CHAPTER 6

Using All Four Frameworks Together

Sequencing, integration, and the decisions that save the most time and money

The question practitioners ask most frequently — and find answered least satisfactorily — is not about any individual framework. It is about all of them together: given that we need to address NIST AI RMF, ISO 42001, the EU AI Act, and the OECD Principles simultaneously, where do we start, how do we avoid duplication, and how do we sequence the work to get maximum value from minimum effort?

This chapter answers that question directly. It explains the layered architecture that makes the frameworks coherent rather than competing, provides the decision framework for choosing where to start based on your specific drivers, and walks through the NovaCred 12-month integrated roadmap — the sequencing and integration decisions that allowed NovaCred to achieve NIST AI RMF alignment, ISO 42001 certification, and EU AI Act compliance for CreditIQ within thirteen months, with deliberate work-sharing across programmes.

6.1 The Layered Architecture

The four frameworks are not alternatives or competitors. They occupy different layers of a governance architecture, each doing something the others cannot. Understanding the architecture is the prerequisite for any sensible sequencing decision.

SEE APP. G

Appendix G: Framework Comparison Master Table
A side-by-side reference table comparing all four frameworks across 14 dimensions: type, authority, certification, scope, evidence requirements, prescriptiveness, audit mechanism, and relationship to each other.

OECD AI PRINCIPLES	Ethical Foundation — Values, fairness, transparency, accountability, robustness
EU AI ACT	Legal Obligation — Binding requirements; high-risk AI obligations; enforcement
ISO/IEC 42001	Management System — Certifiable infrastructure; auditable evidence; continual improvement
NIST AI RMF	Risk Methodology — GOVERN · MAP · MEASURE · MANAGE; risk thinking and culture

Figure 6.1 — The four-layer AI governance architecture

Read from bottom to top, the architecture describes increasing specificity and legal force. NIST AI RMF at the base provides the risk thinking methodology — the

analytical discipline that identifies what needs to be governed and why. ISO 42001 in the next layer provides the management system infrastructure — the documented processes, controls, and evidence trails that make governance auditable. The EU AI Act adds the legal layer — the mandatory obligations that cannot be traded off or deferred. And the OECD Principles at the top provide the ethical reference point that the other three operationalise.

In practice, most organisations encounter the layers in reverse order. They discover the EU AI Act because a regulator or client makes it urgent. They build toward ISO 42001 because a certification requirement emerges from procurement. They adopt NIST AI RMF as the thinking methodology that makes both more tractable. And they come to the OECD Principles when they need to make governance decisions that the other frameworks do not clearly resolve.

> *The order in which frameworks become urgent is not the order in which they are most efficiently implemented. Starting with NIST AI RMF builds the foundation that makes ISO 42001 faster and EU AI Act compliance more coherent.*

6.2 The Duplication Traps — and How to Avoid Them

The most expensive mistake in multi-framework implementation is treating each framework as a separate programme with its own team, its own documentation, and its own processes. Organisations that do this discover that they are producing three versions of the same risk assessment, three versions of the same audit documentation, and three sets of remediation actions that address the same underlying gaps.

The duplication is avoidable because the frameworks share significant common ground. Understanding where they overlap — and designing shared processes to address the overlap once — is the primary source of implementation efficiency.

The AI Inventory: One Exercise, Four Frameworks

Every framework requires an understanding of what AI systems exist in the organisation. NIST AI RMF's MAP function begins here. ISO 42001's scope definition (Clause 4) requires it. EU AI Act compliance begins with the inventory and classification exercise. OECD Principles cannot be applied without knowing what systems they apply to.

An organisation that conducts four separate inventory exercises — one for each framework — is wasting three-quarters of the effort. The inventory should be conducted once, maintained as a living document, and used as the common input to all four frameworks. The format should be designed from the start to support all downstream uses: NIST AI RMF context mapping, ISO 42001 scope documentation, EU AI Act classification, and OECD Principles policy mapping.

