

GOVERNANCE DOCS

EU Artificial Intelligence Act

Gap Assessment Report

EU Artificial Intelligence Act (Regulation (EU) 2024/1689)

Veritas HR Screening (sample)

The CV screening and interview scoring system offered to employers in the EU, and the general-purpose models it relies on.

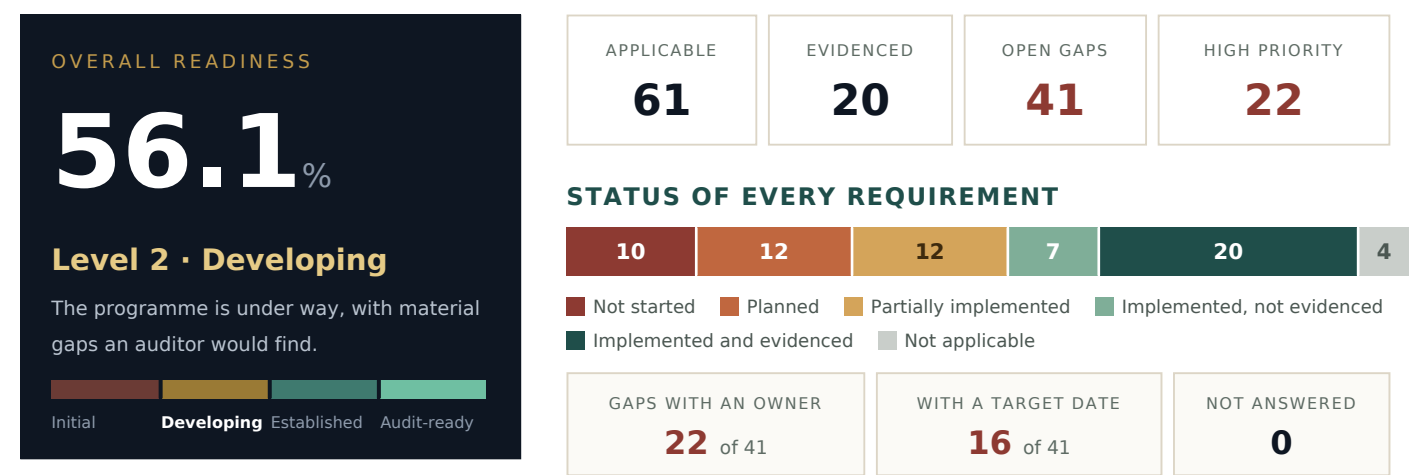
ASSESSED	25 September 2026
EDITION	Regulation (EU) 2024/1689, as amended by Regulation (EU) 2026/1744
IN SCOPE	65 requirements, 61 applicable
PROFILE	Technology, software and SaaS · 50 to 249 people
PREPARED BY	Governance Docs

CONTENTS

- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Veritas HR Screening (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Veritas HR Screening (sample) stands against EU AI Act



WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 56.1% against EU AI Act across 61 applicable controls. 20 of them are implemented and evidenced.
- Most open gaps: Prohibited practices (in force), with 8 at 28%. Strongest area: AI literacy (in force) at 100%.
- 7 controls are operating but not evidenced. Collecting their records alone lifts the score to 59.0% (+2.9 points), the cheapest gain available.
- 22 gaps are high priority (not started or only planned); 5 of them are in Prohibited practices (in force).

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 5 high-priority gaps in Prohibited practices (in force)	HR Manager	Prohibited AI Practices Screening Procedure
2	MEDIUM	Adopt and tailor the Prohibited AI Practices Screening Procedure, which closes 6 open gaps	To assign	Prohibited AI Practices Screening Procedure
3	LOW	Evidence the 7 controls that already operate (+2.9 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

You stand at 56.1% readiness and must immediately screen systems for prohibited practices and formalize risk classification.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

The organization has achieved an overall readiness score of 56.1%, placing us at the Developing stage with 41 open gaps. Our primary vulnerability lies in areas that are already in force, notably prohibited practices and transparency obligations, where readiness is under 30%. To eliminate critical exposure, management needs board backing to assign formal owners and target completion dates for all 22 high-priority gaps. We must direct internal resources toward immediate operational screening and classification across all active AI systems.

WHERE YOU STAND

Your self-assessment against the EU Artificial Intelligence Act places the organization at 56.1% overall readiness, which corresponds to level 2 of 4, or Developing. Out of 61 applicable requirements, there are 41 open gaps, with 22 classified as high priority. While 20 requirements are implemented and evidenced, 10 have not started and 12 remain planned. Strengths appear in areas like AI literacy at 100% and high-risk provider requirements at 90%. However, critical areas in force lag behind, including transparency obligations at 25% and prohibited practices at 28.1%.

