

Integrated Cyber Governance and Resilience Model (ICGRM)

A capability-based architecture for governing cybersecurity, privacy, AI, compliance, assurance and operational resilience

One governance architecture. Shared capabilities.
Multiple obligations. Preserved traceability.

Martyna Prandzioch

Founder & Research Lead

Imagined Illusion Sp. z o.o. | 2026

THE PROBLEM

Governance does not scale with the rulebook

Organizations do not lack frameworks. They struggle with fragmentation **between** them.

WHAT FRAGMENTATION LOOKS LIKE



Duplicated risk and control structures



Repeated evidence collection



Parallel assessments and audits



Fragmented ownership



Limited cross-domain visibility

THE SCALE OF THE PROBLEM

52%

maintain more than one
compliance framework

3.2

average frameworks in
organizations >100M revenue

76%

spent at least 30% of their time
on repetitive administrative work

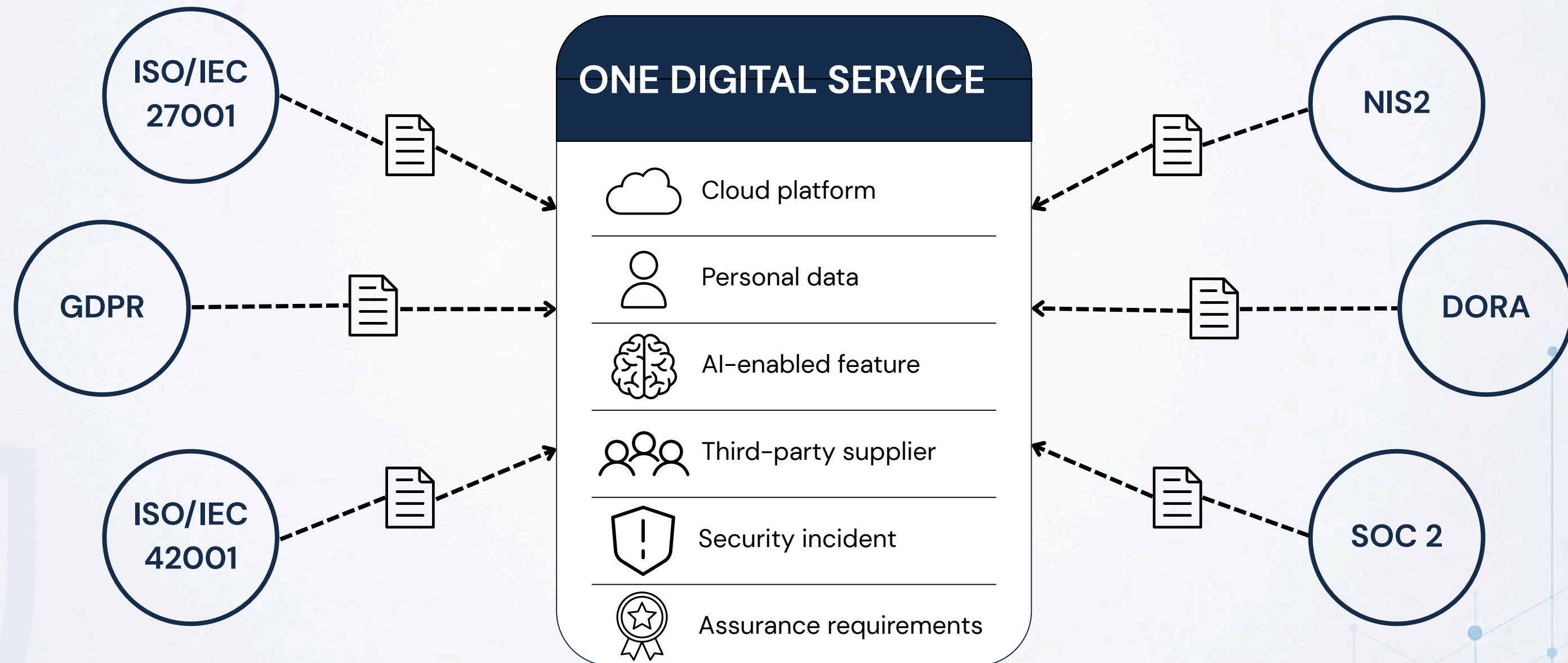
56%

use a common-controls
approach

THE FRAGMENTATION PATTERN

One system, multiple governance streams

A single digital service can simultaneously create security, privacy, AI, supplier, resilience, regulatory and assurance obligations.



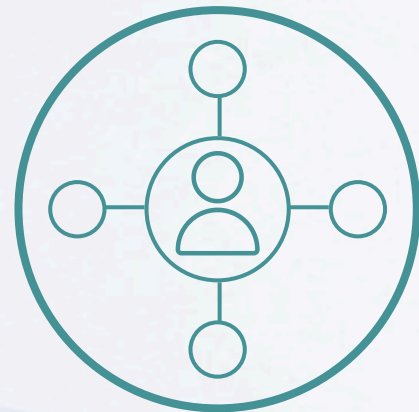
The underlying system is shared. The governance work surrounding it is often duplicated.

