

Notes

This presentation develops the “Standards” area of SEVEN-G in ten slides. It answers a specific question: what SEVEN-G covers of ISO/IEC 42001, NIST (the AI Risk Management Framework, AI RMF, and the Cybersecurity Framework, CSF) and the EU AI Act. And, with the same precision, what it does not cover.

The short answer fits in one sentence. Standards say what must exist. SEVEN-G is the operating layer that makes it work, in each use case and in the portfolio, with investment and value discipline.

Three warnings before starting:

- SEVEN-G does not replace any standard. It relies on them and says where each requirement fits.
- SEVEN-G does not certify. Certification of a management system against ISO/IEC 42001 is issued by an accredited body.
- SEVEN-G does not reproduce the text of the standards. It cites them by number or by topic, with an own summary. Whoever applies them must check against the text they have purchased.

Why it matters: many companies already work with a management standard or with NIST. They do not adopt a new framework unless they see where it fits with what they already do. This area gives them that fit in writing.

The route: why it matters, the key concepts, how SEVEN-G addresses it, the templates and tools, an example, frequent mistakes, questions for management and the classroom, the relationship with other areas and how to start.

Question to open the session: which management standard or framework does your organisation use today, and who is accountable for it?

TERMS ON THIS SLIDE

- **SEVEN-G**: SEVEN-G (Seven-phase Enterprise Value & Governance) is an open framework for a company to implement, govern and measure AI, and to know whether it is transforming or only gaining efficiency. It treats

each use case as an investment with decision gates and gives the board figures it can trust. Management, the AI office, risk and the board use it. The link opens its entry page, with the story, the questions and the examples. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/entrada/index.html

SOURCES AND LINKS

- **Standards area page** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/areas/normas.html
- **Document 04 · SEVEN-G compared with the standards (§5.1)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/04_SEVEN-G_Origenes_diferencias_y_por_que_es_abierto.html#5-1-compared-with-the-standards-seven-g-as-an-ai-operating-model
- **Area page** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/areas/normas.html



Notes

This slide explains why the area exists. The sentence comes from document 04 (section 5.1), which positions SEVEN-G with respect to the standards.

A company that already has an ISO management system, or that reports to its risk committee with NIST, does not want to start from scratch. It wants to know three things: what it already does that is useful, what it must complete and what it must look for elsewhere. If nobody tells it, it rebuilds this by hand in every audit.

The two costly mistakes:

- Believing that the framework certifies. SEVEN-G issues no seal and does not attest conformity with any standard. Whoever claims otherwise misleads their board, their clients or their supervisor.
- Believing that one must choose. SEVEN-G and a standard do not compete. The standard sets what must exist; SEVEN-G turns it into gates, evidence, roles and reporting to the board.

Why it matters for decisions: the board does not need to know technical standards. It needs to know whether the company is duplicating effort, whether it has gaps without an owner and whether what it is told about compliance is true.

Example: document 04 summarises what each reference provides and what SEVEN-G adds. ISO/IEC 42001 provides the requirements of an AI management system, certifiable by an accredited body. SEVEN-G adds the lifecycle of each use case with gates and verifiable criteria, the portfolio as a funnel, value measurement with its status and the board pack.

Question for the classroom: have you ever seen a project that prepared the same evidence twice, once for the audit and once for management?

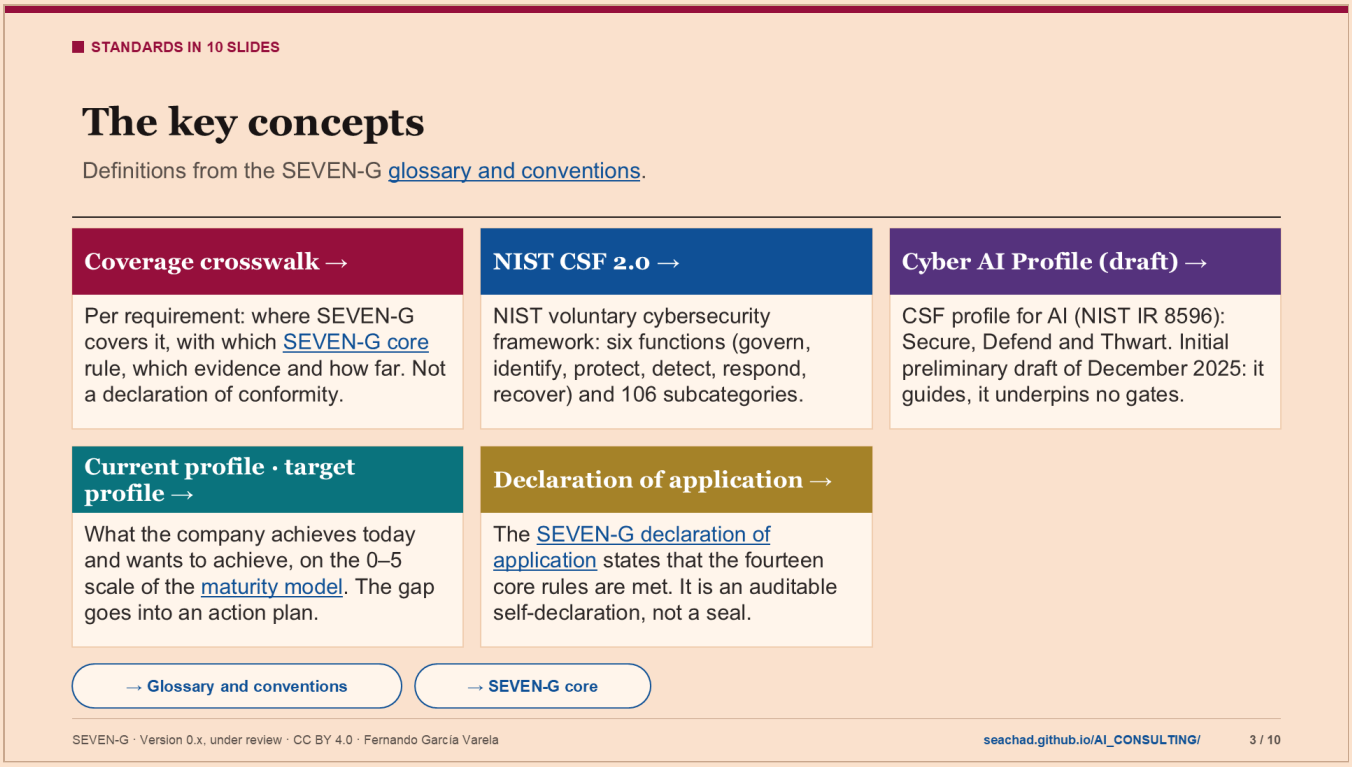
TERMS ON THIS SLIDE

- **SEVEN-G**: SEVEN-G (Seven-phase Enterprise Value & Governance) is an open framework for a company to implement, govern and measure AI, and to know whether it is transforming or only gaining efficiency. It treats

each use case as an investment with decision gates and gives the board figures it can trust. Management, the AI office, risk and the board use it. The link opens its entry page, with the story, the questions and the examples. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/entrada/index.html

SOURCES AND LINKS

- **Document 04 · SEVEN-G compared with the standards (§5.1)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/04_SEVEN-G_Origenes_diferencias_y_por_que_es_abierto.html#5-1-compared-with-the-standards-seven-g-as-an-ai-operating-model
- **ISO/IEC 42001:2023 · AI management system (ISO)** https://www.iso.org/standard/42001
- **SEVEN-G and the standards** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/04_SEVEN-G_Origenes_diferencias_y_por_que_es_abierto.html#5-1-compared-with-the-standards-seven-g-as-an-ai-operating-model



Notes

These five concepts are those of the SEVEN-G glossary for this area. Each card links to where it is explained.

