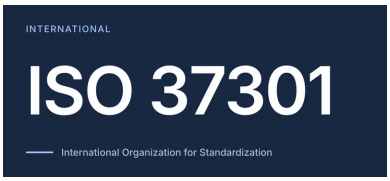
SmartSuite

Framework / Risk Management / ISO Management Systems

ISO 37301:2021 – Compliance Management Systems – Requirements with Guidance for Use

ISO 37301:2021 sets requirements, with guidance, for a compliance management system: obligations, risk, culture, concerns, audit and improvement. ISO published it on April 13, 2021.



What it is

ISO 37301:2021, Compliance management systems — Requirements with guidance for use, is the international standard for establishing, developing, implementing, evaluating, maintaining and improving an effective compliance management system (CMS). The International Organization for Standardization (ISO) published the first edition on April 13, 2021 through technical committee ISO/TC 309, Governance of organizations. It replaces ISO 19600:2014, which gave guidelines only, and it applies to all types of organizations in the public, private and non-profit sectors (Clause 1).

The standard contains requirements, marked "shall", with guidance for use in informative Annex A, and it follows the harmonized structure for ISO management system standards. Its Introduction describes compliance as an ongoing process and the outcome of an organization meeting its obligations, made sustainable by embedding it in culture, and notes that in a number of jurisdictions courts have considered an organization's commitment to compliance through its CMS when determining the penalty for contraventions of relevant laws.

At a glance

PUBLISHER International Organization for Standardization (ISO), ISO/TC 309	TYPE Standard	VERSION ISO 37301:2021 (first edition), with Amendment 1:2024
EFFECTIVE April 13, 2021 (publication date)	DOMAIN Risk Management	FAMILY ISO Management Systems
REGION International	ADOPTION MODEL Certification	IMPLEMENTATION COMPLEXITY Medium

Source: iso.org/standard/75080.html

Why it matters

- **Compliance as culture** The governing body and top management establish and uphold a compliance culture and compliance governance (Clauses 5.1.1 to 5.1.3), and personnel and management have defined responsibilities (Clauses 5.3.3 and 5.3.4).
- **Obligations and risk in one view** The organization determines its compliance obligations (Clause 4.5) and assesses compliance risk (Clause 4.6), so effort follows the obligations most likely to be breached.
- **A route for concerns** Clause 8.3 requires a process for raising concerns and Clause 8.4 requires investigation processes, so suspected noncompliance reaches someone who can act.
- **Evidence for regulators and courts** Compliance reporting and record-keeping (Clauses 9.1.4 and 9.1.5) produce the evidence an organization can show when its commitment to compliance is examined.

How SmartSuite supports ISO 37301:2021

Compliance Obligations Register

Hold the laws, regulatory requirements, industry codes and other commitments that apply, with their sources, owners and review dates (Clause 4.5).

Compliance Risk Assessment

Rate the compliance risk of each obligation and link it to the controls, owners and treatment actions that address it (Clauses 4.6 and 6.1).

Policy, Roles and Governance

Record the compliance policy, the responsibilities of the governing body, top management, the compliance function, management and personnel, and the approvals they give (Clauses 5.2 and 5.3).

Controls, Concerns and Investigations

Track controls and procedures, concerns raised and investigations from intake to outcome (Clauses 8.2 to 8.4).

Monitoring and Internal Audit

Plan indicators and internal audits, record findings and follow nonconformities to closure (Clauses 9.1, 9.2 and 10.2).

Management Review and Reporting

Prepare management review inputs and results and report compliance performance to the governing body and top management (Clauses 9.1.4 and 9.3).

Common framework mappings

ISO 9001:2026 | ISO 27001:2022 | ISO 22301 | ISO 42001 | ISO 31000:2018 | COSO IC 2013 | COSO ERM 2017 | SOX

Official resources

ISO 37301:2021 catalog page

The ISO catalog entry with the standard's status, edition, committee, and purchase and preview options.

iso.org/standard/75080.html

ISO/TC 309 Governance of organizations

The ISO technical committee responsible for ISO 37301, ISO 37001, and the wider governance standards family.

iso.org/committee/6266703.html

ISO 37301:2021 preview on the Online Browsing Platform

ISO's read-only preview of the standard's foreword, introduction, scope, and terms.

iso.org/obp/ui/en/#iso:std:iso:37301:ed-1:v1:en

ISO 19600:2014 (withdrawn)

The catalog entry for the earlier compliance management guideline that ISO 37301 replaced.

iso.org/standard/62342.html

Frequently asked questions

What is ISO 37301 and what did it replace?

ISO 37301:2021 is the international standard for compliance management systems. ISO published the first edition on April 13, 2021 through ISO/TC 309 and it replaced ISO 19600:2014, which contained guidelines only. ISO confirmed the 2021 edition after a systematic review on August 3, 2026, and Amendment 1:2024 adds climate change considerations.

Can an organization be certified to ISO 37301?

Yes. Unlike ISO 19600, ISO 37301 contains requirements, so an internal or external auditor can assess a compliance management system against it (Clause 9.2), and an accredited certification body can issue a certificate. Certification is voluntary.

How does ISO 37301 differ from ISO 37001 and ISO 37302?

ISO 37001 addresses anti-bribery management systems specifically, while ISO 37301 covers the organization's whole range of compliance obligations. ISO 37302:2025 gives guidance on evaluating the effectiveness of a compliance management system and, per its scope, does not add to or change the requirements of ISO 37301.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What does ISO 37301 require of the governing body and the compliance function?

The governing body and top management must show commitment, uphold a compliance culture and set the compliance policy (Clauses 5.1 and 5.2), and their responsibilities, and those of the compliance function, management and personnel, are set out in Clause 5.3. Where there is no separate governing body, these requirements apply to top management (Clause 1).

What must an organization have in place to handle concerns and noncompliance?

Clause 8.2 requires controls and procedures, Clause 8.3 requires a process for raising concerns and Clause 8.4 requires investigation processes. Results feed monitoring, compliance reporting and internal audit (Clause 9) and corrective action (Clause 10.2). The standard notes that a nonconformity is not necessarily a noncompliance (Clause 3.16).

License included / downloadable: No ISO 37301:2021 is a copyrighted ISO standard sold by ISO and by national standards bodies; its text is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/iso-37301-2021-compliance-management-systems-cms