THE PROPOSITION

The ICGRM proposition

ICGRM shifts the organizing principle from external frameworks to **persistent organizational capabilities**.

INTEGRATE



Governance infrastructure

Shared processes, ownership, evidence and monitoring.

PRESERVE



Specialist meaning

Legal, regulatory, technical and assurance requirements remain distinct.

TRACE



End-to-end traceability

Every capability remains linked to its originating obligation.

Requirements do not need to be equivalent for their **governance infrastructure** to be shared.

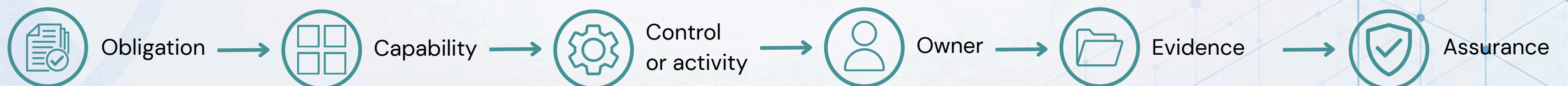
THE ARCHITECTURE

The three-layer architecture

ICGRM connects recurring governance mechanisms with operational capabilities while **preserving framework-specific traceability**.



THE ICGRM SIGNATURE CHAIN



LAYER 1

I4 Governance Mechanisms

Recurring governance structures identified across the analyzed instruments.

01  Executive governance & oversight

02  Roles & accountability

03  Risk assessment & treatment

04  Policy & control governance

05  Asset, data & system inventory

06  Third-party & supply-chain oversight

07  Incident management & reporting

08  Continuity, recovery & operational resilience

09  Monitoring & performance evaluation

I0  Audit & assurance

II  Legal, regulatory & contractual compliance

I2  Privacy & data governance

I3  AI-specific governance

I4  Continual improvement

I3/I4

KEY RESEARCH FINDING

13 of 14 mechanisms met the **high-recurrence threshold** across five or more analyzed instruments