- Coverage crosswalk. It is a table that says, for each requirement of ISO/IEC 42001, 38507, 23894, 42005, the NIST AI RMF and the EU AI Act, where SEVEN-G covers it, with which core rule, with which evidence and with what coverage. It is generated from a versioned data file. Why it matters: it is the tool for a gap analysis or to prepare an audit.
- NIST CSF 2.0. It is the NIST cybersecurity framework, published in its final version in February 2024. It is voluntary. It organises cybersecurity outcomes into six functions, 22 categories and 106 subcategories. Why it matters: many companies already read their cybersecurity in those six functions; AI security can enter the same scorecard.
- Cyber AI Profile. It is the CSF profile for AI. It has three areas: Secure, protecting the components of AI; Defend, using AI in cyber defence; and Thwart, thwarting attacks that use AI. It is an initial preliminary draft of December 2025. Why it matters: telling a draft from a final standard avoids deciding a gate with a text that may still change.
- Current profile and target profile. They are terms of the CSF and the AI RMF. SEVEN-G expresses the degree of each outcome with its 0 to 5 maturity scale, not with the CSF tiers.
- Declaration of application. A company declares that it applies SEVEN-G when it meets the fourteen core rules. It is drafted with template P61 and cites the core version.

Beware of two similar names: the declaration of application (P61) belongs to SEVEN-G; the statement of applicability (P74) belongs to ISO/IEC 42001.

Question for the classroom: why does a framework that wants to be useful to auditors also declare what it does not cover?

TERMS ON THIS SLIDE

- **Glossary and conventions** (documento 02): The official SEVEN-G glossary: each term with its definition, its Spanish equivalent and the document that develops it, plus the scales and codes used across the framework. It ensures everyone calls the same thing by the same name. The link opens the document. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/02_SEVEN-G_Glosario_y_convenciones.html
- **SEVEN-G core** (N-01–N-14): The fourteen rules that always apply, in any company, intensity and size: inventory, register, gates without skipping, the feasibility gate on its own, separation of duties, dual validation, value hypothesis, risks, rollback, board thesis, measurement and nonconformities. They are never lowered. A company declares that it applies SEVEN-G against this core. The link opens its definition in document 01. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/01_SEVEN-G_Metodologia_fundacional.html#14-1-the-seven-g-core
- **Maturity model** (documento 11): It measures how ready the company is to govern AI: seven dimensions (D1 to D7) with levels from 0 (non-existent) to 5 (optimised), 84 evidence-based questions and an overall level capped by strategy and risk. It is applied in the diagnosis and in the annual review. The link opens the dimensions in document 11. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/11_SEVEN-G_Modelo_de_madurez.html#2-1-dimensions
- **SEVEN-G declaration of application** (P61): A document in which a company declares that it applies SEVEN-G, rule by rule of the core, with its evidence. It is a self-declaration that an audit can verify; nobody outside grants it and it is not an accreditation. It lets the company state rigorously what is met and what is not. The link opens template P61. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/plantillas/P61_SEVEN-G_Declaracion_de_aplicacion_de_SEVEN-G.html

SOURCES AND LINKS

- **SEVEN-G glossary (document 02)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/02_SEVEN-G_Glosario_y_convenciones.html#glossary-of-framework-terms
- **NIST CSWP 29 · The NIST Cybersecurity Framework (CSF) 2.0** https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final
- **NIST IR 8596 · Cyber AI Profile (initial preliminary draft)** https://csrc.nist.gov/pubs/ir/8596/iprd
- **Glossary and conventions** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/02_SEVEN-G_Glosario_y_convenciones.html#glossary-of-framework-terms

STANDARDS IN 10 SLIDES

How SEVEN-G addresses it: operating layer and crosswalk

Regulatory mapping and standards crosswalk: requirements by coverage. ISO standards are cited by number or by topic, with an own summary.

Standard (rows)	Direct	Partial	Requires external control	Not covered
ISO/IEC 42001 · management system (17)	14	2	1 (certification)	0
ISO/IEC 38507 · governing body (6)	5	1	0	0
ISO/IEC 23894 · risk management (6)	6	0	0	0
ISO/IEC 42005 · impact assessment (5)	4	1	0	0
NIST AI RMF 1.0 (4)	4	0	0	0
EU AI Act (14)	8	2	2 (conformity, documentation)	2 (arts. 51–55, 99)
Total (52)	41	6	3	2

"Not covered" is information too: it stops the company from assuming what SEVEN-G does not do.

→ Full crosswalk → SEVEN-G maps, does not embed

SEVEN-G · Version 0.x, under review · CC BY 4.0 · Fernando García Varela seachad.github.io/AI_CONSULTING/ 4 / 10

Notes

This slide shows how SEVEN-G addresses the standards. There are two ideas.

First idea: SEVEN-G maps, it does not embed. It does not copy regulation into its phases. It links each obligation to a phase or stage, an accountable role, a piece of evidence and a tool. When a standard changes, the affected row of document 34 is updated, without redoing the lifecycle, the gates or the templates. For ISO/IEC 42001, the corporate cycle (C1 to C5) acts as the management system and the use case lifecycle (phases 0 to 7) as the operating process.

Second idea: the crosswalk. It answers the question asked by an auditor or a committee that already works with a standard: for each requirement, where SEVEN-G covers it, with which core rule, with which evidence and how far. The scale has four values:

- Direct: SEVEN-G requires what the requirement demands, with its evidence.
- Partial: SEVEN-G covers part of it; a note says what is missing and who completes it.
- Requires external control: it is met by a third party or by a procedure outside the framework, such as certification or CE marking; SEVEN-G only places it.
- Not covered: SEVEN-G does not address it; it is listed so that the company does not assume otherwise.

Examples from the table: in ISO/IEC 42001, the certification audit requires external control, because an accredited body carries it out. In the EU AI Act, the obligations of providers of general-purpose models (articles 51 to 55) are not covered: SEVEN-G covers whoever integrates a model, not its provider. The penalties regime (article 99) is cited for information only.

Limits: the crosswalk is not a certification, nor a declaration of conformity, nor legal advice. It serves to guide an audit or a gap analysis.