Risk Assessment and Impact Assessment: Design for Dual Use

NIST AI RMF's MEASURE function produces a risk assessment. ISO 42001's Clause 8.4 requires an AI System Impact Assessment. The EU AI Act requires a risk

management system and, for deployers, a fundamental rights impact assessment. These are not the same document — but they draw on the same underlying analysis.

Organisations that design their risk and impact assessment process from the start to satisfy all three requirements simultaneously — rather than retrofitting additional sections later — save significant time. The key design principle is layered documentation: a core risk and impact analysis that is common across frameworks, with framework-specific sections appended for the specific artefact requirements of each.

Bias Testing: One Programme, Multiple Compliance Outputs

Bias testing is required by ISO 42001 Annex A.5, the EU AI Act Article 10 (data governance), and the OECD Principle 2 (human-centred values and fairness). The testing methodology, the test datasets, and the test results are the same regardless of which framework prompted them. Organisations should run one bias testing programme and produce outputs formatted for each framework's documentation requirements — not three separate testing programmes.

EFFICIENCY PRINCIPLE	For every activity that appears in multiple frameworks, ask: can we design this once and produce multiple framework-compatible outputs? The activities where this principle applies most powerfully: AI inventory, risk/impact assessment, bias testing, audit logging, human oversight design, and model documentation. A well-designed multi-framework implementation programme should reduce total effort by 30–40% compared to running each framework as a separate programme.

6.3 Framework Selection — Where to Start

The starting point depends on your organisation's specific drivers, existing infrastructure, and timeline constraints. There is no single correct sequencing — but there are better and worse starting points for different situations.

If your primary driver is…	OECD	NIST RMF	ISO 42001	EU AI Act
Regulatory compliance (EU/EEA operations or clients)	–	✓	✓	**MANDATORY**
Enterprise client certification requirement	–	Foundation	✓	Enables
Building AI risk culture and internal governance	Values base	✓	Formalises	–
Demonstrating ethics and trust to stakeholders	✓	✓	✓	Supports
UK/Singapore/UAE regulatory alignment	Base	✓	✓	Reference
Starting from zero — no existing governance	✓	**Start here**	Phase 2	Phase 3

If your primary driver is…	OECD	NIST RMF	ISO 42001	EU AI Act
Existing ISO 27001 — fastest path to AI cert	–	Parallel	**Start here**	Parallel
Enforcement deadline pressure (Aug 2026)	–	Foundation	Parallel	**Start here**

Figure 6.2 — Framework selection and sequencing matrix by primary driver

If You Have an Enforcement Deadline (August 2026)

If EU AI Act compliance is your most urgent driver — because you have high-risk AI systems serving EU clients and the enforcement deadline is approaching — start there. Commission your AI inventory and classification analysis immediately. Prioritise technical documentation and human oversight for your highest-risk systems, because these are the critical path items for conformity assessment.

Run NIST AI RMF in parallel as your risk methodology — it will structure the thinking that feeds into your EU AI Act risk management system. Begin ISO 42001 implementation in Month 3 or 4 of your programme, using the outputs from the EU AI Act work as input to the gap analysis baseline. Do not wait until you have achieved EU AI Act compliance before starting ISO 42001 — the frameworks are designed to be implemented in parallel, and the documentation overlap means parallel implementation is more efficient than sequential.

If You Have a Certification Requirement

If a client or procurement process has required ISO 42001 certification — or if your commercial strategy involves certification as a differentiator — start with NIST AI RMF to build the risk thinking foundation, then move to ISO 42001 implementation within the first month. Book your certification body engagement before your implementation begins.

EU AI Act compliance should run as a parallel track, not a sequential follow-on. Many of the artefacts you produce for ISO 42001 — the AI System Impact Assessment, the system documentation, the monitoring processes — directly support EU AI Act compliance. Designing them to meet both sets of requirements from the start avoids costly rework.