LAYER 2

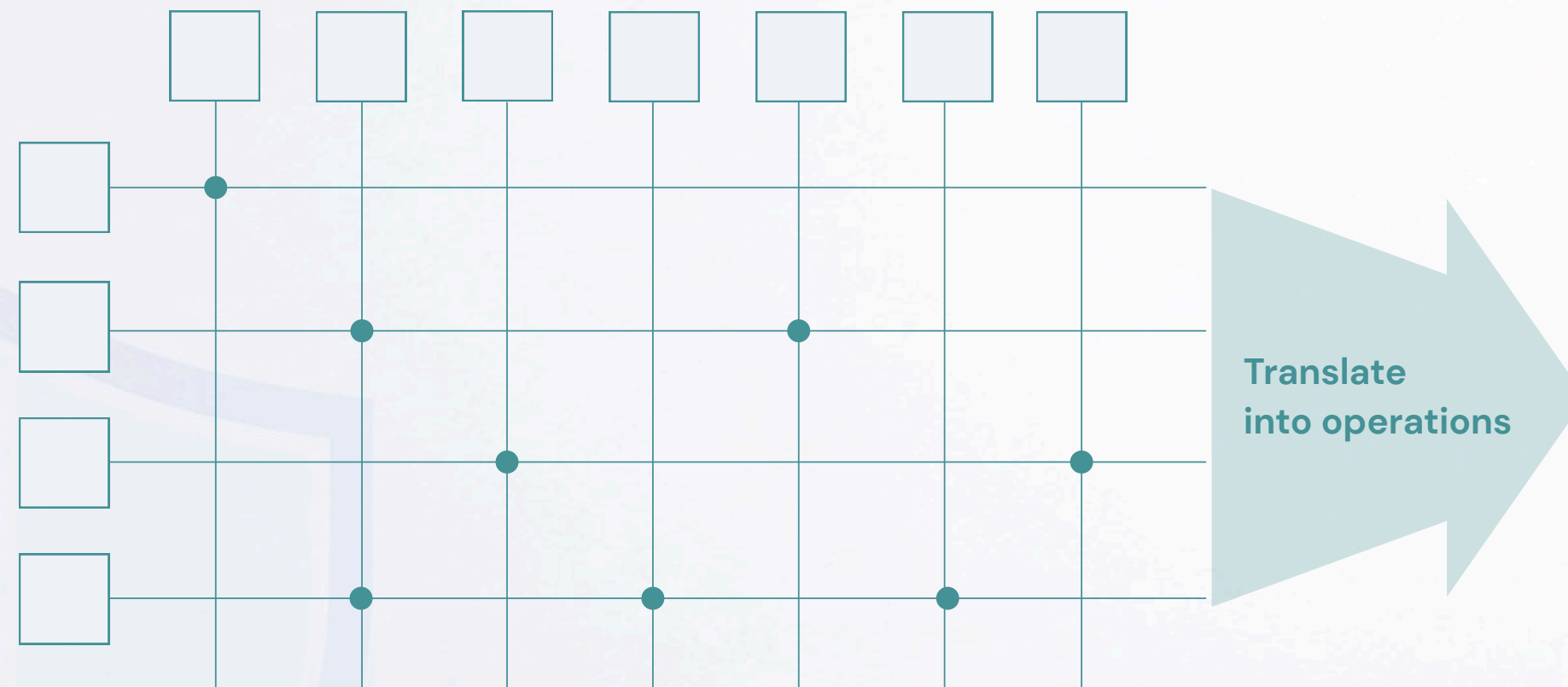
From overlap to operable capabilities

10/48

example capability clusters

A crosswalk shows where requirements relate. ICGRM translates the overlap into capabilities an organization can **assign, operate, evidence and improve**.

A CROSSWALK IDENTIFIES OVERLAP



ICGRM MAKES IT OPERABLE

 Risk identification	 Incident classification
 Policy lifecycle management	 Regulatory-notification assessment
 Control ownership	 Evidence management
 Third-party due diligence	 Assurance coordination
 Contractual governance	 Governance improvement

ICGRM is not another universal control catalogue.
It is an **operating architecture** for governance capabilities

LAYER 3

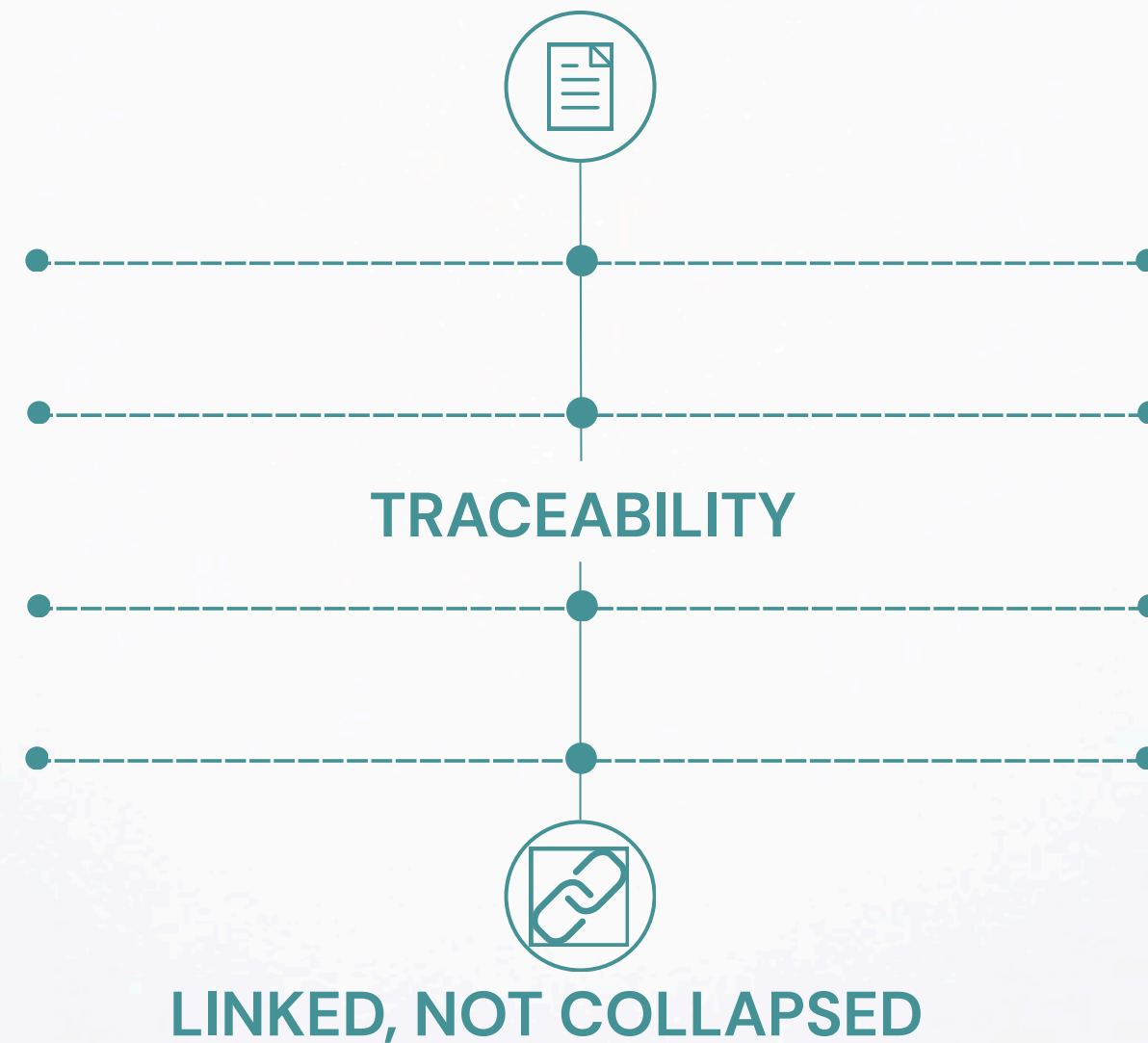
Traceability protects what must remain different

ICGRM integrates the infrastructure of governance while preserving the meaning, applicability and conditions of each originating obligation.