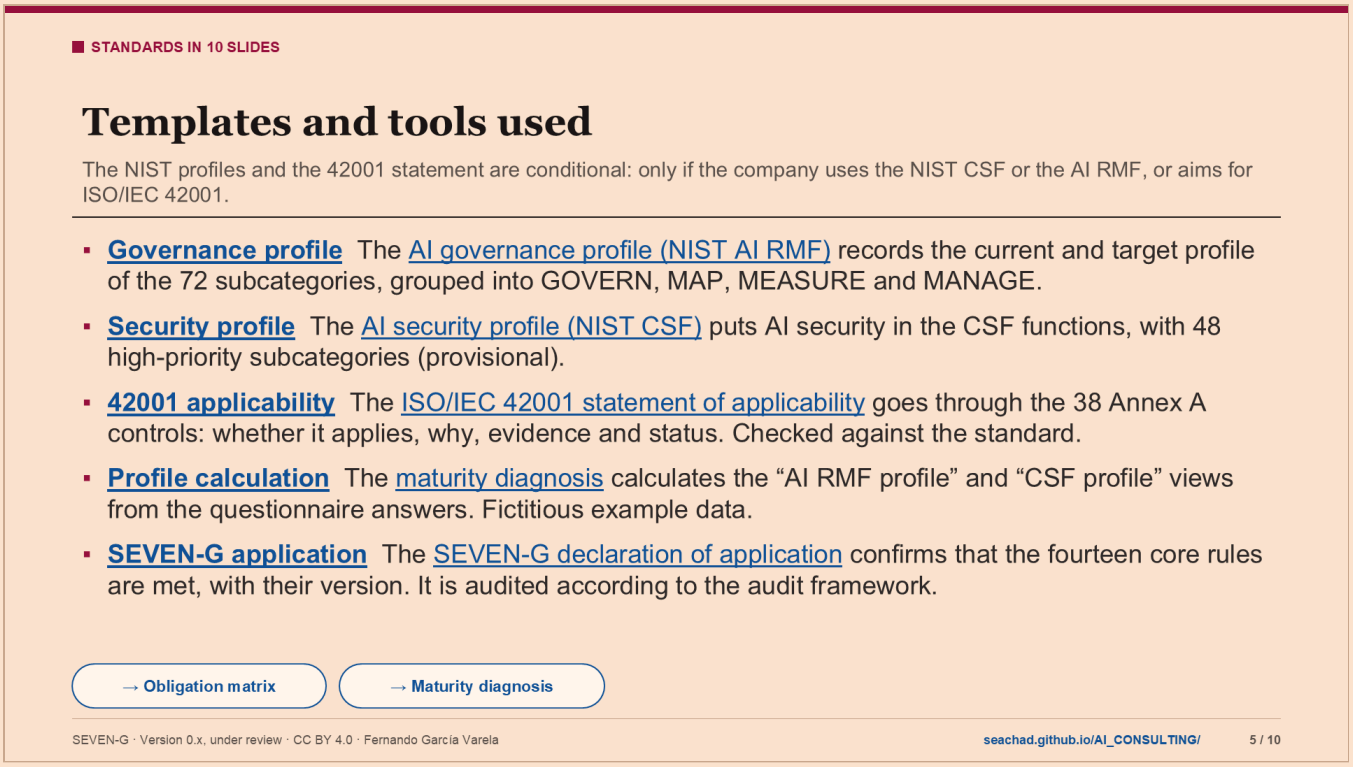
Question for management: who in our company completes the partial rows?

TERMS ON THIS SLIDE

- **Coverage crosswalk**: A coverage table that shows, for each requirement of a standard or regulation (ISO/IEC 42001, NIST AI RMF, the EU AI Act and others), where SEVEN-G covers it, with which core rule and which evidence, and whether coverage is direct, partial, requires an external control or does not exist. It is not a certification or a declaration of conformity. The link opens the table in document 34. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#9-1-coverage-crosswalk-standards-and-regulation-seven-g
- **Regulatory mapping and standards crosswalk** (documento 34): It relates SEVEN-G to regulation and standards (European AI Act, ISO/IEC 42001, NIST AI RMF, NIST CSF and others). Its crosswalk table says, row by row, what the framework covers, where and with which evidence, and what needs an external control. It does not replace the standard or an adviser. The link opens the table in document 34. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#9-1-coverage-crosswalk-standards-and-regulation-seven-g
- **SEVEN-G**: SEVEN-G (Seven-phase Enterprise Value & Governance) is an open framework for a company to implement, govern and measure AI, and to know whether it is transforming or only gaining efficiency. It treats each use case as an investment with decision gates and gives the board figures it can trust. Management, the AI office, risk and the board use it. The link opens its entry page, with the story, the questions and the examples. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/entrada/index.html

SOURCES AND LINKS

- **Document 34 · ISO/IEC 42001, clauses 4 to 10 (§4.1)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#4-1-clauses-4-to-10
- **Regulation (EU) 2024/1689 · EU AI Act (EUR-Lex)** https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
- **NIST AI 100-1 · AI Risk Management Framework (AI RMF 1.0)** https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10
- **SEVEN-G maps, does not embed** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#1-1-principle-seven-g-maps-it-does-not-embed



Notes

This slide lists the instruments of the area. In SEVEN-G, what is mandatory is the evidence, not the format: a template is an instrument that makes the work easier.

- AI governance profile (P73). It records the current and target profile of the 72 subcategories of the NIST AI RMF. It keeps the characteristics of trustworthy AI in view, such as bias, transparency, accountability and human oversight. The AI Office fills it in from the verified maturity assessment.
- AI security profile (P72). It puts AI security into the language of the CSF. It uses the 48 subcategories to which the Cyber AI Profile gives high priority in at least one area. The selection is provisional while the profile is a draft. The security (SEG) and agent (AG) controls of document 35 provide the evidence.
- ISO/IEC 42001 statement of applicability (P74). The standard requires declaring which controls are applied, which are excluded and why. The template does not reproduce the standard: it identifies each control by its code and summarises its topic. The AI auditor or the third line verifies it. A legal adviser or an ISO/IEC 42001 auditor should review it before it is offered.
- Maturity diagnosis (T15). It is the site tool that applies the questionnaire of document 11. It calculates the profiles from the same answers. Its example data are fictitious.
- SEVEN-G declaration of application (P61). It is the declaration that the company meets the core. It is not a seal: it is audited.

Why it matters: the three NIST and ISO templates are conditional. A company that does not use those standards does not need them. In this way the framework does not add load for those who do not ask for it.

Question for the classroom: what is the advantage of deriving the profiles from the same questionnaire instead of carrying out a separate assessment?