If You Are Starting from Zero

If your organisation has no existing AI governance infrastructure, start with the OECD Principles as your values foundation and NIST AI RMF as your risk methodology. These two frameworks can be implemented without external audit or certification, which means you can begin immediately and build momentum before engaging the formal certification process.

Use the first 60 to 90 days to build the AI inventory, establish governance structure, and conduct the initial risk assessment. Then use the outputs of that work as the baseline for your ISO 42001 gap analysis and EU AI Act classification exercise. Starting from zero does not mean starting slowly — it means starting with the foundations that make everything else more tractable.

6.4 The Integration Points — Where Frameworks Share the Most Ground

Beyond the duplication traps, there are specific integration points where the frameworks reinforce each other so strongly that addressing them once produces outsized returns across the whole governance programme.

Integration Point	Frameworks	Design Principle	Efficiency Gain
AI system inventory	All four	Single living inventory with fields designed for all framework uses	Eliminates 3 separate inventory exercises
Risk and impact assessment	NIST MAP/MEASURE + ISO 8.4 + EU AI Act Article 9	Layered document: core analysis + framework-specific appendices	Saves 40–60% of assessment effort
Bias testing programme	ISO A.5 + EU AI Act Art.10 + OECD P2	One programme, multiple formatted outputs	Eliminates duplicate test runs
Technical documentation	ISO A.8 + EU AI Act Annex IV	Single model documentation standard meeting both requirements	One document reviewed by two auditors
Human oversight design	NIST MANAGE + ISO A.10 + EU AI Act Art.14	One oversight mechanism, documented for all three frameworks	Avoids three separate design cycles
Audit logging	NIST MANAGE + ISO 9.1 + EU AI Act Art.12	Single logging architecture meeting all three standards	One implementation, three compliance outputs
Management review	ISO 9.3 + EU AI Act Art.17 + NIST GOVERN	AI risk as standing agenda item with framework-mapped reporting	One process satisfies three requirements

Figure 6.3 — Key integration points and efficiency gains across frameworks

APPENDIX F

OECD AI Principles Policy Mapping

Assess adoption level per principle and track the gap from policy endorsement to operational embedding

Referenced in: Chapter 5 (Section 5.6 — NovaCred Policy Mapping Exercise)

NOTE	Score adoption level 1 (policy endorsement only), 2 (operationalised — embedded in processes and decision checkpoints), or 3 (embedded — shapes how AI decisions are made across the organisation). The goal is Level 2 for all significant AI systems.

PART 1 — BLANK TEMPLATE

Principle	Level (1–3)	Gap: What Is Missing for Level 2	Action & Owner
P1 — Inclusive Growth & Sustainable Development			
P2 — Human-Centred Values & Fairness			
P3 — Transparency & Explainability			
P4 — Robustness, Security & Safety			
P5 — Accountability			

Appendix F — Blank OECD AI Principles Policy Mapping Template

PART 2 — NOVACRED COMPLETED EXAMPLE

Principle	Level M0	Gap Identified at M0	Action Taken (M2)
P1 — Inclusive Growth	1	*No disaggregated analysis of who benefits and who is disadvantaged by CreditIQ. No geographic approval rate analysis. Distributional impact completely unassessed.*	Commissioned disaggregated approval rate analysis. Found 7.3% disparate impact on South Asian nationality group. Incorporated into bias mitigation programme. Geographic approval rate dashboard established.
P2 — Human-Centred Values	1	*Fairness mentioned in AI ethics statement but no operational definition. No protected characteristic testing. No demographic performance metrics.*	Defined equalized odds and demographic parity as fairness metrics. Embedded in model validation checklist. Quarterly bias monitoring report established. Bias finding disclosed to AI risk committee.
P3 — Transparency	2	*System description documentation exists. No customer-facing explanation of adverse decisions. No plain-language model card for deployer transparency.*	Adverse action explanation module deployed. Plain-language explanation to declined applicants within 5 working days. Model card published on developer portal. Complies with EU AI Act Art.13.
P4 — Robustness & Safety	2	*Standard performance monitoring in place. No adversarial robustness testing. No drift detection threshold defined. Model drift could go undetected for months.*	Drift detection alerts set at 3% performance degradation. Adversarial robustness test suite added to model validation. Monthly performance review with drift status as standing agenda item.
P5 — Accountability	2	*AI Risk Owner appointed. Accountability for individual model decisions not documented at decision level. No audit trail linking specific decisions to model version and reviewer.*	Audit log implemented: each CreditIQ output linked to model version, input features, SHAP values, and reviewer identity. Override decisions recorded with rationale. Retention: 7 years.

