CERTIFIED

Information Security™

CIS Assessment System

Solution Brief and User Guide

Version 2.5.42.11 | May 2026

Compliance, Cyber, AI Risk, & ERM Assessment Platform

ISO/IEC 42001:2023 | ISO/IEC 27001:2022 | NIST AI RMF 1.0 | NIST CSF 2.0 | ISO 31000 ERM Family

Certified Information Security

www.certifiedinfosec.com

Document series: User Guide -- published at each governed release

1. What the CIS Assessment System is

The CIS Assessment System is a free, public-facing tool that measures an organization's current state against five internationally recognized risk and security frameworks: ISO 27001, ISO 42001, ISO 31000 ERM Family, NIST CSF 2.0, and NIST AI RMF. It runs as a Joomla 5 component at https://www.certifiedinfosec.com/assessments and requires no software installation on the assessor machine.

The system exists to serve a specific conversion thesis: equip practitioners to discover their own control gaps with precision, then connect them to the executive training that closes those gaps. Every architectural and content decision in this tool serves that thesis.

2. Who this guide is for

This guide addresses the full range of people who use or evaluate the CIS Assessment System. Senior managers and risk officers need to understand what the tool produces and why. Assessors run the tool directly against a framework. AI and cyber executives evaluate fit against their organization's governance needs. Training students arrive at the tool as a prerequisite to or companion for Allen Keele executive training programs.

The Admin Guide (Technical Design) addresses build engineers, integrators, and deployment operators. Its content is not repeated here.

3. Assessment experience

When an assessor opens the system, they select one of the five active frameworks. The tool presents every control or subcategory in that framework with a scored response interface. For conformance-mode frameworks (ISO 27001, ISO 42001), assessors select among Major Non-Conformance, Minor Non-Conformance, Opportunity for Improvement, and Satisfactory Conformance. For maturity-mode frameworks (ISO 31000 ERM Family, NIST CSF 2.0, NIST AI RMF), they select among the maturity levels defined by the framework scoring model.

The tool derives a T1 top-level score from the distribution of T2 control responses. A conformance-ceiling rule prevents a high T1 rating from coexisting with a floor of materially low T2 scores -- the composite score reflects the realistic aggregate, not the optimistic average alone. An uneven-maturity banner alerts the assessor when the spread across controls is large enough to warrant independent attention.

At any point during the assessment, the right-rail navigator shows which controls remain incomplete. Assessors can save progress and return; the session-lifecycle heartbeat maintains connection state and warns before the session expires. All previously generated assessment records and saved progress persist across sessions.

4. Scoring integrity -- floor-rule conformance (v2.5.42.11)

v2.5.42.11 corrects a persistence-layer defect that could cause a stale T1 conformance or maturity band to persist on the Results page and in the PDF report after an assessor re-scored T2 controls downward. The scoring engine itself was always correct: the weakest-link cap and floor-rule logic embedded in the shared scoring model applied the correct ceiling at computation time. The defect was in the persistence layer -- when T2 responses were saved, the previously persisted T1 value was not recapped to reflect the more restrictive new cap.

The practical consequence for assessors: if a T2 re-score produced a lower minimum T2 value, the displayed Tier 1 conformance band or maturity band could show a level higher than the scoring model permitted for that T2 floor. After v2.5.42.11, any T2 re-score that produces a more restrictive cap will silently re-cap the T1 value in the same transaction, clear any stale override flag, and recompute the risk fields. Assessors do not need to take any action. Assessments that were completed under v2.5.42.10 or earlier should be reviewed if they were saved after a T2 re-score; re-opening and saving any such assessment will trigger the re-cap automatically.

This correction applies to all five frameworks. The floor-rule engine is shared across ISO 27001, ISO 42001, ISO 31000 ERM Family, NIST CSF 2.0, and NIST AI RMF. The defect was first identified in the NIST AI RMF context, but the persistence bug affected the entire framework set.

5. Workspace change -- evidence attachment panel removed (v2.5.42.11)

The Assess workspace previously displayed a per-control evidence-attachment panel that allowed file uploads to be associated with individual controls. This panel has been removed entirely in v2.5.42.11.

The feature was not part of the authorised scope for the CIS Assessment System. It was introduced without explicit authorisation and has been eliminated. The evidence-attachment upload table in the database is dropped automatically on upgrade to v2.5.42.11.

