardware Binding and the ASIA sovereignty module (sections 11-20). It automatically enforces REGULATED + GOV + CLASSIFIED (guardrail CV-03) and activates Cognitive SLA Tier 3 (CV-06).

CDF methodology

See also: REGULATED (ACE tag)

Online entry

Sovereign AI

Sovereign AI

A model of AI deployment and operation in which the organisation retains a high degree of, or full, control over the data, the model, the logs, the integrations and the operational layer.

Sovereignty and architecture

Online entry

Sovereign AI Rationale

Rationale for a sovereign AI architecture

Justification of the strategic, regulatory and operational grounds for choosing a sovereign AI architecture, prepared in phase F0 as an element of the Sovereignty Level Assessment (input to A-F0-04 SLA-S Report and A-F1-04 Sovereignty Architecture Decision Record). It covers: analysis of geopolitical risks, data residency requirements, compliance with the EU AI Act and NIS2/uKSC, assessment of the Dual-Orbit Sovereignty Matrix and justification of the sovereignty level (MSS). The NASK 2026 baseline (75% of responses pointing to national public institutions) constitutes an input to the rationale in the GOV profile. Required for the GOV, SOVEREIGN and DEFENSE profiles. It has no separate entry in the CDF Artefact Catalogue.

CDF methodology

See also: Dual-Orbit Sovereignty Matrix, NIS2/uKSC, SOVEREIGN (ACE tag), DEFENSE (ACE tag), AI Act

Online entry

Sovereign Compute

Sovereign computing resources

Computing infrastructure assessed in terms of the legal and operational control of the organisation or the state. CDF defines four levels of compute sovereignty (the CDF Scales and Taxonomies block; Annex F, section 2.6, Table 81): S1 Sovereign (infrastructure, management and data in the EU, e.g. EuroHPC AI Factories), S2 EU-compliant (hyperscaler with an EU region, contract governed by EU law), S3 Non-EU (infrastructure outside the EU, jurisdictional risk), S4 Self-Hosted (open-weight model on-premises with no external dependencies). The scale is distinct from the AI sovereignty levels (Level 1-3). CSE-GOV requires a minimum of S1 or S2; choosing S3 for regulated data requires justification in the Compliance Readiness Report.

Sovereignty and architecture

Online entry

Sovereign Deployment Pattern

Sovereign deployment pattern

The final choice of the operating model for AI infrastructure, made in CDF Phase 1 on the basis of the Data Gravity Assessment and the Sovereignty Level Assessment, from among three options: Fully On-Premises (full sovereignty), Hybrid Sovereign-Cloud (critical data kept locally, computation in the cloud) and Air-Gapped Defense (physical network isolation for the defence sector).

CDF methodology

See also: SLA-S, Sovereignty Level Assessment (SLA-S), Data Gravity Assessment, Hybrid Sovereign-Cloud, Air-Gapped Defense

Online entry

Sovereignty Dimensions

Sovereignty dimensions

Four criteria for assessing the required level of AI sovereignty: data classification, regulatory exposure, operational criticality and supply chain dependency.

Sovereignty and architecture

Online entry

Sovereignty Level Assessment (SLA-S)

Sovereignty level assessment

A Phase 0 tool examining a given business area across four dimensions in order to assign it to the appropriate level and AI deployment pattern. It protects the organisation against over-sizing or under-estimating the level of isolation and control.

CDF methodology

Online entry

SPIFFE/SPIRE

Secure Production Identity Framework / SPIFFE Runtime Environment

A CNCF standard (Secure Production Identity Framework for Everyone) and its reference implementation (SPIRE) for managing workload identity in distributed environments. In CDF it is applied as a recommendation for identifying AI agents in the Agent Identity Schema, providing cryptographically verifiable identities without reliance on shared secrets.