WHAT IT MEANS FOR THE ORGANIZATION

The assessment shows that governance mechanisms are functioning in pockets, but substantial operational risks remain unaddressed. Crucially, areas that are already in force, such as prohibited practices and general-purpose AI models, show low completion rates of 28.1% and 35.7%. Currently, only 22 gaps have an assigned owner and 16 have a target date. Without assigned ownership across all 41 open gaps, execution will stall. Material gaps remain that an external auditor would identify, leaving the organization exposed across foundational compliance obligations.

WHERE TO FOCUS FIRST

Immediate attention must turn to screening existing systems against prohibited practices to prevent illicit deployments. Your next priority is establishing procedures for AI risk classification and general-purpose AI model obligations. Addressing items that are partially implemented or planned will significantly lift your position; completing what is planned raises your score to 83.6%, and finishing what is partly in place reaches 68.9%. Begin by implementing the screening and classification procedures that address the largest clusters of high-priority gaps across your systems.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Screen systems against prohibited AI practices 5.1c Social scoring · 5.1e Untargeted facial scraping · 5.1a Manipulative and deceptive techniques	Unchecked systems risk violating requirements that are already in force. Deploying prohibited practices creates severe operational and legal vulnerability.	Draft the screening procedure to evaluate active software against banned manipulative techniques, social scoring, and biometric scraping.	Prohibited AI Practices Screening Procedure Comprehensive EU AI Act Toolkit – 60 Compliance Templates	30 DAYS
2 Implement AI risk classification and trigger procedures 6.1 Annex I high-risk · RC.6 Reclassification triggers · 6.3 Derogation assessment	Failing to classify systems accurately leaves high-risk systems unmanaged. It also prevents the organization from tracking mandatory conformity requirements.	Define operational criteria and derogation workflows within a formal risk classification procedure.	AI Risk Classification Procedure Comprehensive EU AI Act Toolkit – 60 Compliance Templates	30 DAYS
3 Establish transparency and synthetic content disclosure mechanisms 50.5 Clear and accessible disclosure · 50.2 Marking synthetic content · 50.1 Disclosing human-AI interaction	Transparency rules are in force and require clear disclosure to users interacting with AI. Non-compliance exposes user-facing software to immediate regulatory challenge.	Create standard disclosure notices for user interactions and establish synthetic content marking guidelines.	AI Transparency Policy Comprehensive EU AI Act Toolkit – 60 Compliance Templates	60 DAYS
4 Operationalize general-purpose AI model compliance obligations 51 GPAI model classification · 55 Systemic risk obligations · 53.1b Information to downstream providers	General-purpose AI rules are in force and require systemic risk evaluation. Downstream transparency is mandatory for models provided to partners.	Adopt a systemic risk assessment workflow to evaluate model classification thresholds and downstream information flows.	GPAI Systemic Risk Assessment Procedure (Article 55) Comprehensive EU AI Act Toolkit – 60 Compliance Templates	60 DAYS
5 Establish conformity assessment and post-market monitoring controls 43 Conformity assessment · 49 EU database registration · 72 Post-market monitoring	High-risk systems require formal conformity assessment and EU database registration before deployment. Ongoing monitoring is essential to catch incidents post-release.	Draft a conformity assessment procedure and set up templates for post-market monitoring plans.	Conformity Assessment Procedure (Article 43) Comprehensive EU AI Act Toolkit – 60 Compliance Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Roll out the Prohibited AI Practices Screening Procedure across active software deployments.
- Adopt the AI Risk Classification Procedure to review Annex I and Annex III applicability.
- Assign accountable owners and completion deadlines to all 22 high priority gaps.

DAYS 31 TO 60

- Publish the AI Transparency Policy and implement disclosure notices for human-AI interaction.
- Establish systemic risk assessment procedures for general-purpose AI models.
- Gather operational evidence for the 7 requirements currently marked as implemented but unevidenced.