Appendix F — NovaCred OECD AI Principles Policy Mapping (Month 0 → Month 2)

APPENDIX G

Framework Comparison Master Table

Side-by-side reference across all four frameworks for key governance dimensions

Referenced in: Chapter 6 (Section 6.1 — The Layered Architecture)

Dimension	NIST AI RMF	ISO/IEC 42001	EU AI Act	OECD AI Principles
Type	Voluntary framework	Certifiable standard	Binding regulation	Intergovernmental policy
Issued by	US NIST (Jan 2023)	ISO (Dec 2023)	EU legislature (Aug 2024)	OECD (2019, updated 2024)
Legally binding?	No	No (certification is voluntary)	YES — EU law, extraterritorial	No
Certification?	None	YES — third-party audit	Conformity assessment (self or third-party)	None
Geographic scope	US-centric, global adoption	International	EU + extraterritorial	40+ countries endorsed
Primary audience	Any org developing/using AI	Orgs needing formal AIMS	Providers and deployers in scope	Governments and AI actors
Core structure	GOVERN, MAP, MEASURE, MANAGE	10 clauses + 39 Annex A controls	4 risk tiers + 12 high-risk obligations	5 principles
Risk philosophy	Sociotechnical risk lens — trustworthiness, bias, explainability	Organisational risk management and control effectiveness	Proportionate regulation by risk tier — highest obligations for highest risk	Ethical values foundation — human-centred, accountable, transparent

Dimension	NIST AI RMF	ISO/IEC 42001	EU AI Act	OECD AI Principles
Prescriptiveness	Low — tells you what to think about, not what to implement	High — specifies documented evidence and auditable processes	Very high for high-risk — specific obligations and artefacts required	Low — principles-based, not rules-based
Evidence required?	No formal requirement	YES — documented policies, procedures, records, audit trails	YES — technical documentation, conformity assessment, registration	No formal requirement
Audit mechanism	None	Internal audit + external certification audit	Market surveillance by national authority	None
Update cadence	Playbook updated periodically	Standard review cycle (typically 5 years)	Delegated acts may update Annex III lists	Updated 2024; periodic review
Best used for	Building AI risk thinking and governance culture	Demonstrating AI governance to auditors, clients, regulators	Legal compliance — EU/EEA operations or clients	Policy foundation; sense-check for governance decisions
Relationship to others	Foundation risk methodology — feeds ISO 42001 and EU AI Act	Management system that operationalises NIST RMF and EU AI Act	Legal layer that mandates what OECD Principles recommend	Ethical base that NIST RMF, ISO 42001, and EU AI Act operationalise

Appendix G — Framework Comparison Master Table

APPENDIX H

Glossary of Key Terms

Definitions of the 35 most important terms across all four AI governance frameworks

