EXECUTIVE & SECURITY OVERVIEW

Understanding Your Systemores AI Compliance Dossier

Before an autonomous AI agent interacts with customers, makes underwriting or hiring recommendations, or triggers company APIs, leaders need objective proof that it will behave safely, fairly, and predictably. Every Systemores Compliance Dossier evaluates an agent across **four independent governance pillars (0–100)** plus a safeguarded **Overall Score**.

4 Pillar Scores (0–100)
Independent lenses for Legal, Risk Ops, Fairness Compliance & InfoSec/CISO teams.

80+ Weakest-Link Gate
A green **CERTIFIED** status requires an 80+ average *and* 80+ on every single pillar.

Zero-Retention + SHA-256
Prompts, schemas, and traces run strictly in memory—never stored or used to train models.

LIVE REFERENCE SPECIMEN • DOS-SYSTEMORES-REFERENCE
Overall Score: 95 / 100 CERTIFIED

EU AI ACT	NIST RMF	EEOC/ECOA	SOC 2 AI
96	95	97	92

1 The 4 Regulatory & Security Pillar Scores (0–100)

Distinct enterprise lenses — zero cross-masking

PILLAR 01 • EU 2024/1689 — Legal & Policy

EU AI Act — Behavioral Boundaries & Human Oversight

"Can users trick, pressure, or flatter this AI into breaking its rules—and does it know when to hand off to a human?"

What it measures: Guardrail rigidity under adversarial Murray Needs-Press stress tests, resistance to *sycophancy* (agreeing with false premises under pressure), clear AI transparency, and supervisor escalation (Arts. 13–14).

Why it matters: Proves readiness under Europe's flagship AI law while stopping agents from inventing policies, making unauthorized promises, or folding under prompt injection.

PILLAR 02 • NIST AI RMF 1.0 — Risk & Engineering Ops

NIST AI RMF 1.0 — Reliability, Drift & Operational Control

"Does this AI stay calm, dependable, and cost-controlled over long, messy, real-world conversations?"

What it measures: Alignment with `GOVERN` • `MAP` • `MEASURE` • `MANAGE`: 10+ turn persona drift resistance, behavioral persistence, graceful recovery during API/tool failures, and OpenTelemetry loop/cost-burn checks.

Why it matters: Most failures happen mid-session or during outages—not on turn #1. A strong score proves consistent, financially predictable production behavior.

PILLAR 03 • EEOC / ECOA — Compliance & Brand

EEOC / ECOA Fairness — Non-Discrimination & Objectivity

"Does this AI treat every person fairly and objectively—without overt bias or hidden demographic shortcuts?"

What it measures: Statutory fairness across hiring (EEOC), fair lending (ECOA), and housing criteria. Verifies calm impartiality and blocks subtle proxy shortcuts like ZIP codes or neighborhoods when primary data is sparse.

Why it matters: Essential for fintech, lending, HR, healthcare, and customer support—reducing disparate-impact legal exposure by anchoring decisions to objective facts.

PILLAR 04 • SOC 2 TYPE II AI — CISO & InfoSec

SOC 2 AI Addendum — Security & Tool-Access Guardrails

"When connected to real APIs, databases, and sub-agents, does this AI stay strictly inside its security lane?"

What it measures: Least-privilege discipline, MCP 2026 tool schema safety (catching injection risks or destructive tools mislabeled as `readOnlyHint: true`), input skepticism, and multi-agent privilege checks blocking `public → admin` escalation.

Why it matters: Answers InfoSec's #1 question: verifying autonomous tool actions won't leak credentials, corrupt databases, or bypass access controls.

2 The Overall Score (Average) & Certification Status Matrix

Rounded mean of the 4 pillars, gated by per-pillar minimums

The **Overall Score (0–100)** displayed at the top of every dossier and on the Systemores Trust Badge is the rounded average of the four pillar scores. It gives executives and procurement teams a single trackable benchmark across releases—paired with three clear deployment verdicts:

SCORE BAND	PILLAR RATING	CERTIFICATION STATUS	WHAT IT MEANS FOR PRODUCTION DEPLOYMENT
80 – 100	PASS	**CERTIFIED** *(Green Badge)*	**Production-Ready:** Overall average is **80+** *and* **every single evaluated pillar independently scored 80+**. Ready for customer-facing rollout and enterprise procurement sign-off.
60 – 79	REVIEW	**CONDITIONAL APPROVAL** *(Amber)*	**Controlled Rollout:** Every pillar meets the **60+** floor, but one or more scored **60–79**. Suitable for supervised pilots while flagged controls are tightened prior to full certification.
0 – 59	FAIL	**NON-COMPLIANT** *(Red Alert)*	**Hold & Remediate:** Triggered whenever the overall average is below **60**, *or* if **even one individual pillar dropped below 60**. Deployment must wait until gaps are fixed.

WHY THE OVERALL AVERAGE CAN'T BE "GAMED" — THE WEAKEST-LINK SAFEGUARD

Zero Blind-Spot Rule

Traditional averages allow three strong categories to hide a dangerous flaw. Systemores enforces a strict weakest-link gate: a high mathematical average never grants `CERTIFIED` status if any pillar fails its minimum threshold.

`EU AI Act: 95 (PASS)` `NIST RMF: 95 (PASS)` `EEOC / ECOA: 95 (PASS)` `SOC 2 Tool Security: 50 (FAIL)`

NAIVE MATHEMATICAL AVERAGE

84 / 100

Looks like a reassuring "B / A-" on paper—masking an unguarded database or admin tool vulnerability.

SYSTEMORES OFFICIAL VERDICT

NON-COMPLIANT

Automatically blocks certification because SOC 2 fell below 60. When buyers see green **CERTIFIED**, every pillar cleared 80+.

3 Why Prospective Clients & Partners Trust the Dossier

Standardized proof designed for buyer legal, security & risk review

1. Faster Enterprise Procurement

Legal (EU AI Act / EEOC-ECOA), Risk & Ops (NIST AI RMF), and InfoSec (SOC 2 AI) each get their exact domain scored in one concise report instead of weeks of custom questionnaires.

2. Tamper-Evident Cryptographic Proof

Every dossier publishes a unique `/verify/dos-...` certificate URL and embeddable SVG Trust Badge backed by a signed SHA-256 integrity hash for one-click verification.

3. Zero-Retention IP Confidentiality

Proprietary system prompts, internal MCP tool schemas, and OpenTelemetry traces are evaluated strictly in memory (`zeroRetentionVerified: true`) and never stored or trained on.

4. 7 Global Locales + <250ms Runtime Defense

Share localized certificates across EN, ES, DE, FR, PT, JA, and ZH with an invariant hash, and pair pre-deploy dossiers with **System One** live inline circuit-breaking.

READY TO CERTIFY YOUR AI AGENTS?

Inspect Our Live Reference Dossier or Audit a Prompt Today

Run pre-deployment behavioral audits in the Playground, wire our 12-tool MCP 2026 server into your IDE or CI/CD pipeline, or schedule a partner compliance walkthrough.

audit.systemores.com/docs/dossier-guide
audit.systemores.com/verify/dos-systemores-reference
github.com/bobcar0/systemores-plugin
hello@systemores.com

© 2026 Systemores LLC • Liberty Hill, TX • Texas Governing Law