SHARED INFRASTRUCTURE



	Common intake
	Shared evidence
	Coordinated ownership
	Common monitoring
	Reusable workflows



PRESERVED DIFFERENCES



	Applicability
	Legal thresholds
	Notification deadlines
	Required recipients
	Sector-specific obligations
	Audit and assurance criteria

Integration occurs at the level of **governance infrastructure** – not at the expense of regulatory meaning.

WORKED EXAMPLE

Third-party governance

One supplier can simultaneously create security, privacy, AI, resilience, regulatory and assurance obligations.

ORIGINATING OBLIGATIONS



Distinct requirements remain traceable

SHARED CAPABILITY CLUSTERS

- 01 Third-party classification →
- 02 Due diligence →
- 03 Contractual governance →
- 04 Ongoing monitoring →
- 05 Exit and transition →

REUSABLE EVIDENCE

Supplier inventory	Questionnaire
Risk assessment	Approval record
DPA/security clauses	Monitoring record
Exit plan	

Reused where appropriate

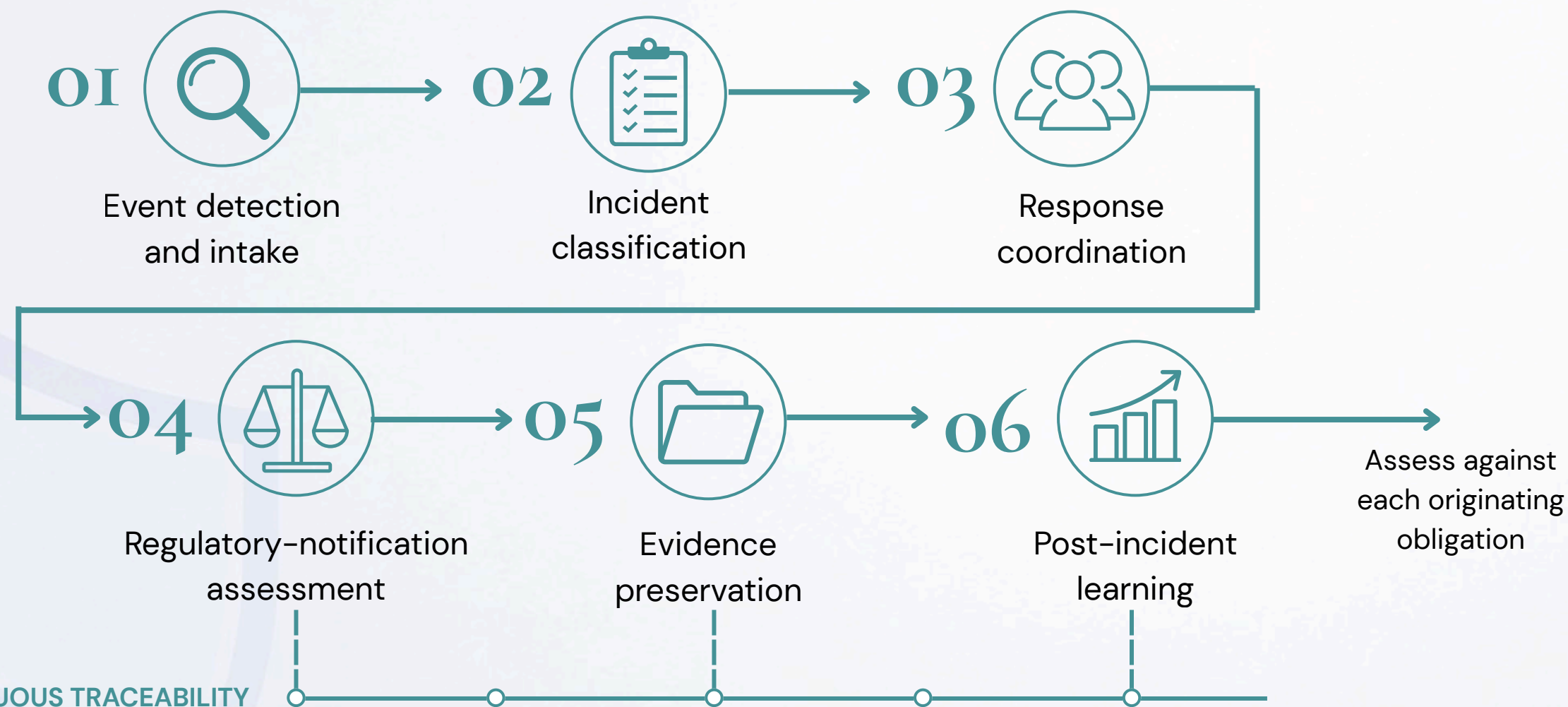
One coordinated supplier-governance process can support multiple obligations **without making those obligations equivalent.**

WORKED EXAMPLE

Incident governance

A coordinated incident-governance sequence can support detection, response, evidence and learning across multiple obligations.

