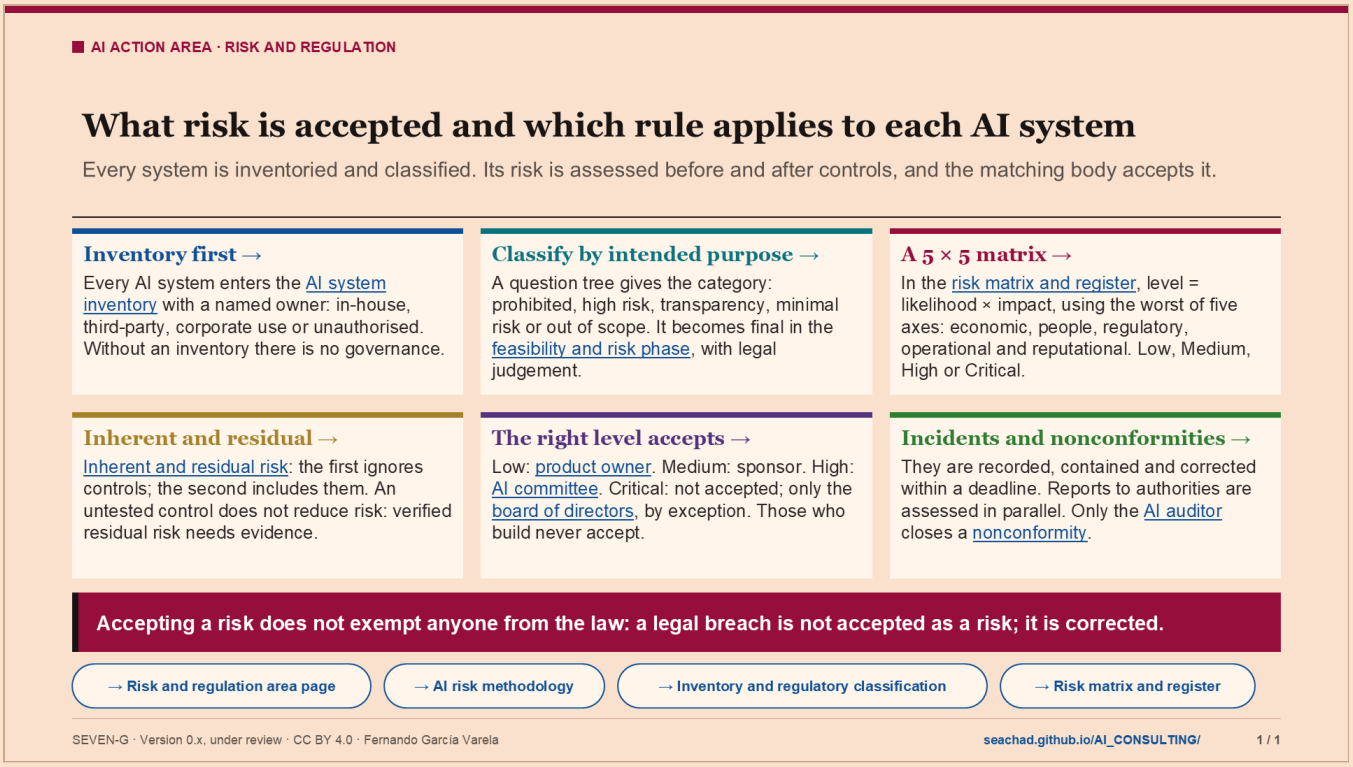

Notes

This slide summarises the Risk and regulation action area of SEVEN-G. It answers two questions the board needs to answer for every AI system: what risk the company accepts and which rule applies to it. The answer has six parts, read in order.

- Inventory first. All AI systems of four types of use are inventoried: in-house use cases, third-party AI integrated in processes, corporate use of general-purpose tools and unauthorised use. Each system has a named owner, not a generic area. Why it matters: without knowing which systems exist, risks cannot be managed, obligations cannot be met and the board cannot be informed (document 32).
- Classify by intended purpose. A question tree, based on the EU AI Act, gives the system's category: prohibited, high risk, transparency obligations, minimal risk or out of scope. Classification follows the intended use, not the technology. It is provisional in phase 0 and final in phase 3, with qualified legal judgement. When in doubt, the most demanding category applies.
- A 5 × 5 matrix. The risk level is likelihood times impact, each from 1 to 5. Impact is the worst of five axes: economic, people and rights, regulatory, operational and reputational. It is not averaged. There are four levels: Low (1 to 4), Medium (5 to 9), High (10 to 15) and Critical (16 to 25).
- Inherent and residual. Inherent risk is the level without the use case's specific controls. Residual risk is the level with controls: target at design time and verified when there is evidence that the controls work. An untested control does not reduce verified risk.
- The right level accepts. Each residual level is accepted by a different body. A Critical residual is not accepted: only, by exception, the board or its board committee approves it. A Critical residual without that approval blocks the feasibility gate (G3) and the go-live gate (G5).
- Incidents and nonconformities. An AI incident is an event in which a system causes or may cause harm. A nonconformity is a failure to meet a mandatory requirement of the framework. Both are recorded, contained and corrected within a deadline.

