FALNOA

AI AGENTS UNDER CONTROL

What DORA and the EU AI Act ask for, in plain language, and a 12-point checklist.

BANKING AND INSURANCE IN THE EUROPEAN UNION

PRACTICAL GUIDE · NOVEMBER 2026

IN ONE MINUTE

FOUR IDEAS

1

AI agents no longer just answer.

They carry out steps in real processes: they change records, send messages, start payments.

2

DORA has applied since 17 January 2025.

It does not mention agents. It covers the systems they run on and the suppliers that deliver them.

3

The AI Act moved high-risk rules to 2 December 2027.

The obligations are the same. There is more time to meet them well.

4

Control means being able to answer three questions.

Who let the agent do this, who approved it, and where the proof is.

THE PROBLEM

FROM ANSWERING TO ACTING

An assistant that gets it wrong gives a bad answer. An agent that gets it wrong makes a bad transfer. The risk changes in kind once software has hands.

OWASP calls this risk “excessive agency” and names three causes:

TOO MANY FUNCTIONS

The agent can reach tools it does not need for the task.

TOO MANY PERMISSIONS

Those tools let it do more than it should in other systems.

TOO MUCH AUTONOMY

Actions with impact go ahead without a person confirming them.

WHO LET IT DO THIS?
WHO APPROVED?
WHERE IS IT RECORDED?

Source: OWASP Top 10 for LLM Applications 2025, LLM06:2025 Excessive Agency.

THE CALENDAR

WHAT APPLIES, AND WHEN

17 JAN 2025

DORA

The regulation applies to banks, insurers and other financial entities.

DORA ART. 64

2 FEB 2025

AI Act: prohibited practices

The first prohibitions start to apply.

AI ACT ART. 113

2 AUG 2026

AI Act: transparency

People who talk to an AI must be told so.

AI ACT ART. 50

TODAY: NOVEMBER 2026

2 DEC 2027

High risk: Annex III uses

Consumer credit, life and health insurance, recruitment. It was 2 August 2026 before.

REG. (EU) 2026/1744

2 AUG 2028

High risk: regulated products

AI systems built into Annex I products.

REG. (EU) 2026/1744

> The delay came with Regulation (EU) 2026/1744, published on 24 July 2026 and in force since 27 July 2026.

Sources: Regulation (EU) 2022/2554; Regulation (EU) 2024/1689 as amended by Regulation (EU) 2026/1744; European Commission, "AI Act".

DORA IN PLAIN LANGUAGE

FIVE THINGS DORA ASKS FOR

THE BOARD ANSWERS

ART. 5

The management body bears the ultimate responsibility for managing ICT risk. It cannot be handed to a supplier or a technical team.

KNOW WHAT YOU HAVE

ART. 8

Identify and document the business functions that ICT supports and the assets they depend on.

KNOW YOUR SUPPLIERS

ART. 28

Keep a register of information on every contract for ICT services. For critical or important functions, have an exit strategy.

TEST

ART. 24

Run a testing programme. Systems that support critical or important functions are tested at least once a year.

REPORT MAJOR INCIDENTS

ARTS. 17 AND 19

Have a process to detect, manage and record incidents. Major ones go to the authority: initial notification, intermediate report, final report.

> **And agents?** DORA does not mention them. In our reading, an agent that carries out steps in a critical process is part of that system. If a supplier provides it, that contract belongs in the register.

Source: Regulation (EU) 2022/2554. Register of information templates: Implementing Regulation (EU) 2024/2956.

THE AI ACT IN PLAIN LANGUAGE

WHEN IT IS HIGH RISK, AND WHAT CHANGES

IT IS HIGH RISK WHEN ANNEX III	The system evaluates the creditworthiness or credit score of people (fraud detection excepted), assesses risk and pricing in life and health insurance, or is used to recruit and to decide about workers.
PEOPLE WITH AUTHORITY ARTS. 14 AND 26	Human oversight goes to people with competence, training and authority. They must be able to disregard or reverse an output and to stop the system.
RECORDS KEPT ARTS. 12 AND 26	The system records events automatically. Whoever uses it keeps those logs for at least six months. Financial institutions keep them with the documentation financial law already requires.
ASSESS THE IMPACT ART. 27	Before using a credit or life and health insurance system, assess its impact on fundamental rights.
ALREADY APPLIES ART. 50	A person who interacts with an AI must be told so, unless it is obvious.

> **Is an agent an "AI system"?** The definition covers systems that operate "with varying levels of autonomy" (Art. 3). The GDPR still applies to solely automated decisions (Art. 22).

Sources: Regulation (EU) 2024/1689 as amended by Regulation (EU) 2026/1744; Regulation (EU) 2016/679.

DELAYED IS NOT WAIVED

The high-risk deadline moved. The obligations did not. And DORA already applies today to any agent that touches a critical process.