TERMS ON THIS SLIDE

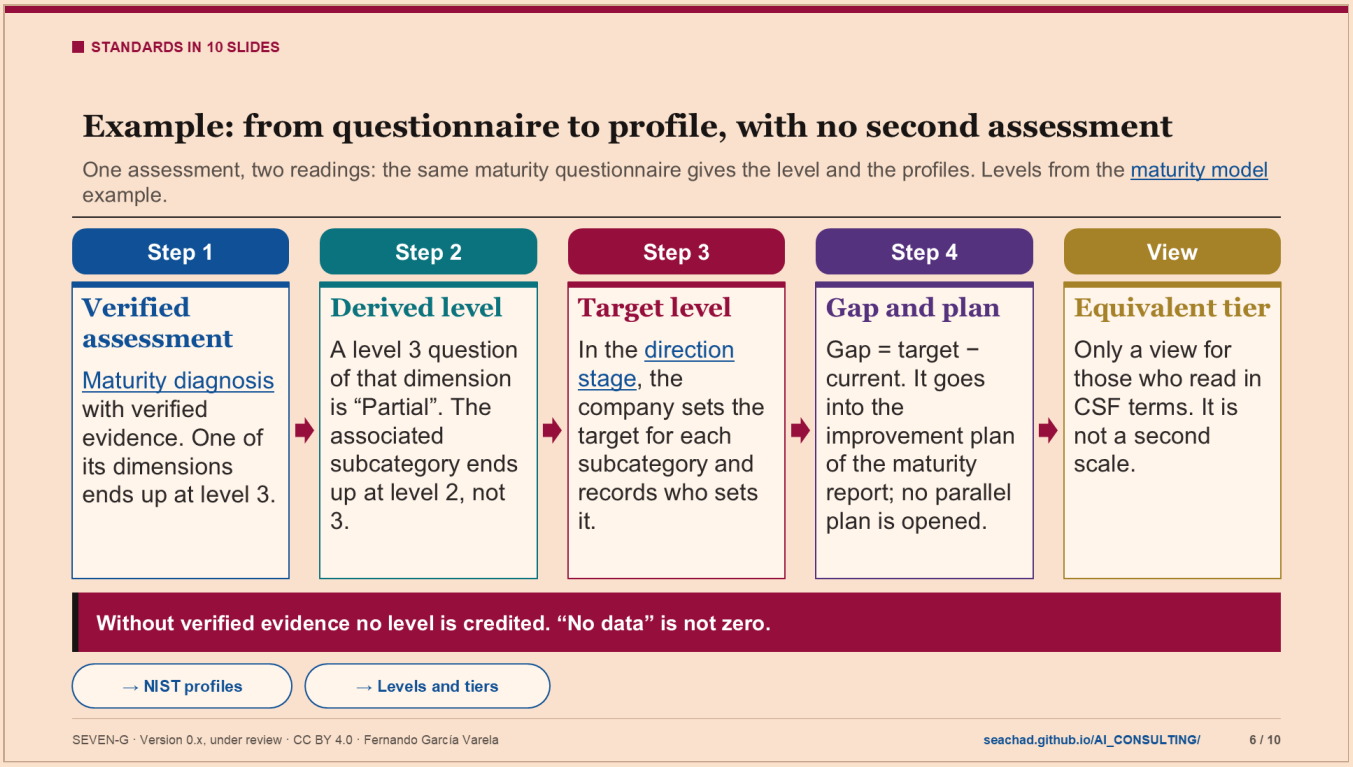
- **AI governance profile (NIST AI RMF)** (P73): A template for companies that use the NIST AI risk management framework: current and target level of its 72 subcategories, derived from the maturity diagnosis

without assessing twice, with the gap and the actions. It is conditional. The link opens the template. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/plantillas/P73_SEVEN-G_Perfil_de_gobierno_de_IA_NIST_AI_RMF.html

- **AI security profile (NIST CSF)** (P72): A template for companies that use the NIST cybersecurity framework: current and target profile of AI security, subcategory by subcategory, with the gap and the actions. The NIST AI profile it relies on is still a draft. It is conditional: only if the company uses that framework. The link opens the template. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/plantillas/P72_SEVEN-G_Perfil_de_seguridad_de_IA_CSF_y_Cyber_AI_Profile.html
- **ISO/IEC 42001 statement of applicability** (P74): A template for companies aiming at the ISO/IEC 42001 AI management system standard: for each Annex A control, whether it applies, why, where SEVEN-G covers it and with what evidence. It must be checked against the standard's text and reviewed by an expert; conformity is attested by an external body. The link opens the template. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/plantillas/P74_SEVEN-G_Declaracion_de_aplicabilidad_ISO_IEC_42001.html
- **Maturity diagnosis** (T15): A questionnaire of 84 evidence-based questions that measures the company's maturity in seven dimensions, from 0 to 5, and calculates the overall level. It also shows the three-lens reading and the NIST profiles. It is done in the initial diagnosis and at each annual review; its report is template P34. An unverified self-assessment does not give a valid level. The link opens an example with fictitious data. https://seachad.github.io/AI_CONSULTING/SEVEN-G/herramientas/T15_diagnostico_madurez/madurez.html
- **SEVEN-G declaration of application** (P61): A document in which a company declares that it applies SEVEN-G, rule by rule of the core, with its evidence. It is a self-declaration that an audit can verify; nobody outside grants it and it is not an accreditation. It lets the company state rigorously what is met and what is not. The link opens template P61. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/plantillas/P61_SEVEN-G_Declaracion_de_aplicacion_de_SEVEN-G.html

SOURCES AND LINKS

- **Document 94 · Requirement matrix (§7.2)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/94_SEVEN-G_Matriz_de_obligatoriedad_y_lectura_por_capas.html#7-2-company-board-compliance-third-parties-audit-and-implementation-p32-p74
- **Obligation matrix** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/94_SEVEN-G_Matriz_de_obligatoriedad_y_lectura_por_capas.html#7-2-company-board-compliance-third-parties-audit-and-implementation-p32-p74



Notes

This example uses the case that document 11 itself provides (section 7.5). It shows how a company obtains its NIST profiles without carrying out another assessment.

- Step 1, in the Diagnosis (C1). The company answers the maturity questionnaire of document 11 with evidence, and an independent verifier reviews it. In the example, dimension D6 (risk, security and compliance) ends up at level 3, "Defined".
- Step 2, derived level. Each AI RMF or CSF subcategory has a reference dimension and, where they exist, associated questions. Its level is that of the dimension, lowered to the level before that of the lowest-level associated question that is not "Yes" or "Not applicable". In the example, question D6.08, of level 3, is "Partial". The subcategory ends up at level 2.
- Step 3, in the Direction stage (C2). The company sets the target level for each subcategory, with the same proportionality as the other maturity targets. Who sets it is recorded.
- Step 4, gap and plan. The gap is the target minus the current level. Gaps are prioritised and go, with an owner and a deadline, into the improvement plan of the maturity report.
- Step 5, the tier view. For those who read in CSF terms, SEVEN-G calculates an equivalent tier. It is for guidance only: tiers describe the rigour of the whole organisation and are not a maturity level for each subcategory.

Why it matters: a company that already reports with the AI RMF or the CSF does not need a second assessment or a second number. The board sees a single scale, and the gap comes from evidence, not from a separate self-assessment.

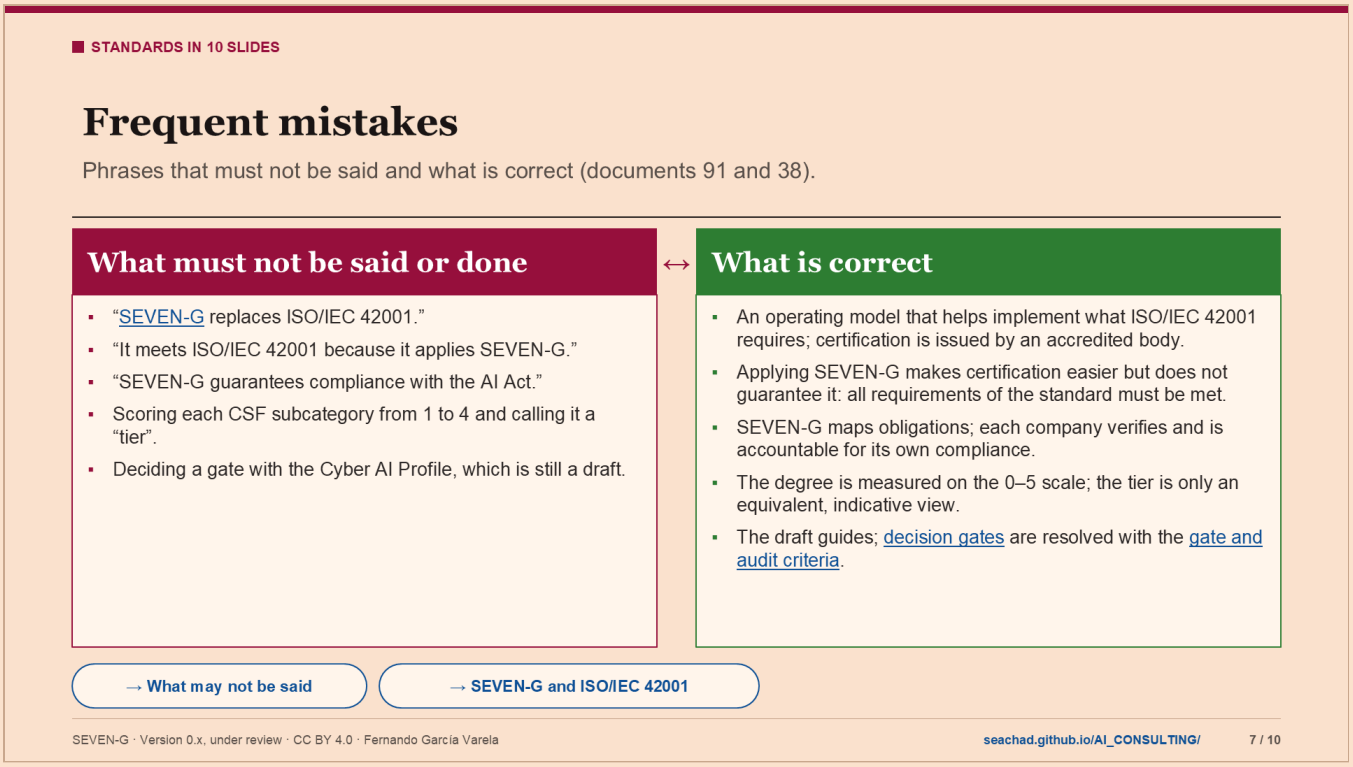
Question for the classroom: why is it better for a subcategory without evidence to be "no data" rather than zero?