Sovereignty and architecture

Online entry

Standard Status

Standard Status

Designation of the state of an item in the CDF source canon. In the Compliance Timeline Tracker (Table 20) and in the note to Matrix E.4 the following values are used: Published (published and in force), Draft (draft under consultation), Pending (awaiting adoption or publication), None / draft. The Status column of Matrix E.1, by contrast, expresses the status of CDF's coverage of a requirement: ALIGNED, PARTIAL, GAP and RESERVED (mapping reserved until the standard is published). From 1.6.0 the force of a source is additionally determined by the Class column (W, M, N, D - see CDF Source Taxonomy).

CDF methodology

Online entry

Statement of Applicability

Statement of Applicability (SoA)

See SoA. A Phase F1.5 document (artefact A-F15-02) mapping the 38 controls of ISO/IEC 42001 Annex A onto CDF phases, artefacts and mechanisms, with a decision to include or exclude each control, a justification, an owner and a coverage status (ALIGNED / PARTIAL). Generated on the basis of the ACE profile; a living document - updated at every change of scope and at least once a year as part of the F6 review. See Table 8 in the Methodology.

Regulations and standards

See also: SoA

Online entry

Substantial Modification

Substantial Modification

A significant change to an AI system (fine-tuning, continuous learning, a substantial update) after it has been placed on the market, which may shift the deployer into the role of manufacturer within the meaning of Article 8(2) of the PLD Directive 2024/2853, with the assumption of liability. Tracked in the register of substantial modifications (control LER-2). Introduced in CDF 1.5.0.

Regulations and standards

AI Act · PLD 2024/2853

See also: AI Act

Online entry

Superteam

Human-AI superteam

CDF term describing a highly effective team in which an AI agent augments the employee's capabilities while the human provides judgement, accountability and context.

Deployment and governance

Online entry

System Availability

System Availability

Cognitive SLA metric (Table 14 of the Methodology): availability of the AI system's underlying platform. Target: ≥ 99.9%. The only infrastructure metric in Tier 1 (alongside three reasoning quality metrics). See Uptime.

Sovereignty and architecture

See also: Uptime

Online entry

Tacit Knowledge

Tacit Knowledge

Knowledge that an employee possesses but which is not documented in the organisation's formal systems - held in their head, on a local drive, in private notes and in informal interpretations. The CBP aims to capture and formalise tacit knowledge.

AI fundamentals

Online entry

Tacit Opinion (SSI)

Tacit Individual Opinion

The effect provided for in Article 12(3) of the Act on Artificial Intelligence Systems: failure to issue an individual opinion within the 30 or 60 day time limit is deemed the issue of an opinion consistent with the position presented in the application, favourable to the applicant.

Regulations and standards

Online entry

TCO

Total Cost of Ownership

The total cost of owning a solution, covering not only purchase or build but also integration, maintenance, energy, personnel, compliance and the cost of switching provider.

Deployment and governance

Online entry

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment

Technologies-in-Practice Monitoring Plan

Technologies-in-Practice Monitoring Plan

A Phase 3 artefact for observing how employees actually use AI in practice and whether suboptimal, unsafe or non-compliant usage patterns are becoming entrenched.

CDF methodology

Online entry

Tenant

Tenant

A single organisation’s separated space in a provider’s cloud service: its own accounts, data and settings on shared infrastructure. Data is processed in the provider’s region and on its terms - the organisation administers, but does not choose the location or control metadata; the opposite of an on-premises environment

Sovereignty and architecture

RODO

See also: On-premises / On-prem, Hybrid Sovereign-Cloud, Vendor Lock-in, Data Gravity, Sovereignty Dimensions

Online entry

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment

TK Pending (flag)

Constitutional Tribunal Pending (CDF flag)

Designation of a regulatory item that is the subject of proceedings pending before the Constitutional Tribunal. The flag denotes legal risk arising from the pending proceedings, not a suspension of the application of the provisions; under ex post review the act remains in force until any ruling of unconstitutionality. As at 12.09.2026: application of the President of the Republic of Poland of 19.02.2026 concerning the amendment to the uKSC; the case reference number has not been published. The Methodology does not give an anticipated case reference number.