CHECKLIST

12 POINTS, YES OR NO

KNOW WHAT EXISTS

- [ ] 01 **Every agent is in an inventory.**
  With its purpose, model and the data it uses.
  DORA 8

- [ ] 02 **Every agent has an owner.**
  A named person, not a team.
  DORA 5
  AI ACT 26

- [ ] 03 **Suppliers are in the register.**
  Third-party models and agents, with an exit plan.
  DORA 28

CONTROL BEFORE THE ACTION

- [ ] 04 **The limits are written down.**
  What each agent does alone and what waits for a person.
  AI ACT 14
  OWASP LLM06

- [ ] 05 **Actions with impact wait for approval.**
  With a written reason. Two people for the largest.
  AI ACT 14
  GOOD PRACTICE

- [ ] 06 **You can stop every agent at once.**
  And you have tried it.
  AI ACT 14

CHECKLIST

12 POINTS, CONTINUED

PROVE AFTER THE ACTION

- [ ] 07 **Every action and every approval is recorded.**
  Who, what, when and why.
  AI ACT 12, 26

- [ ] 08 **You can show the record was not changed.**
  An altered copy is detected.
  GOOD PRACTICE

- [ ] 09 **An auditor reaches the proof without a separate project.**
  Read-only access, limited in time.
  GOOD PRACTICE

TEST AND RESPOND

- [ ] 10 **No change reaches production untested.**
  The same questions, asked again at every change.
  DORA 24
  AI ACT 15

- [ ] 11 **Someone tries to fool the agent, on purpose.**
  Prompt injection, data leaks.
  DORA 24
  OWASP

- [ ] 12 **An agent failure enters the incident process.**
  With reporting deadlines defined.
  DORA 17, 19

> Where to start: points 1, 5 and 7. Without an inventory, approval and a record, the others do not hold.

HOW BLUE FALNOA RESPONDS

THE SAME FOUR VERBS, IN ONE APPLICATION

Blue Falnoa is the application where people supervise the AI agents their business runs. It connects to the agents you already have.

KNOW

- **Register of AI systems**: every agent with owner, purpose, model, data and risk class.
- **Register of ICT and AI suppliers**: criticality, location, contract end, exit plan. Exports to a spreadsheet.

CONTROL

- **Action gateway**: the agent asks before it acts and waits for the decision.
- **Rules by amount, risk, time of day and action**, with two-person approval and a written reason.
- **Emergency stop**: suspends every agent at once.

PROVE

- **Chained audit log**: an altered copy is detected.
- **Signed seals** that can be verified outside the application, offline.
- **Auditor portal**: a read-only account that ends on its own.

TEST

- **Evaluations and release gates**: a version is released only above a score floor.
- **Adversarial campaigns**: injection, prompt leak, secret extraction.
- **Incident log** with a reporting clock and editable deadlines.

One instance per customer, in the customer's infrastructure. Interface in English and Portuguese.

HONESTLY

WHAT BLUE FALNOA IS NOT

✕

It is not a certification

Falnoa holds no SOC 2 report and no ISO 27001 certificate. No external penetration test has been done yet.

✕

It is not legal advice

The application organises control and proof. Whether that meets a given obligation is for each entity to decide with its counsel.

✕

It does not control what does not ask

The gateway is a control point for the agents that call it. Connecting each agent is part of the work.

✕

It is not proven everywhere

We publish what was verified for real, what only has automated tests and what was not done.

> The status ledger is public: falnoa.com/en/trust/status-ledger

SOURCES

WHERE TO CHECK

1 Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Arts. 5, 8, 17, 19, 24, 28 and 64.
https://eur-lex.europa.eu/eli/reg/2022/2554/oj

2 Implementing Regulation (EU) 2024/2956, standard templates for the register of information.
https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj

3 Regulation (EU) 2024/1689, the Artificial Intelligence Act. Arts. 3, 12, 14, 15, 26, 27, 50, 113 and Annex III.
https://eur-lex.europa.eu/eli/reg/2024/1689/oj

4 Regulation (EU) 2026/1744 amending Regulation (EU) 2024/1689 (Digital Omnibus on AI).
https://eur-lex.europa.eu/eli/reg/2026/1744/oj

5 European Commission, "AI Act", application timeline. Accessed 13 November 2026.
https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

6 Regulation (EU) 2016/679 (GDPR), Art. 22.
https://eur-lex.europa.eu/eli/reg/2016/679/oj

7 OWASP Top 10 for LLM Applications 2025, LLM06:2025 Excessive Agency.
https://genai.owasp.org/llmrisk/llm062025-excessive-agency/

This guide summarises legal texts in plain language and is not legal advice. Article references are pointers for reading. Always check the consolidated version in force and your own counsel. The links drawn between DORA and AI agents are Falnoa's reading, not the position of any authority. No rule names Blue Falnoa and Falnoa holds no certification. Regulatory facts checked on 13 November 2026.

WANT TO SEE IT WORKING?

falnoa.com/en/products/blue-falnoa
hello@falnoa.com

© 2026 Falnoa