TERMS ON THIS SLIDE

- **Maturity model** (documento 11): It measures how ready the company is to govern AI: seven dimensions (D1 to D7) with levels from 0 (non-existent) to 5 (optimised), 84 evidence-based questions and an overall level capped by strategy and risk. It is applied in the diagnosis and in the annual review. The link opens the dimensions in document 11. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/11_SEVEN-G_Modelo_de_madurez.html#2-1-dimensions
- **Maturity diagnosis** (T15): A questionnaire of 84 evidence-based questions that measures the company's maturity in seven dimensions, from 0 to 5, and calculates the overall level. It also shows the three-lens reading and the NIST profiles. It is done in the initial diagnosis and at each annual review; its report is template P34. An unverified self-assessment does not give a valid level. The link opens an example with fictitious data. https://seachad.github.io/AI_CONSULTING/SEVEN-G/herramientas/T15_diagnostico_madurez/madurez.html
- **Direction stage** (C2): The second stage of the corporate cycle. The board approves the AI thesis (what the company wants AI for), the ambition per sphere, the risk appetite, the budget envelope and the thresholds the whole framework will use. It is the decision that gives meaning to the rest: without it, each use case is approved on its own criteria. The link opens how that decision is taken in document 13. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/13_SEVEN-G_Tesis_de_IA_ambicion_y_apetito_de_riesgo.html#the-c2-decision-as-a-whole

SOURCES AND LINKS

- **Document 11 · NIST profiles (§7.5)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/11_SEVEN-G_Modelo_de_madurez.html#7-5-with-the-nist-profiles-ai-rmf-and-csf
- **Document 34 · AI RMF profile by subcategory (§5.4)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#5-4-ai-rmf-profile-by-subcategory
- **Document 34 · CSF 2.0 subcategories for AI (§5.5)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#5-5-ai-security-profile-csf-2-0-subcategories
- **NIST profiles** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/11_SEVEN-G_Modelo_de_madurez.html#7-5-with-the-nist-profiles-ai-rmf-and-csf
- **Levels and tiers** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/11_SEVEN-G_Modelo_de_madurez.html#2-2-levels



Notes

This slide gathers the mistakes that the site warns about explicitly. The guide for consultants (document 91, section 6.2) lists the phrases that may not be said and what to say instead.

- Presenting SEVEN-G as a substitute for a standard or as equivalent to a certification. They are different things: the standard says what must exist and is certified; SEVEN-G makes it work in each use case and does not certify.
- Saying that a company meets ISO/IEC 42001 because it applies SEVEN-G. Document 38 (section 12.1) makes it clear: to be certified, all requirements of the standard must be met, including the Annex A controls declared applicable. SEVEN-G makes certification easier but does not guarantee it. The certification audit is carried out by an accredited certification body.
- Promising compliance with the EU AI Act. SEVEN-G maps obligations; it does not guarantee compliance with them. Each organisation is solely responsible for identifying the regulation that applies to it and for verifying its compliance, with qualified advice.
- Inventing a tier scale. The CSF tiers (Partial, Risk Informed, Repeatable, Adaptive) describe the rigour of the whole organisation. They are not a level per subcategory, and the AI RMF has no tiers. SEVEN-G does not create a second scale.
- Using a draft as a rule. While the Cyber AI Profile is a draft, its selection and priorities are provisional and underpin no gate criterion.

One more mistake, of vocabulary: confusing the SEVEN-G declaration of application (P61) with the ISO/IEC 42001 statement of applicability (P74).

Why it matters: each of these mistakes reaches the board, a client or a supervisor as a false statement about compliance.

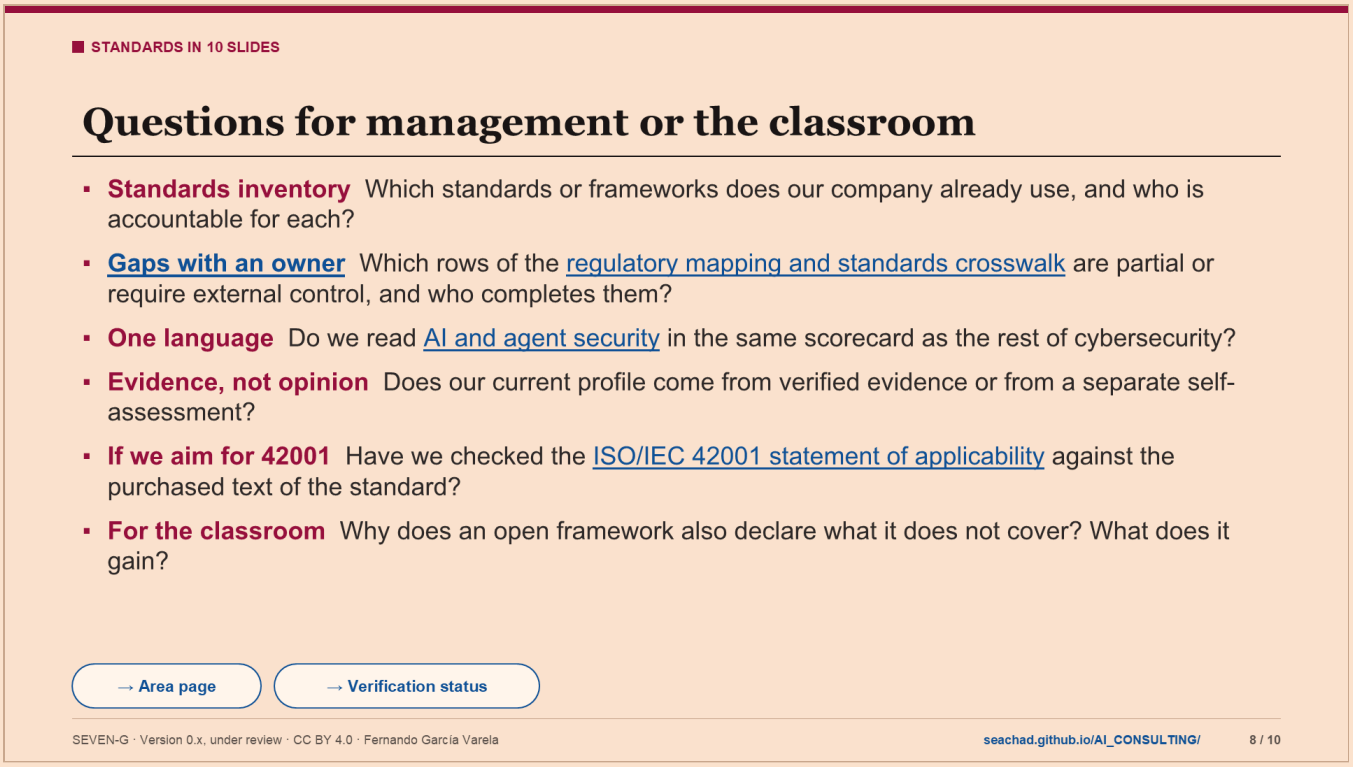
Question for management: what do our commercial or audit documents say today about AI standards?