Referenced in: All chapters

Term	Definition
AI Management System (AIMS)	The organisational system established under ISO 42001 for managing AI-related risks and impacts. Includes policies, processes, roles, controls, and continual improvement mechanisms.
AI Risk Management Framework (AI RMF)	The NIST framework for identifying, assessing, and managing AI risk, organised around four functions: GOVERN, MAP, MEASURE, MANAGE.
AI System Impact Assessment (ASIA)	The structured analysis required by ISO 42001 Clause 8.4, assessing the potential impacts of an AI system on individuals, groups, and society. Designed to also satisfy EU AI Act Article 11 / Annex IV requirements.
Annex III	The annex to the EU AI Act listing specific application areas in which AI systems are presumed to be High-Risk. Includes credit scoring, employment screening, and access to essential services.
Annex SL	The ISO meta-standard defining the common high-level structure for all management system standards (ISO 9001, ISO 27001, ISO 42001, etc.). Enables integrated implementation.
Bias Evaluation	The systematic assessment of whether an AI system produces differential outcomes across demographic groups (age, gender, nationality, etc.). Required by ISO 42001 Annex A.5 and EU AI Act Article 10.
CE Marking	The marking affixed to products (including AI systems) indicating conformity with EU requirements. Required for high-risk AI systems under the EU AI Act after a valid declaration of conformity has been issued.

Term	Definition
Certification Body (CB)	An accredited third-party organisation authorised to conduct ISO 42001 (and other management system) audits and issue certificates. Also called a notified body in the EU AI Act context.
Conformity Assessment	The process by which a provider demonstrates that a high-risk AI system meets EU AI Act requirements. May be self-assessed (for most systems) or third-party assessed (for certain biometric and critical infrastructure systems).
Continual Improvement	A core requirement of ISO 42001 and other management system standards — the ongoing process of reviewing and enhancing the AIMS based on audit findings, performance data, and corrective actions.
Corrective Action	A documented response to a non-conformity identified in an audit or incident — addressing the root cause and preventing recurrence. Required evidence for ISO 42001 Clause 10.
Declaration of Conformity	A formal document signed by the provider declaring that a high-risk AI system meets EU AI Act requirements. Required before market placement; must accompany EU database registration.
Deployer	Under the EU AI Act, any organisation or individual that uses a high-risk AI system in the course of a professional activity. Deployers have specific obligations including fundamental rights impact assessment and human oversight.
Demographic Parity	A fairness metric requiring that an AI system's positive outcome rate is equal across demographic groups. One of the fairness metrics implemented in NovaCred's bias evaluation.
Disparate Impact	A situation where an AI system produces significantly different outcomes for different demographic groups, even when those groups have equivalent underlying characteristics relevant to the decision.
Equalized Odds	A fairness metric requiring that an AI system has equal true positive and false positive rates across demographic groups. Complements demographic parity as a bias evaluation metric.
EU AI Act	Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial

Term	Definition
	intelligence. In force August 2024; high-risk obligations enforceable from August 2026.
Fundamental Rights Impact Assessment (FRIA)	An assessment required of deployers of high-risk AI systems under the EU AI Act (Article 26), evaluating the specific impact of the AI system in their deployment context on fundamental rights.
GOVERN (NIST AI RMF)	The first of the four NIST AI RMF functions. Covers the policies, roles, processes, and culture that enable AI risk management across the organisation.
High-Risk AI	Under the EU AI Act, AI systems listed in Annex III or embedded in products covered by Union harmonisation legislation. Subject to the full set of twelve high-risk AI obligations.
Human Oversight	Under the EU AI Act Article 14, the requirement that high-risk AI systems be designed to allow natural persons to effectively oversee and intervene in the system's operation. Must be effective in practice, not merely theoretical.
Internal Audit	A systematic, documented review of whether the AI Management System is operating as intended. Required by ISO 42001 Clause 9.2. Distinct from external certification audits.
ISO/IEC 42001:2023	The first international standard for AI Management Systems. Published December 2023. Certifiable standard built on Annex SL architecture.
Management Review	A periodic review of the AIMS by top management, required by ISO 42001 Clause 9.3. Must include review of AI objectives, audit findings, risk status, and improvement opportunities.
MAP (NIST AI RMF)	The second of the four NIST AI RMF functions. Covers context-setting and risk identification — understanding the AI system, its stakeholders, and where harm could arise.