SHARED OPERATIONAL SEQUENCE



Definitions, reporting thresholds, deadlines, recipients and required content **remain framework-specific**.



WHAT REMAINS FRAMEWORK-SPECIFIC



Definitions



Reporting thresholds



Deadlines



Recipients

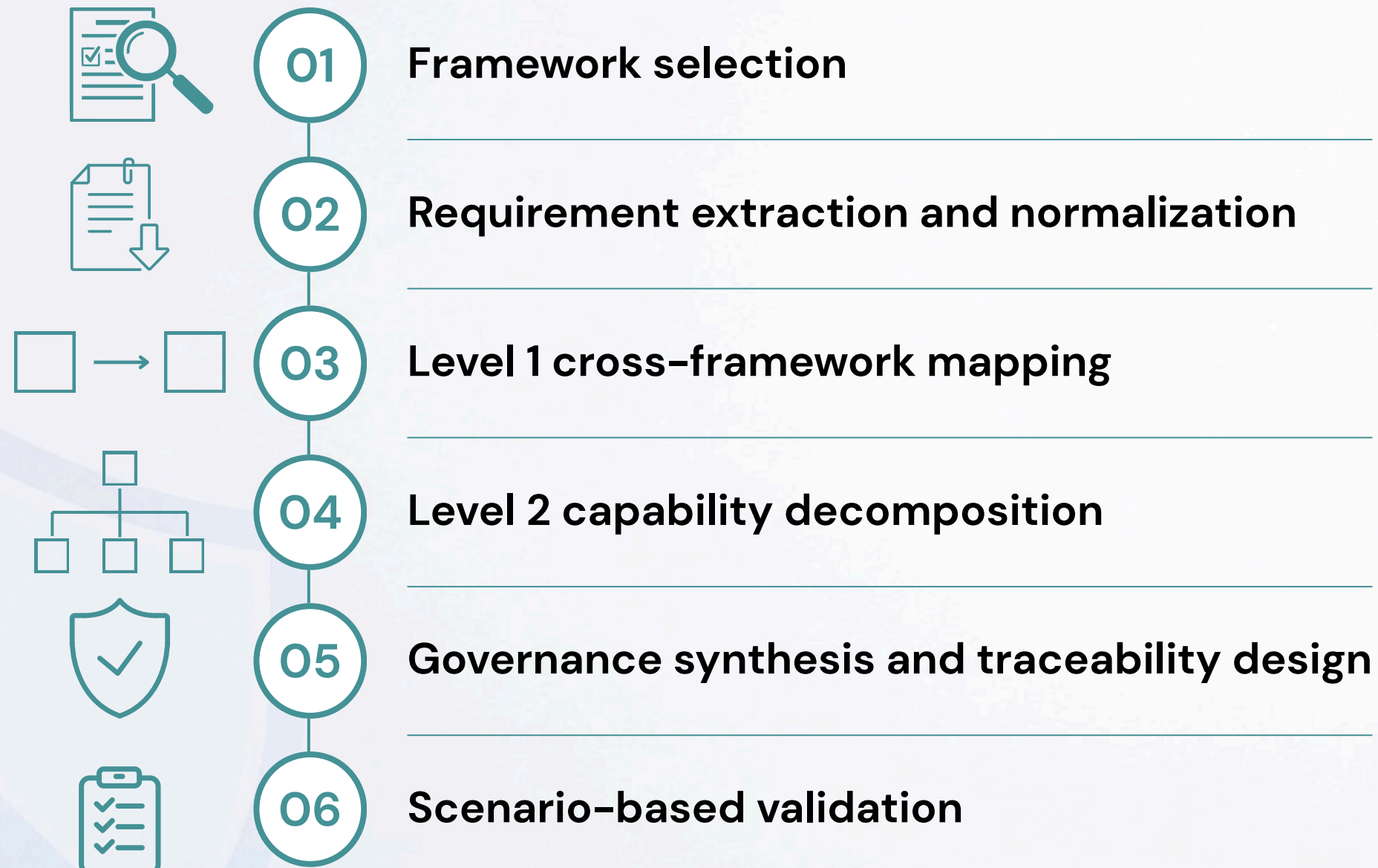


Required content

RESEARCH METHODOLOGY

Research design and evidence base

A structured six-stage process connects source requirements to an operational, traceable governance architecture.



Ambiguous relationships were coded conservatively.