TERMS ON THIS SLIDE

- **SEVEN-G**: SEVEN-G (Seven-phase Enterprise Value & Governance) is an open framework for a company to implement, govern and measure AI, and to know whether it is transforming or only gaining efficiency. It treats each use case as an investment with decision gates and gives the board figures it can trust. Management, the AI office, risk and the board use it. The link opens its entry page, with the story, the questions and the examples. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/entrada/index.html
- **Decision gates** (G0–G7): At the end of each phase there is a gate: a moment when a body decides, with verified evidence, whether the use case continues, continues with conditions, iterates, pivots or stops. There are at most two iterations before the decision is escalated. Gates turn enthusiasm into recorded decisions. The link opens their definition in document 01. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/01_SEVEN-G_Metodologia_fundacional.html#decision-gates
- **Gate and audit criteria** (documento 21): The list of criteria assessed at each gate, with their code, the evidence that substantiates them, whether they are mandatory and how they are verified; also the reduced Express list and when evidence the company already has can be used without redoing it. It is what verifiers and deciders use. The link opens the document. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/21_SEVEN-G_Criterios_de_gate_y_auditoria.html

SOURCES AND LINKS

- **Document 91 · What may not be said (§6.2)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/91_SEVEN-G_Guia_para_consultores.html#6-2-what-may-not-be-said
- **Document 38 · Relationship with ISO/IEC 42001 (§12.1)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/38_SEVEN-G_Marco_de_auditoria_de_IA.html#12-1-iso-iec-42001
- **Document 34 · NIST CSF 2.0 and Cyber AI Profile (§5.3)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#5-3-nist-csf-2-0-and-cyber-ai-profile
- **ISO/IEC 42006:2025 · Audit and certification bodies (ISO)** https://www.iso.org/standard/42006
- **What may not be said** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/91_SEVEN-G_Guia_para_consultores.html#6-2-what-may-not-be-said
- **SEVEN-G and ISO/IEC 42001** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/38_SEVEN-G_Marco_de_auditoria_de_IA.html#12-1-iso-iec-42001



Notes

These six questions are for a management meeting, a risk committee session or a classroom debate. Each one relies on what the site already defines.

- Standards inventory. Before mapping anything, one must know which standards or frameworks the company uses: ISO/IEC 42001, ISO/IEC 27001, the NIST CSF, the AI RMF or others. Each one needs an owner.
- Gaps with an owner. The crosswalk flags which rows are partial and which require external control. The note of each row says what is missing and who completes it. If nobody completes it, the gap stays open even if the framework is implemented.
- One language. The CSF organises cybersecurity into six functions. The security controls of document 35 state which function they contribute to. In this way AI security enters the same action plan as the rest.
- Evidence, not opinion. SEVEN-G profiles come from the verified maturity questionnaire. Without evidence there is no level.
- If we aim for 42001. The statement of applicability (P74) is always checked against the text of the standard that the company has purchased. SEVEN-G does not reproduce the text of standards.
- For the classroom. Declaring what is not covered builds trust and avoids false promises.

A note on rigour: the sources of document 34 are official or primary, with their consultation date. A draft, such as the Cyber AI Profile, is marked as such. Before using a row in a decision, its validity must be verified in the official source.

Why it matters: good questions turn a technical mapping into management decisions: who completes, who is accountable and with what evidence.

TERMS ON THIS SLIDE

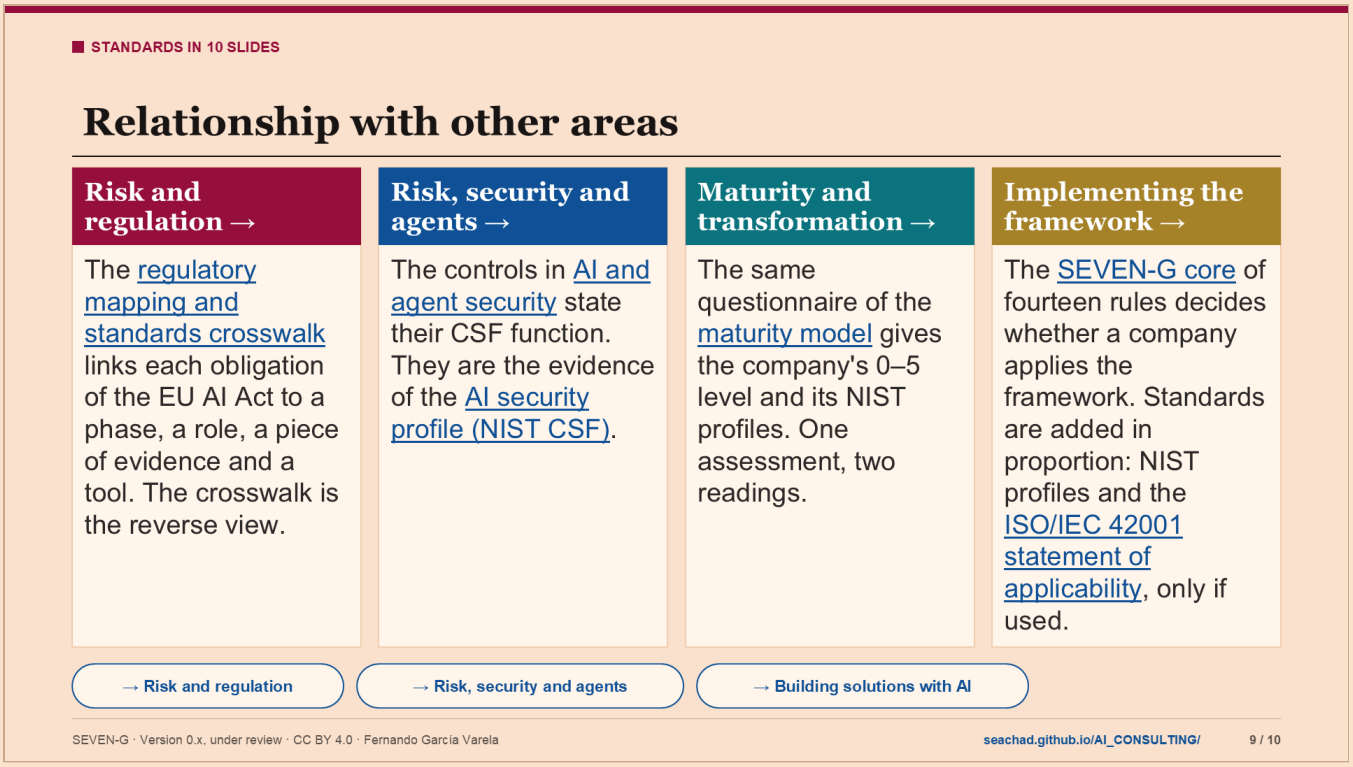
- **Regulatory mapping and standards crosswalk** (documento 34): It relates SEVEN-G to regulation and standards (European AI Act, ISO/IEC 42001, NIST AI RMF, NIST CSF and others). Its crosswalk table says, row