DAYS 61 TO 90

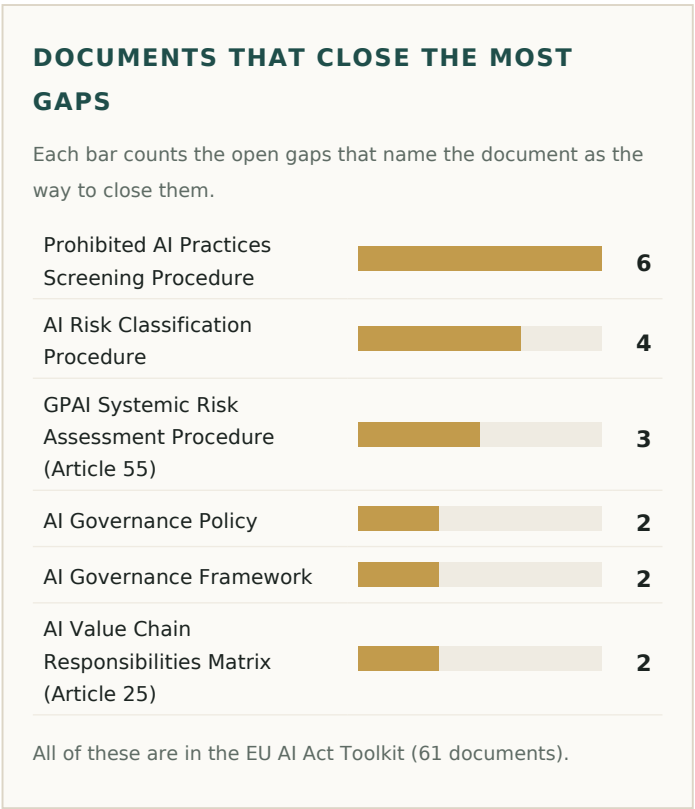
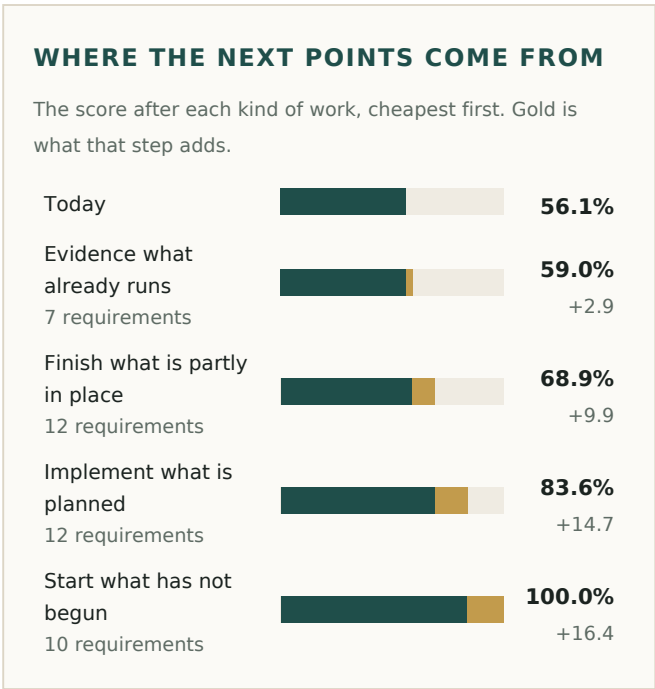
- Formalize the Conformity Assessment Procedure and prepare registration workflows for the EU database.
- Complete implementation for all 12 items currently in planned status.
- Deploy the Post-Market Monitoring Policy and activate serious incident reporting procedures.

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Scope, roles and inventory	3 1 3	64%	3 0 1
AI literacy (in force)	2	100%	0 0 0
Prohibited practices (in force)	2 3 3 1	28%	5 3 0
Risk classification	2 2 1 1	33%	4 1 0
Transparency obligations (in force)	1 1 1 2	25%	2 1 0
General-purpose AI models (in force)	2 2 2 1	36%	4 2 0
High-risk: provider requirements	4 6	90%	0 0 4
High-risk: conformity and post-market	2 3 1	42%	2 3 0
Deployer obligations	1 1 1 5	81%	1 1 1
Governance and enforcement	1 1 1 1 1	56%	1 1 1

Not started Planned Partially implemented Implemented, not evidenced Implemented and evidenced Not applicable



Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 10

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
5.1c	Social scoring	Prohibited practices (in force)	Operations Manager 21 Jan 2027	Prohibited AI Practices Screening Procedure
5.1e	Untargeted facial scraping	Prohibited practices (in force)	To assign	Prohibited AI Practices Screening Procedure
6.1	Annex I high-risk	Risk classification	Operations Manager 4 Feb 2027	AI Risk Classification Policy · AI Risk Classification Procedure
RC.6	Reclassification triggers	Risk classification	To assign	AI Risk Classification Procedure · AI Value Chain Responsibilities Matrix (Article 25)
50.5	Clear and accessible disclosure	Transparency obligations (in force)	Risk Manager 4 Feb 2027	AI Transparency Policy
51	GPAI model classification	General-purpose AI models (in force)	Operations Manager 26 Nov 2026	General-Purpose AI Model Compliance Policy · GPAI Systemic Risk Assessment Procedure (Article 55)
55	Systemic risk obligations	General-purpose AI models (in force)	Risk Manager	GPAI Systemic Risk Assessment Procedure (Article 55)
43	Conformity assessment	High-risk: conformity and post-market	To assign	Conformity Assessment Policy · Conformity Assessment Procedure (Article 43)
49	EU database registration	High-risk: conformity and post-market	To assign	EU Database Registration Procedure (Article 49)
99	Penalty exposure understood	Governance and enforcement	Compliance Lead 10 Dec 2026	AI Governance Policy · EU Artificial Intelligence Act — Regulation Reference Guide