EVIDENCE BASE

7 instruments analyzed	14 Governance Mechanisms	98 possible framework- to-mechanism relationships
-------------------------------------	---------------------------------------	---

91 MATERIAL RELATIONSHIPS

$$\begin{array}{c} 76 \\ \text{explicit / substantial} \end{array} + \begin{array}{c} 15 \\ \text{indirect / supporting} \end{array} = 91$$

48 Governance
Capability Clusters

Designed to avoid overstating cross-framework recurrence.

RESEARCH BOUNDARIES

What has been validated and what has not

The current evidence establishes the model's architecture and structural feasibility – not quantified implementation outcomes.

ESTABLISHED BY THE CURRENT RESEARCH

- ☒ Cross-framework recurrence at the governance-mechanism level
- ☒ A 14-mechanism governance taxonomy
- ☒ A 48-cluster capability architecture
- ☒ Framework-specific traceability logic
- ☒ Structural feasibility in scenario-based validation

NOT YET ESTABLISHED

Requires empirical validation

- ☐ Percentage cost reduction
- ☐ Shorter audit duration
- ☐ Staffing reduction
- ☐ Fewer incidents
- ☐ Quantified resilience improvement
- ☐ Measured implementation outcomes

Clear research boundaries strengthen – not weaken – the model.

They define the next phase: expert review, controlled pilots and measurable implementation research.



EXPERT REVIEW



CONTROLLED PILOTS



EMPIRICAL MEASUREMENT

PRACTICAL VALUE

Where ICGRM can create value

ICGRM is designed to help organizations:



REDUCE DUPLICATION

- ✓ Identify duplicated governance processes
- ✓ Reuse evidence where appropriate



CONNECT GOVERNANCE

- ✓ Clarify capability ownership
- ✓ Connect regulatory and assurance views
- ✓ Improve cross-domain risk visibility



BUILD ADAPTIVE CAPACITY

- ✓ Assess whether new obligations can be absorbed by existing capabilities
- ✓ Preserve organizational knowledge beyond individual employees

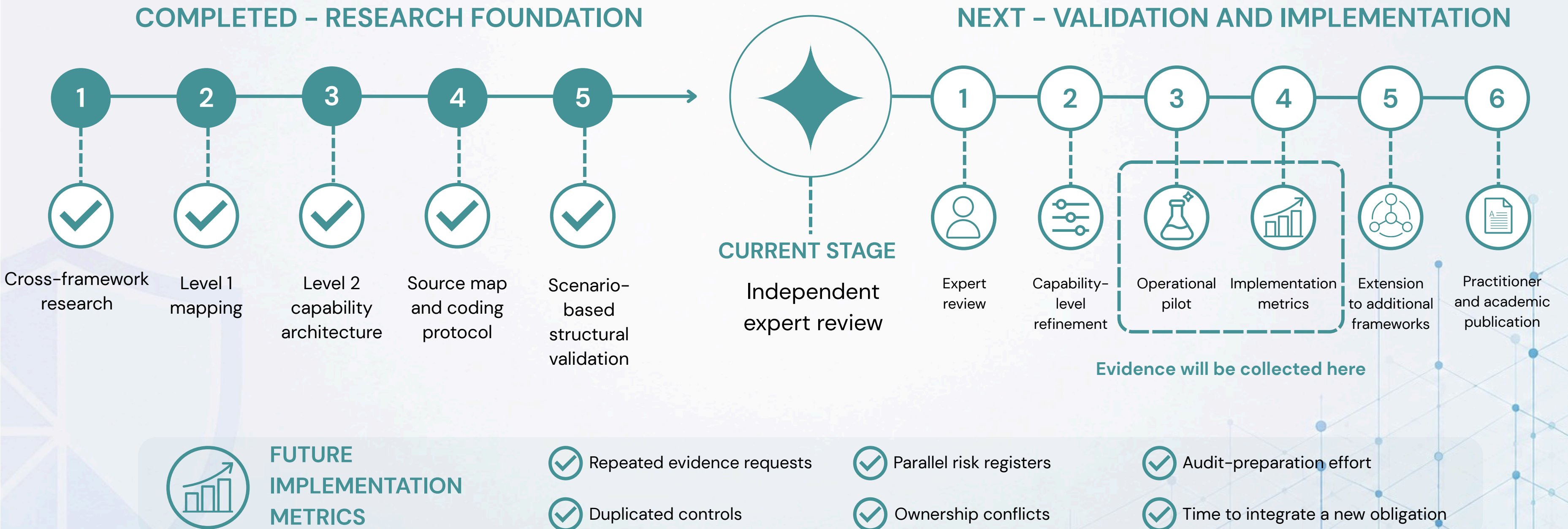


The model creates the conditions in which duplication can be **identified, measured and reduced.**

ROADMAP

Research and implementation roadmap

The architecture is established. The next phase moves from structured research to independent review, operational testing and measurable outcomes.



Proposed measures for empirical pilot evaluation.

INVITATION TO COLLABORATE

Help test how integrated governance works in practice

ICGRM is moving from structural validation toward independent review and controlled real-world testing.