by row, what the framework covers, where and with which evidence, and what needs an external control. It does not replace the standard or an adviser. The link opens the table in document 34. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#9-1-coverage-crosswalk-standards-and-regulation-seven-g

- **AI and agent security** (documento 35): The threats specific to AI (prompt injection, data leakage, poisoning, agent abuse) and their controls: autonomy levels, a corporate gateway, an agent test bench, non-human identities and the use of AI in cyber defence. The link opens the document. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/35_SEVEN-G_Seguridad_de_IA_y_agentes.html
- **ISO/IEC 42001 statement of applicability** (P74): A template for companies aiming at the ISO/IEC 42001 AI management system standard: for each Annex A control, whether it applies, why, where SEVEN-G covers it and with what evidence. It must be checked against the standard's text and reviewed by an expert; conformity is attested by an external body. The link opens the template. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/plantillas/P74_SEVEN-G_Declaracion_de_aplicabilidad_ISO_IEC_42001.html

SOURCES AND LINKS

- **Document 34 · Regulatory mapping** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html
- **ISO/IEC 27001:2022 · Information security (ISO)** https://www.iso.org/standard/27001
- **Area page** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/areas/normas.html
- **Verification status** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#1-4-verification-status



Notes

Standards are not an isolated area. This slide shows which other SEVEN-G areas they connect with.

- Risk and regulation. Document 34 covers the EU AI Act, the GDPR, DORA, NIS2 and Spanish regulation. For each obligation it says in which phase it is handled, who is accountable, with which evidence and with which tool. The crosswalk takes the reverse route: it starts from the standard and says where it is in SEVEN-G.
- Risk, security and agents. Document 35 defines the security controls for AI and for agents. Each control states which CSF function it contributes to. Those controls are the evidence of the security profile (P72).
- Maturity and transformation. The maturity model of document 11 gives the company's level from 0 to 5 in seven dimensions. The AI RMF and CSF profiles are obtained from the same answers.
- Implementing the framework. The company applies SEVEN-G if it meets the fourteen core rules. The rest is applied in proportion to risk. The matrix of document 94 marks P72, P73 and P74 as conditional.

In the crosswalk, the AI system lifecycle (Annex A.6 of ISO/IEC 42001) points, among other evidence, to document 53, which sets what SEVEN-G requires when building with AI: human review, traceability, tests and security, checked at the design gate (G4) and the go-live gate (G5). There is also a relationship with SPHERES, which explains the nine spheres and the three ambition levels.

Why it matters: a committee that sees these connections avoids keeping three different mappings of the same standard.

Question for the classroom: which area of your organisation should own the crosswalk?

TERMS ON THIS SLIDE

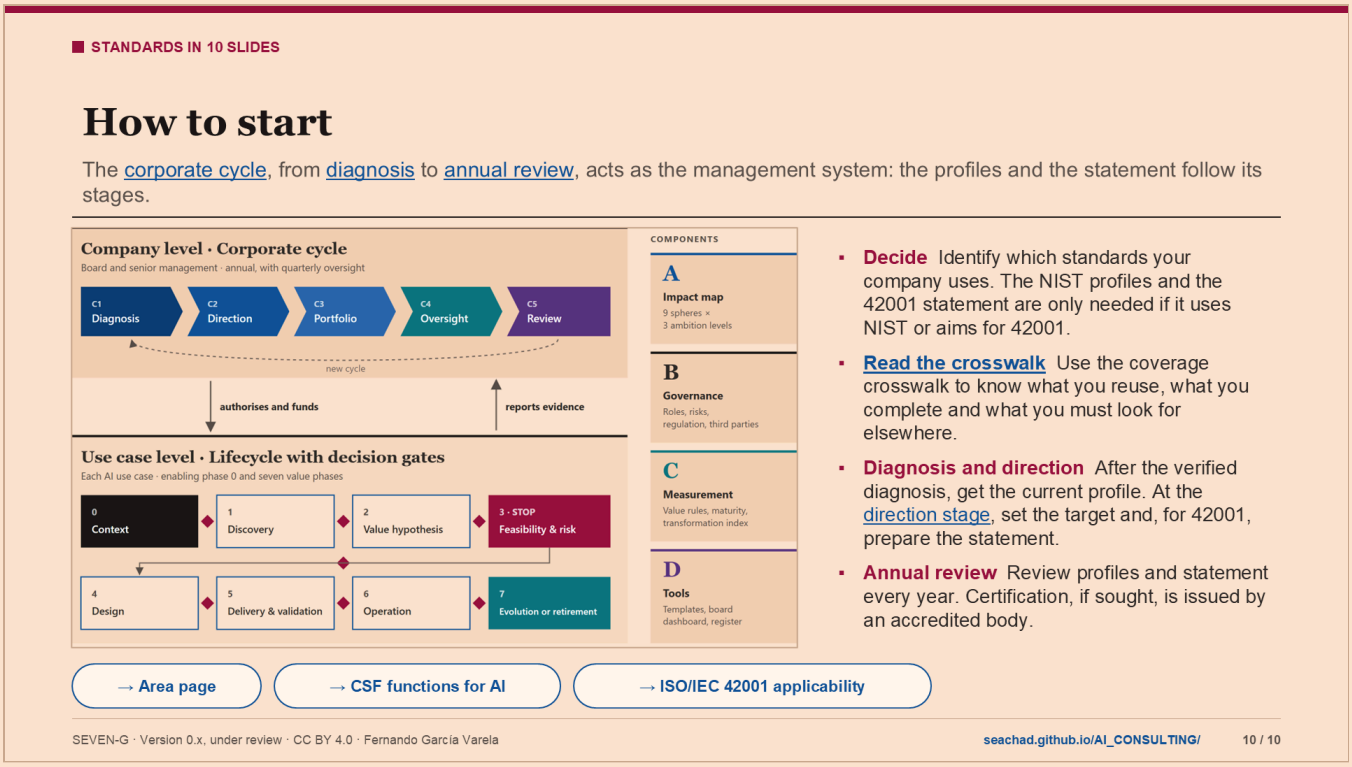
- **Regulatory mapping and standards crosswalk** (documento 34): It relates SEVEN-G to regulation and standards (European AI Act, ISO/IEC 42001, NIST AI RMF, NIST CSF and others). Its crosswalk table says, row by row, what the framework covers, where and with which evidence, and what needs an external control. It does

not replace the standard or an adviser. The link opens the table in document 34. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#9-1-coverage-crosswalk-standards-and-regulation-seven-g