CDF methodology

Online entry

Token

Unit of text

The basic unit of text processing by LLM models, corresponding to a fragment of a word, a whole word or a character, depending on the tokeniser.

AI fundamentals

Online entry

Token Budget Governance

Token budget governance

A mechanism for controlling the operating costs of AI agents through cost limits per agent per interaction (in units of LLM tokens). A mandatory element of Agent Governance from Phase 2, particularly critical for Autonomous Swarms (L2-L3).

Deployment and governance

Online entry

Training data

dane treningowe

The texts and examples a model learns from. Their quality decides the quality of the model: errors, gaps and bias in the data come back in the answers. For high-risk AI systems the AI Act requires governance of training, validation and testing data, and providers of general-purpose AI models publish a summary of the content used for training

AI fundamentals

AI Act (Art. 10, Art. 53(1)(d))

See also: Overfitting, Fine-tuning, Data Provenance Tracking, Generative AI

Online entry

Transparency Notice

Notice of an AI system

The obligation to inform users that they are interacting with an AI system (Article 50 of the AI Act). It applies to chatbots, deepfakes, emotion recognition systems and biometric categorisation systems. In CDF it is delivered in F2 through the SA-XAI Framework and the Transparency Notice - a mechanism for explicitly notifying users.

Regulations and standards

AI Act

See also: AI Act

Online entry

Where we cover this: Act on AI systems

Where we cover this: AI use policy - template

Turing test

imitation game

A test proposed by Alan Turing in 1950: a judge holds a written conversation with a human and a machine and has to tell which is which. In a 2025 study by Jones and Bergen, GPT-4.5, prompted to act human, was judged to be human in 73% of conversations. The TURING:AI game turns the roles around: it tests not the machine but the person who has to spot it

AI fundamentals

See also: LLM, Chatbot

Online entry

Where we cover this: TURING:AI game

Uptime

System availability

The percentage of time during which the system remains available and operates at the expected service level. See System Availability (Cognitive SLA metric).

Sovereignty and architecture

See also: System Availability

Online entry

US-EU AI Governance Divergence

US-EU AI Governance Divergence

Analysis of 8 areas of regulatory divergence between the EU and the US (Annex F, section 2.11). See Table 84 and the entry Governance Divergence Matrix.

Regulations and standards

See also: NIST

Online entry

Vendor Disruption Protocol (VDP)

Vendor disruption protocol

A five-step protocol for responding to loss of access to an AI vendor (blacklisting, sanctions, bankruptcy). It comprises: VDP-1 Multi-Vendor Fallback, VDP-2 Sovereign AI Continuity, VDP-3 Migration Runbook, VDP-4 Supply Chain Cascade Assessment, VDP-5 Prime Contractor Liability. Activated in F0, enforced in F2/F3.

Sovereignty and architecture

Online entry

Vendor Lock-in

Dependence on a vendor

A situation in which the organisation's ability to change its technology vendor is materially restricted owing to data formats, architecture, contractual terms or lack of control over code and integrations.

Sovereignty and architecture

Data Act

See also: Data Act (Reg. 2023/2854)

Online entry

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment

Vendor Risk Assessment

Vendor risk assessment

The process of assessing the risk associated with providers of AI models and components of cognitive infrastructure, formalised in CDF as the AI Model & Vendor Risk Assessment (artefact A-F15-07, Phase F1.5, REGULATED tag, introduced in 1.5.0). It covers the criteria in Table 12 of the Methodology: jurisdiction of the vendor and of the training data, compliance disclosure, vendor lock-in and migration, regulatory history, continuity of access. It feeds the SLA-S, the SoA, the Exit Strategy and the Risk Register.

Sovereignty and architecture

AI Act · DORA · NIS2/uKSC

See also: AI Act, DORA

Online entry

Vera Rubin NVL72

NVIDIA Vera Rubin NVL72

NVIDIA's next-generation computing platform (announced at GTC 2026, available H2 2026), the successor to the Blackwell architecture. NVL72 configuration: 72 Rubin GPUs + 36 Vera CPUs. In CDF it is included in the computing infrastructure benchmarks (Table 15 in the Methodology) as a reference for large-scale sovereign inference.