An example with fictitious data from the site's example register: the customer service conversational assistant (IA-2025-002) is classified with transparency obligations, because people talk to an AI. Its risk that a prompt injection reveals another customer's data is Critical without controls (4 × 4 = 16) and Medium with tested controls (2 × 4 = 8). That is why the AI Sponsor accepts it, with clearance from the AI Risk Owner.

Important notice: SEVEN-G is not legal advice and does not guarantee compliance with any rule. Each organisation identifies the regulation that applies to it, including that of its sector, and verifies that it is in force with qualified advice (document 34).

Question for the classroom: in your organisation, who signs off the acceptance of a high risk in an AI system today? Is it the same person who builds it?

TERMS ON THIS SLIDE

- **AI system inventory** (T02): A list of all the company's AI systems: its own, third-party AI embedded in processes, the assistants employees use and any unauthorised use detected. Each system has an owner, a regulatory classification, an intensity and an autonomy level. It comes first, because you cannot govern what you do not know. It is a view of the use case register: open the link and choose «Inventory» (fictitious data). https://seachad.github.io/AI_CONSULTING/SEVEN-G/herramientas/T01_registro_iniciativas/registro.html
- **Feasibility and risk** (fase 3): The phase in which a limited test checks whether the use case is technically and economically feasible, it is classified under regulation and its risks are recorded. It ends at the feasibility gate (G3), the main stop gate before the big spend. It is where stopping in time saves the most money. The link opens the phase manual in document 20. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/20_SEVEN-G_Manuales_de_fase.html#phase-3-feasibility-and-risk
- **Risk matrix and register** (T06): A likelihood-by-impact matrix (5 × 5) and register of each use case's risks: inherent and residual risk, controls and their effectiveness, response, contingency and who accepts the risk. It is mandatory from phase 3. It is filled in with template P12 or in the «Risks» view of the use case register, which also downloads an Excel file for the use case with proposed mitigation plans. Fictitious data. https://seachad.github.io/AI_CONSULTING/SEVEN-G/herramientas/T01_registro_iniciativas/registro.html
- **Inherent and residual risk**: Inherent risk is the risk a use case has without controls; residual risk is what remains after applying them. Both are measured as likelihood by impact on a 5 × 5 matrix. The residual level decides who must accept the risk: only the board accepts a Critical one. The link opens the explanation in document 33. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#inherent-risk-controls-and-residual-risk
- **AI product owner**: The role that builds the use case: accountable for the value hypothesis, actual use and adoption. Because of segregation of duties, it cannot verify evidence or decide the gates of its own use case. It is the team's day-to-day contact with the sponsor. The link opens the roles in document 01. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/01_SEVEN-G_Metodologia_fundacional.html#8-1-use-case-roles
- **AI committee**: A management body that decides the portfolio and the gates at its level, allocates budget and escalates to the board what belongs there. It brings together business, technology, finance and risk, and follows rules of procedure (P38). It matters because it turns scattered decisions into a single portfolio. The link opens its role in the governance model (document 30). https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/30_SEVEN-G_Modelo_de_gobierno.html#3-3-ai-committee
- **Board of directors**: The company's highest body. In SEVEN-G it approves the AI thesis and risk appetite (C2), Transform bets and their scaling, and oversees AI every quarter. AI is a strategic asset: its big decisions are not only for technology. The link opens its role in the governance model (document 30). https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/30_SEVEN-G_Modelo_de_gobierno.html#3-1-board-of-directors
- **AI auditor**: An independent person who verifies gate evidence in Enterprise-intensity use cases (in Lite the AI office does it). They do not build, sponsor or decide the use case they verify. They give the board assurance that figures and controls are not signed only by those who defend them. The link opens their independence and competences in document 38. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/38_SEVEN-G_Marco_de_auditoria_de_IA.html#independence-and-competences-of-the-ai-auditor

- **Nonconformity** (P50): A breach of a framework rule or a control, even if it caused no harm (for example, a use case in production without sign-off). It is classed as minor, major or critical, recorded (P50), its root cause analysed (P52) and corrected on time. It lets governance learn from its failures. The link opens the process in document 37. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/37_SEVEN-G_No_conformidades_e_incidentes.html#nonconformity-process

SOURCES AND LINKS

- **Risk and regulation area page** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/areas/riesgo.html
- **Document 33 · AI risk methodology** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html
- **Document 32 · Inventory and regulatory classification** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html
- **Document 34 §1 · Scope and responsibility of the regulatory mapping** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/34_SEVEN-G_Mapeo_regulatorio.html#purpose-and-scope
- **Document 37 · Nonconformities and incidents** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/37_SEVEN-G_No_conformidades_e_incidentes.html
- **Regulation (EU) 2024/1689 (EU AI Act), EUR-Lex** https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
- **AI risk methodology** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html
- **Inventory and regulatory classification** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/en/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.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/