- **AI and agent security** (documento 35): The threats specific to AI (prompt injection, data leakage, poisoning, agent abuse) and their controls: autonomy levels, a corporate gateway, an agent test bench, non-human identities and the use of AI in cyber defence. The link opens the document. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/35_SEVEN-G_Seguridad_de_IA_y_agentes.html
- **AI security profile (NIST CSF)** (P72): A template for companies that use the NIST cybersecurity framework: current and target profile of AI security, subcategory by subcategory, with the gap and the actions. The NIST AI profile it relies on is still a draft. It is conditional: only if the company uses that framework. The link opens the template. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/plantillas/P72_SEVEN-G_Perfil_de_seguridad_de_IA_CSF_y_Cyber_AI_Profile.html
- **Maturity model** (documento 11): It measures how ready the company is to govern AI: seven dimensions (D1 to D7) with levels from 0 (non-existent) to 5 (optimised), 84 evidence-based questions and an overall level capped by strategy and risk. It is applied in the diagnosis and in the annual review. The link opens the dimensions in document 11. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/11_SEVEN-G_Modelo_de_madurez.html#2-1-dimensions
- **SEVEN-G core** (N-01–N-14): The fourteen rules that always apply, in any company, intensity and size: inventory, register, gates without skipping, the feasibility gate on its own, separation of duties, dual validation, value hypothesis, risks, rollback, board thesis, measurement and nonconformities. They are never lowered. A company declares that it applies SEVEN-G against this core. The link opens its definition in document 01. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/01_SEVEN-G_Metodologia_fundacional.html#14-1-the-seven-g-core
- **ISO/IEC 42001 statement of applicability** (P74): A template for companies aiming at the ISO/IEC 42001 AI management system standard: for each Annex A control, whether it applies, why, where SEVEN-G covers it and with what evidence. It must be checked against the standard's text and reviewed by an expert; conformity is attested by an external body. The link opens the template. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/plantillas/P74_SEVEN-G_Declaracion_de_aplicabilidad_ISO_IEC_42001.html

SOURCES AND LINKS

- **Risk and regulation area page** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/areas/riesgo.html
- **Risk, security and agents area page** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/areas/seguridad.html
- **Document 34 · ISO/IEC 42001, Annex A by group (§4.2)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#4-2-annex-a-controls-by-group
- **Document 53, section 7: requirements for AI-generated code** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/53_SEVEN-G_Construccion_de_soluciones_con_IA.html#seven-g-minimum-requirements-for-ai-generated-code
- **SPHERES · What it is and what it is for** https://seachad.github.io/AI_CONSULTING/SPHERES/html/en/00_SPHERES_Que_es_y_para_que_sirve.html
- **Risk and regulation** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/areas/riesgo.html
- **Risk, security and agents** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/areas/seguridad.html
- **Building solutions with AI** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/53_SEVEN-G_Construccion_de_soluciones_con_IA.html



Notes

This slide gives the first steps. The figure shows the two levels of SEVEN-G: the corporate cycle (C1 to C5) and the lifecycle of each use case. For ISO/IEC 42001, the corporate cycle acts as the management system and the lifecycle as the operating process.

- Decide. First, which standards the company uses. Templates P72, P73 and P74 are conditional: only if the company uses the NIST CSF or the NIST AI RMF, or aims for ISO/IEC 42001. If not, they are not needed.
- Read the crosswalk. Document 34 (section 9.1) says what the company reuses, what it must complete and what it must look for elsewhere, such as certification or CE marking.
- In the Diagnosis (C1) and the Direction (C2). After the verified maturity assessment, the current profile is obtained. In C2 the company sets the target profile. If it aims for ISO/IEC 42001, it prepares the statement of applicability when it defines the scope of its AI management system.
- In the Review (C5). The profiles and the statement are reviewed. Document 34 is reviewed with its own procedure: monthly monitoring, formal quarterly review and full annual review. If a standard changes, the affected row is updated.

If the company seeks ISO/IEC 42001 certification, the audit is carried out by an accredited certification body. SEVEN-G audits are internal, first-party or second-party.

Why it matters: starting with the crosswalk avoids the most costly mistake, implementing the same thing twice.

Note: the figure is a site component. The figures in the site's examples are fictitious.

Final question for the classroom: if you had to present to your board tomorrow what your company covers of ISO/IEC 42001, which crosswalk row would you start with?

TERMS ON THIS SLIDE

- **Corporate cycle** (C1–C5): The company level of SEVEN-G: five stages repeated every year. Diagnosis (C1), direction with thesis and risk appetite (C2), portfolio (C3), quarterly oversight (C4) and annual review (C5). Senior management and the board lead it. It sets the frame each use case lives in: how much is wanted, how much risk is accepted and how it is overseen. The link opens its explanation in document 01. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/01_SEVEN-G_Metodologia_fundacional.html#company-level-corporate-cycle
- **Diagnosis** (C1): The first stage of the corporate cycle. The company looks at where it stands: what AI it uses (including unauthorised use), which use cases are under way, its maturity and its risks. The AI office does it with the management sponsor. Without this starting point, the thesis and the portfolio are decided blind. The link opens the diagnosis report template (P33). https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/plantillas/P33_SEVEN-G_Informe_de_diagnostico_C1.html
- **Annual review** (C5): The fifth stage of the corporate cycle. Once a year, the company reviews whether the thesis was met, how much value was realised, how maturity changed, what it learned and which thresholds it recalibrates; the bodies assess themselves. It is recorded in template P37. It closes the cycle and opens the next. The link opens the annual pack in document 60. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/60_SEVEN-G_Paquete_para_el_consejo.html#3-3-annual-review-pack-c5
- **Direction stage** (C2): The second stage of the corporate cycle. The board approves the AI thesis (what the company wants AI for), the ambition per sphere, the risk appetite, the budget envelope and the thresholds the whole framework will use. It is the decision that gives meaning to the rest: without it, each use case is approved on its own criteria. The link opens how that decision is taken in document 13. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/13_SEVEN-G_Tesis_de_IA_ambicion_y_apetito_de_riesgo.html#the-c2-decision-as-a-whole

SOURCES AND LINKS

- **Document 34 · ISO/IEC 42001, clauses 4 to 10 (§4.1)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#4-1-clauses-4-to-10
- **Document 38 · Relationship with ISO/IEC 42001 (§12.1)** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/38_SEVEN-G_Marco_de_auditoria_de_IA.html#12-1-iso-iec-42001
- **ISO/IEC 42001:2023 · AI management system (ISO)** https://www.iso.org/standard/42001
- **Standards area page** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/areas/normas.html
- **Area page** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/areas/normas.html
- **CSF functions for AI** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#5-3-nist-csf-2-0-and-cyber-ai-profile
- **ISO/IEC 42001 applicability** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/plantillas/P74_SEVEN-G_Declaracion_de_aplicabilidad_ISO_IEC_42001.html

LEGAL NOTICE

Legal notice: a generic, free methodological aid provided "as is" for information purposes; it is not legal advice and has not been legally reviewed for any case. Each organisation adapts it and is responsible for its legal review and its regulatory compliance; it may not reflect recent regulatory changes. To the fullest extent permitted by law, the author accepts no liability whatsoever for the effects of its application. It does not grant certification of any kind. Details in document 93.

CC BY 4.0 (content) · MIT (code) · Fernando García Varela · seachad.github.io/AI_CONSULTING/