01

EXPERT REVIEW

Challenge the architecture, boundaries and assumptions.



02

RESEARCH COLLABORATION

Support empirical validation and publication.



03

PILOT IMPLEMENTATION

Apply selected capabilities in a real organizational environment.



Independent evidence and practical learning

ICGRM is currently open for expert review, research collaboration and controlled pilot applications.



Martyna Prandzioch



LinkedIn: [Imagined Illusion](#)



[ICGRM.com](#)



ICGRM@imaginedillusion.com

SUPPORTING EVIDENCE

Appendix



Methodology, evidence and supporting research materials

Source selection • Coding protocol • Analytical matrices • Validation

APPENDIX A1 – SOURCE SELECTION

Instruments included in the study

Seven complementary instruments were selected to represent distinct governance domains, authority types and analytical perspectives.

INSTRUMENT	GOVERNANCE PERSPECTIVE	FORM OF AUTHORITY	ANALYTICAL ROLE
ISO/IEC 27001	Information security management	Certifiable international standard	Baseline for risk-based management-system governance
NIST CSF 2.0	Cybersecurity risk and organizational governance	Voluntary framework and guidance	Outcome-oriented cybersecurity governance perspective
ISO/IEC 42001	Artificial intelligence management	Certifiable international standard	AI-specific governance and management-system perspective
GDPR	Privacy and personal-data governance	Binding EU regulation	Rights-based, accountability and data-governance perspective
NIS2	Cybersecurity risk management and incident reporting	EU directive implemented through national law	Critical-entity governance and supervisory perspective
DORA	Digital operational resilience in financial services	Binding sector-specific EU regulation	Resilience, third-party risk and regulatory-reporting perspective
SOC 2	Trust-services assurance	Professional assurance criteria and reporting framework	Independent-assurance and evidence perspective

SELECTION RATIONALE

The set was selected to combine management-system standards, voluntary guidance, binding regulation, sector-specific requirements and assurance criteria across security, privacy, AI and operational resilience. It is analytically diverse, not exhaustive.

Selection was designed to test cross-framework recurrence across materially different governance instruments.

APPENDIX A2 – CODING METHODOLOGY

Level 1 coding protocol

Each instrument-to-mechanism relationship was assigned an ordinal code based on the material strength of its governance connection.

CODING SCALE

0	NOT MATERIALLY ADDRESSED
I	INDIRECTLY OR SUPPORTIVELY ADDRESSED
2	EXPLICITLY OR SUBSTANTIALLY ADDRESSED

INTERPRETATION RULES

- 01

SUBSTANCE OVER TERMINOLOGY
Coding was based on governance substance, not shared terminology.
- 02

CONSERVATIVE JUDGMENT
Ambiguous relationships were coded conservatively.
- 03

RELATIONSHIP, NOT EQUIVALENCE
Scores represent analytical relationships, not framework equivalence.

Code ≠ compliance status

The scale does not measure implementation maturity, control effectiveness or legal conformity.

The coding protocol identifies where governance mechanisms recur across instruments while preserving the distinct meaning and authority of each source.

Ordinal codes support structured comparison; they are not statistical weights.

APPENDIX A3 – LEVEL 1 RESULTS

Cross-framework recurrence matrix

GOVERNANCE MECHANISM	ISO 27001	NIST CSF	ISO 42001	GDPR	NIS2	DORA	SOC 2	RECURRENCE
1. Executive governance & oversight	2	2	2	1	2	2	2	7/7
2. Roles & accountability	2	2	2	2	2	2	2	7/7
3. Risk assessment & treatment	2	2	2	2	2	2	2	7/7
4. Policy & control governance	2	2	2	2	2	2	2	7/7
5. Asset, data & system inventory	2	2	1	2	2	2	1	7/7
6. Third-party & supply-chain oversight	2	2	2	2	2	2	2	7/7
7. Incident management & reporting	2	2	1	2	2	2	2	7/7
8. Continuity, recovery & operational resilience	2	2	0	2	2	2	2	6/7
9. Monitoring & performance evaluation	2	2	2	2	2	2	2	7/7
10. Audit & assurance	2	2	1	2	1	1	2	7/7
11. Legal, regulatory & contractual compliance	2	2	2	2	2	2	1	7/7
12. Privacy & data governance	2	1	1	2	2	1	1	7/7
13. AI-specific governance	0	0	2	0	0	0	0	1/7
14. Continual improvement	1	2	2	2	1	1	2	7/7

0 Not materially addressed

1 Indirectly/
supportively addressed

2 Explicitly/
substantially addressed

91 of 98 possible relationships were coded as material:
76 explicit/ substantial and 15 indirect/ supporting

Recurrence counts relationships coded 1 or 2

APPENDIX A4 – LEVEL 2 ARCHITECTURE

Complete capability architecture - Part I

Governance Capability Clusters GC-001–GC-028, organized under the first seven Governance Mechanisms.