HIGH Planned · 12

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
SR.1	Territorial scope	Scope, roles and inventory	To assign	AI Governance Policy · AI Governance Framework
SR.3	AI system inventory	Scope, roles and inventory	Compliance Lead	AI System Inventory & Register

SR.6	Authorised representative	Scope, roles and inventory	To assign	Provider Obligations Procedure (Article 16)
5.1a	Manipulative and deceptive techniques	Prohibited practices (in force)	HR Manager 10 Dec 2026	Prohibited AI Practices Screening Procedure · Prohibited AI Practices Assessment Checklist
5.1ba	Non-consensual intimate imagery	Prohibited practices (in force)	Operations Manager 24 Dec 2026	Prohibited AI Practices Policy · Prohibited AI Practices Screening Procedure
5.1g	Sensitive biometric categorisation	Prohibited practices (in force)	To assign	Prohibited AI Practices Screening Procedure
6.3	Derogation assessment	Risk classification	Compliance Lead 4 Feb 2027	AI Risk Classification Procedure
6.1a	Safety component carve-outs	Risk classification	Compliance Lead 21 Jan 2027	AI Risk Classification Policy
50.2	Marking synthetic content	Transparency obligations (in force)	To assign	Transparency Obligations Procedure (Article 50)
53.1b	Information to downstream providers	General-purpose AI models (in force)	Compliance Lead 26 Nov 2026	GPAI Model Obligations Procedure (Article 53)
53.1c	Copyright and text and data mining policy	General-purpose AI models (in force)	To assign	General-Purpose AI Model Compliance Policy
26.2	Competent human oversight	Deployer obligations	IT Manager 4 Feb 2027	Human Oversight Roles & Competency Matrix · Deployer Obligations Procedure (Article 26)

MEDIUM Partially implemented · 12

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
5.1b	Exploiting vulnerabilities	Prohibited practices (in force)	HR Manager 7 Jan 2027	Prohibited AI Practices Screening Procedure
5.1bb	Child sexual abuse material	Prohibited practices (in force)	HR Manager 12 Nov 2026	Prohibited AI Practices Policy
5.1f	Emotion inference at work and school	Prohibited practices (in force)	HR Manager 21 Jan 2027	Prohibited AI Practices Assessment Checklist
6.2	Annex III high-risk	Risk classification	Risk Manager 4 Feb 2027	AI Risk Classification Procedure · High-Risk AI System Requirements Checklist
50.1	Disclosing human-AI interaction	Transparency obligations (in force)	To assign	AI Transparency Policy · AI System Disclosure Notice Template
52	Notification to the AI Office	General-purpose AI models (in force)	To assign	GPAI Systemic Risk Assessment Procedure (Article 55)
53.1a	GPAI technical documentation	General-purpose AI models (in force)	To assign	GPAI Technical Documentation Template · GPAI Model Obligations Procedure (Article 53)

47	EU declaration of conformity	High-risk: conformity and post-market	Risk Manager	EU Declaration of Conformity Template (Article 47)
72	Post-market monitoring	High-risk: conformity and post-market	IT Manager	Post-Market Monitoring Policy · Post-Market Monitoring Plan Template (Article 72)
73	Serious incident reporting	High-risk: conformity and post-market	HR Manager 12 Nov 2026	Serious Incident Reporting Procedure (Article 73) · Serious Incident Report Template +1 more
27	Fundamental rights impact assessment	Deployer obligations	Compliance Lead	Fundamental Rights Impact Assessment Procedure (Article 27) · Fundamental Rights Impact Assessment Template
GE.2	Ethics and responsible use	Governance and enforcement	HR Manager	AI Ethics & Responsible Use Policy

LOW Implemented, not evidenced · 7

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
SR.4	Operator role per system	Scope, roles and inventory	To assign	AI Value Chain Responsibilities Matrix (Article 25) · Provider Obligations Procedure (Article 16)
10.bias	Bias detection and mitigation	High-risk: provider requirements	To assign	Bias Detection & Mitigation Procedure · Data Quality Assessment Template
13	Transparency and instructions for use	High-risk: provider requirements	To assign	Instructions for Use Template (Article 13)
14	Human oversight	High-risk: provider requirements	To assign	Human Oversight Policy (Article 14) · Human Oversight Procedure & Controls +1 more
17	Quality management system	High-risk: provider requirements	To assign	Quality Management System for AI Procedure (Article 17)
26.11	Informing affected individuals	Deployer obligations	To assign	Deployer Obligations Procedure (Article 26) · AI System Disclosure Notice Template
GE.1	AI governance and accountability	Governance and enforcement	To assign	AI Governance Framework · AI Governance Roles & Responsibilities (RACI Matrix)

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com