COURSE · MODULE 05

Module 05 · Governance and risk

Who builds, who verifies, who decides and who can accept a risk

Fernando García Varela Version 0.1 (working draft) 19-09-2026 Draft for review

20	3	25	4
minutes	safeguards that are never reduced	cells in the risk matrix	risk levels

IN THIS DOCUMENT

01 Objective

02 Key ideas

03 Guided tour

04 Exercise

05 Self-check

06 Next step

Legal notice and disclaimer. SEVEN-G is a reference methodological framework provided "as is" and for information purposes only. It does not constitute legal, regulatory, financial or professional advice, nor does it guarantee compliance with any law or standard. References to general regulation (such as the EU AI Act, the GDPR, DORA or NIS2), to technical standards and to regulation specific to each sector or jurisdiction may be incomplete, may not apply to a particular case or may become out of date as a result of regulatory changes, interpretations or supervisory positions after their consultation date. **Each organisation that uses SEVEN-G is solely responsible for identifying the regulation that applies to it, verifying that it is current and certifying its own regulatory compliance**, with the appropriate qualified advice. This methodology is a generic, free aid shared with the community so that nobody has to start from scratch; each person or organisation can and should adapt it to its own use. It must not be inferred that its legally sensitive parts have been reviewed by legal counsel: those reviews, for each company or sector, are the ultimate responsibility of the company, consultant or organisation that uses it. Although every effort is made to keep it up to date, some regulation may have changed without being reflected here. To the fullest extent permitted by law, the author accepts no responsibility whatsoever for the effects of its application in any organisation or for its full applicability. The methodology does not grant certification of any kind. The author accepts no liability for any use made of this content or for any decisions taken on the basis of it. The data, figures, companies and cases in the examples are fictitious or illustrative.

01

Objective

By the end you will be able to explain the framework's segregation of duties, assign the roles of a use case without incompatibilities and read a risk register: inherent level, residual level and the body that can accept it.

02

Key ideas

1. **Nobody approves themselves.** Whoever builds neither verifies nor decides their own work; risk clearance is independent of the team; the board approves the direction and the risk appetite.
2. **There is no need to create new bodies.** In a medium-sized company, the management committee with a monthly AI item, a one-person AI Office and an independent auditor for Enterprise use cases are enough.

3. **Risk = probability × impact**, from 1 to 25, in four levels. It is assessed before controls (inherent) and after them (residual).
4. **Each level has its accepting body.** A Critical residual risk can only be accepted by the board; without that approval, it blocks G3 and G5.

03

Guided tour

Step	What to open	What to look at
1	document 01, section 8	Use case roles, incompatibilities and company bodies.
2	document 30, section 11	The adaptation to small organisations.
3	document 33, sections 4 to 7	Scales, inherent and residual risk, responses and acceptance.
4	document 32, section 5	The regulatory classification tree: it is done before design.
5	T06 (risk view of the register)	The 5 × 5 matrix of the example portfolio and the observations it generates.

04

Exercise

In the risk view of the example register, click the cell with the highest residual risk. Which use case is it, who has accepted it and does it have a contingency plan? Then switch to inherent risk and see how much the controls reduce the risk: is that reduction credible?

05

Self-check

1. Can the sponsor also be the risk owner of their own use case?
2. Who accepts a High residual risk?
3. By which phase must the risk register already exist?
4. What happens to a Lite use case that starts processing specially protected data?

06

Next step

Module 06 · Measuring value · Course guide

Answers. 1) No: they are incompatible roles. 2) The AI Committee. 3) Phase 3; it is a G3 criterion. 4) It moves to Enterprise intensity: intensity is reviewed at G3 and at each R6, and one criterion is enough.