01 EXECUTIVE GOVERNANCE & OVERSIGHT

- GC-001 Governance mandate
- GC-002 Executive oversight
- GC-003 Governance reporting

02 ROLES & ACCOUNTABILITY

- GC-004 Role assignment
- GC-005 Decision rights
- GC-006 Escalation governance

03 RISK ASSESSMENT & TREATMENT

- GC-007 Risk identification
- GC-008 Risk analysis and evaluation
- GC-009 Risk treatment
- GC-010 Risk acceptance

04 POLICY & CONTROL GOVERNANCE

- GC-011 Policy lifecycle management
- GC-012 Control design
- GC-013 Control ownership
- GC-014 Exception management

05 ASSET, DATA & SYSTEM INVENTORY

- GC-015 Asset inventory
- GC-016 Data and processing inventory
- GC-017 Dependency mapping

06 THIRD-PARTY & SUPPLY-CHAIN OVERSIGHT

- GC-018 Third-party classification
- GC-019 Third-party due diligence
- GC-020 Contractual governance
- GC-021 Ongoing third-party monitoring
- GC-022 Third-party exit and transition

07 INCIDENT MANAGEMENT & REPORTING

- GC-023 Event detection and intake
- GC-024 Incident classification
- GC-025 Incident response coordination
- GC-026 Regulatory notification assessment
- GC-027 Incident evidence preservation
- GC-028 Post-incident learning

APPENDIX A5 – LEVEL 2 ARCHITECTURE

Complete capability architecture - Part II

Governance Capability Clusters GC-029–GC-048, organized under the remaining seven Governance Mechanisms.

08 CONTINUITY, RECOVERY & OPERATIONAL RESILIENCE

- GC-029 Business continuity governance
- GC-030 Backup and restoration
- GC-031 Recovery planning
- GC-032 Resilience testing

09 MONITORING & PERFORMANCE EVALUATION

- GC-033 Control monitoring
- GC-034 Governance metrics and KPIs
- GC-035 Effectiveness evaluation

10 AUDIT & ASSURANCE

- GC-036 Internal audit
- GC-037 Control testing
- GC-038 Evidence management
- GC-039 Findings and remediation management

11 LEGAL, REGULATORY & CONTRACTUAL COMPLIANCE

- GC-040 Obligation identification
- GC-041 Obligation-to-control traceability
- GC-042 Compliance change management

12 PRIVACY & DATA GOVERNANCE

- GC-043 Privacy accountability
- GC-044 Data lifecycle governance
- GC-045 Privacy impact assessment

13 AI-SPECIFIC GOVERNANCE

- GC-046 AI system governance
- GC-047 AI impact and risk governance

14 CONTINUAL IMPROVEMENT

- GC-048 Governance improvement cycle

APPENDIX A6 – SCENARIO VALIDATION

Scenario-based validation

Five architectural conditions were tested across representative governance scenarios.

VALIDATION CONDITION	RESULT
01 Capabilities can be shared	✔ SUPPORTED STRUCTURALLY
02 Specialist obligations remain visible	✔ SUPPORTED STRUCTURALLY
03 Responsibility remains explicit	✔ SUPPORTED STRUCTURALLY
04 Evidence remains traceable	✔ SUPPORTED STRUCTURALLY
05 No source requirement must be discarded	✔ SUPPORTED STRUCTURALLY

 Structural support indicates architectural feasibility within the analyzed scenarios – not proof of operational effectiveness

APPENDIX A7 – RESEARCH BOUNDARIES

Research limitations

Current limitations define the next stages of validation and model development.

CURRENT LIMITATION

WHAT FOLLOWS

01	Seven-instrument scope	→	Extension to additional frameworks
02	Jurisdiction and sector applicability	→	Context-specific testing
03	Analytical synthesis	→	Independent expert review
04	Scenario-based validation	→	Controlled operational pilots
05	No implementation outcome data	→	Empirical measurement

i Limitations are treated as an explicit research agenda – not concealed as established evidence

APPENDIX A8 – SOURCES & MATERIALS

References and research materials

Selected primary instruments underpinning the ICGRM analysis.

SELECTED PRIMARY REFERENCES

- 01

ISO/IEC 27001:2022 – Information security management systems
- 02

NIST Cybersecurity Framework 2.0 (2024)
- 03

ISO/IEC 42001:2023 – Artificial intelligence management systems
- 04

Regulation (EU) 2016/679 – General Data Protection Regulation
- 05

Directive (EU) 2022/2555 – NIS2
- 06

Regulation (EU) 2022/2554 – Digital Operational Resilience Act
- 07

AICPA Trust Services Criteria (2017; revised points of focus 2022)

AVAILABLE ICGRM RESEARCH MATERIALS



Research
Supplement



Methodology and
Coding Protocol



Scenario-Based
Validation



Research Context
Report



Extended References
and Source Map



Full research materials and source documentation are available upon request through ICGRM.com