Sovereignty and architecture

Online entry

Voice cloning

klonowanie głosu

Recreating a specific person’s voice with an AI model from a short recording, for example a social media video. A dozen or so seconds of recording are enough to clone a voice. Fraudsters use the technique in “grandparent” and “bank employee” scams, which is why the Polish Police advise agreeing a family password

AI fundamentals

AI Act (Art. 50(4)), GDPR

See also: Deepfake, Voicebot

Online entry

Where we cover this: TURING:AI game

Voicebot

voice assistant on a helpline

A program that holds a spoken conversation: it recognises speech, works out what the caller needs and replies in a synthesised voice. Companies use voicebots on helplines, for example to take a claim or route the call to the right adviser. Since 2 August 2026 the caller must be informed that they are talking to AI

AI fundamentals

AI Act (Art. 50(1))

See also: Chatbot, Transparency Notice, Voice cloning

Online entry

Where we cover this: TURING:AI game

Vulnerability Disclosure

Vulnerability reporting and handling process

The obligation of the manufacturer of a product with digital elements to report actively exploited vulnerabilities and severe incidents (CRA Article 14: 24 h early warning, 72 h notification, 14 days final report; via the ENISA platform; applicable from 11.09.2026), together with the coordinated vulnerability disclosure process. In CDF it is mapped onto F5/F6 - the Incident Response Plan, CogOps Monitoring and the CogOps Dashboard (Annex D.2b).

Regulations and standards

CRA

See also: CRA (Cyber Resilience Act)

Online entry

Watermarking (AI)

AI Content Watermarking

The obligation to mark content generated by AI systems, arising from Article 50 of the EU AI Act. It comprises two-layer marking: digitally signed provenance metadata (machine-readable information) and an imperceptible watermark embedded during inference or post-processing. Deadlines: the Article 50 obligations apply from 02.08.2026; for systems generating synthetic content placed on the market before that date, machine-readable marking (Article 50(2)) is required from 02.12.2026 (Regulation (EU) 2026/1744). In CDF it is delivered in F4 through the Art. 50 AI-Generated Content Compliance Checklist (Annex B, Table 64) and the SA-XAI Framework; informed by the European Commission guidelines of 20.07.2026 and the Code of Practice of 10.06.2026 (class M).

AI fundamentals

AI Act

See also: AI Act

Online entry

Workflow Redesign Mandate

Process redesign mandate

A CDF principle (Phase 5) stating that every workflow must be redesigned before integration with an AI agent. AI is not layered onto inefficient legacy processes. It prevents the replication and automation of the flaws of existing processes.

Deployment and governance

Online entry

WORM log

WORM log

An event log written in “write once, read many” mode - an entry, once written, cannot be changed or deleted. In an AI environment it covers requests, responses, models used and access-policy decisions; it is evidence for inspections (AI Act Art. 26(6) - high-risk system logs for at least 6 months) and for ISO/IEC 27001 and 42001 audits

Sovereignty and architecture

AI Act · ISO/IEC 27001

See also: Immutable Audit Trail, Chain of Custody, Non-repudiation, Evidence Readiness, AI gateway

Online entry

Where we cover this: Act on AI systems

Where we cover this: Shadow AI

Where we cover this: Bielik and PLLuM

Where we cover this: ChatGPT Enterprise, Copilot or your own AI environment

XAI

Explainable AI

Explainable artificial intelligence - techniques and methods that make it possible to understand how a model reached a decision, on what basis and with what level of confidence.

AI fundamentals

AI Act

See also: AI Act

Online entry

Zero Trust

Zero trust architecture

A security model assuming that no user, device or agent is trusted by default, regardless of its location in the network. In CDF it is applied as a design principle for the security architecture of AI systems, in particular in multi-agent environments.

Sovereignty and architecture

Online entry