No assessor action is required. Existing assessments are not affected beyond the removal of the attachment panel itself. Assessment records, saved T2 responses, T1 conformance or maturity bands, evidence notes, and PDF report generation are all unaffected. Any files previously uploaded via the attachment panel were purged from production storage before this release.

The removal simplifies the workspace interface. The control inventory, scoring interface, and evidence-note fields continue to operate as before.

6. Frameworks covered

ISO 27001 -- Information Security Management System. Annex A of ISO/IEC 27001:2022 provides 93 controls across four themes: organizational controls, people controls, physical controls, and technological controls. The CIS Assessment System implements all 93 controls with per-control evidence guidance drawn from ISO 27001:2022 Annex A directly.

ISO 42001 -- AI Management System. ISO/IEC 42001:2023 Annex A provides 38 controls across ten domains, covering AI system design, data governance, risk management, and responsible AI objectives. The assessment aligns to the normative control inventory in Table A.1 of the published standard.

ISO 31000 ERM Family. The ISO 31000 Enterprise Risk Management family is delivered as a unified composite framework drawing from ISO 31000:2018 (risk management principles and guidelines), ISO 23894 (AI risk guidance), ISO 31010 (risk assessment techniques), and ISO 27005:2022 (information security risk management). The composite presents 23 clauses covering principles, framework, and process across all four source standards.

NIST CSF 2.0 -- Cybersecurity Framework. NIST CSF 2.0 provides six Functions (Govern, Identify, Protect, Detect, Respond, Recover), 22 Categories, and 106 Subcategories with 363 Implementation Examples. The CIS Assessment System covers all 106 Subcategories.

NIST AI RMF -- AI Risk Management Framework. The NIST AI Risk Management Framework provides 72 subcategories across four Functions: Govern, Map, Measure, and Manage. The assessment includes Suggested Actions drawn from NIST AI 600-1 where the T2 maturity average meets the configured threshold.

7. Output: PDF assessment report

When the assessor concludes their work, the tool generates a PDF assessment report. The report includes a cover page showing the framework, assessed organization name, assessor role, and assessment date. The body delivers:

- A T1 conformance or maturity summary with color-coded status band
- Per-grouping distribution charts showing the spread of T2 responses
- Detailed per-control records with the assessor selected response and any evidence notes
- A Suggested Actions section (maturity-mode frameworks) ordered by priority
- An Evidence Companion Guide cross-referencing the control inventory against evidence categories
- A Training appendix with course options relevant to the framework assessed

Reports are downloadable as PDF files and optionally emailed to the assessor's registered address. The filename prefix is framework-specific, derived from the report.filePrefix field in the framework JSON.

8. Assessment-to-training pathway

The CIS Assessment System surfaces, with precision, the specific control gaps that Allen Keele executive training programs address. That connection is not incidental -- it is the point of the tool. An assessor who scores Major Non-Conformance on ISO 42001 Clause A.6 AI system data management, or who rates NIST AI RMF GOVERN 1.2 at Maturity Level 1, leaves the tool with documentary evidence of where they stand and a clear path to the training that closes the gap.

Allen Keele executive training programs cover ISO 31000 enterprise risk management, ISO 42001 AI management, NIST AI Risk Management Framework, NIST CSF 2.0, and ISO 27001 information security management. The training is positioned at the executive practitioner level -- practitioners who need to build and lead these programs, not merely be aware of them.

Each framework Training appendix in the PDF report contains card-level descriptions of the relevant training programs and direct enrollment contact information.

9. Install and validation

Install the current release zip via Joomla Extensions > Manage > Install. The confirmation banner reads: CIS Assessment System updated to the current version successfully. Confirm the version chip in Joomla admin > Components > CIS Assessment System matches the installed version.

Open any in-progress assessment and confirm the workspace loads without error. Perform one save and confirm it completes normally. Confirm the evidence attachment panel no longer appears in the Assess workspace.

Rollback is instant: re-install the prior release zip. Note that the database upgrade to v2.5.42.11 drops the attachments table; rollback to a prior version after this upgrade will not restore that table. All other tables are unaffected.

10. Release cadence

The CIS Assessment System is released on a continuous-improvement cadence governed by the project release process. Each release passes a gate triple (automated quality, security audit, and build verification) before deployment to production. Release history, including version numbers, dates, and per-release change summaries, is documented in the Technical Design (Admin Guide) and the PROJECT_CONFIG change log.

The Admin Guide (Technical Design) covers build procedures, file-by-file change records, gate-triple specifications, schema delta, and rollback procedures for each release.