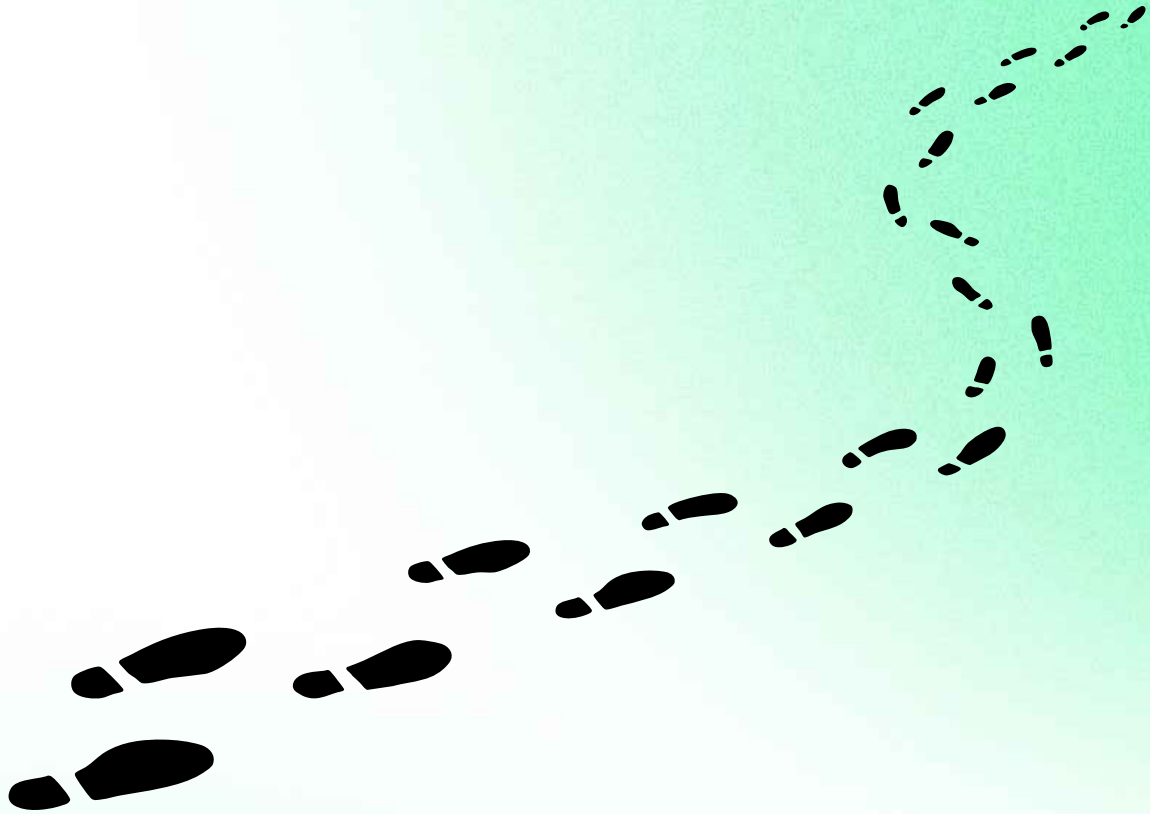
isms·online



No Shortcuts, Just Smart Steps

Your guide to SOC2 success

Build your SOC 2 management system and achieve compliance with minimal time, money and stress.

SOC 2

Public V2.0

So, you need to get SOC 2 certified?

Ensuring your organization meets SOC 2 requirements can feel overwhelming, but it doesn't have to be. This guide will break down the process step by step, helping you understand the framework, its benefits, and how to streamline your compliance journey

So, let's get going!

In this guide, we'll help you understand:

- The fundamentals of SOC 2 compliance
- What an effective SOC 2 management system looks like
- How you can achieve certification efficiently

Understanding SOC 2

The ISMS.online Solution

What is SOC 2?

SOC 2 compliance refers to the Service Organization Control 2 framework developed by the American Institute of Certified Public Accountants (AICPA).

SOC 2 is a security framework that defines how companies should manage, process, and store customer data based on the Trust Services Categories (TSC).

Unlike many frameworks, SOC 2 compliance is unique to each company. Organizations choose the relevant trust service categories applicable to their business and then design how they will meet the requirements of those categories instead of using a prescriptive list of controls. As a result, every organization's security practices will look different, meaning they can achieve SOC 2 compliance with custom policies and processes relevant to their business's operations

The Five Trust Service Categories

- **Security (mandatory)**
- **Processing Integrity**
- **Availability**
- **Confidentiality**
- **Privacy**

Why is SOC 2 Compliance Important?

While SOC 2 compliance is not a mandatory regulatory requirement, it holds immense significance as a widely accepted global compliance benchmark.

Adopting SOC 2 guidelines showcases an organization's commitment to maintaining high data security standards and establishes stakeholder trust.

Key benefits of SOC 2

Enhanced Data Security

SOC 2 compliance provides a robust framework for identifying and mitigating potential risks to sensitive data. Organizations can ensure the confidentiality, integrity, and availability of their systems and data by implementing and maintaining the necessary controls.

Competitive Edge and Market Differentiation

Achieving SOC 2 compliance establishes your organization as a trustworthy and secure partner and gives you a competitive advantage. It demonstrates your commitment to data protection and can serve as a differentiating factor when customers choose between service providers.

Strengthened Customer Trust

SOC 2 compliance assures customers that their data is handled with the highest level of security and confidentiality. By meeting the rigorous requirements of SOC 2, organizations can build trust and instil confidence in their customer base, leading to stronger relationships and long-term loyalty.

Streamlined Vendor Management

SOC 2 compliance is an essential criterion when evaluating potential vendors or partners. By selecting SOC 2-compliant partners, organizations can minimize the risk of data breaches and ensure that their data is in safe hands.

Regulatory Compliance Alignment

Many industry-specific regulations, such as HIPAA or GDPR, require organizations to implement appropriate controls and safeguards. SOC 2 compliance helps align with these regulatory requirements, streamlining the overall compliance process.

Understanding The Three Different SOC Certifications

The “SOC” family includes three types, each designed for different assurance objectives.

SOC 1

SOC 1 is for organizations whose internal security controls can impact a customer’s financial statements. Think payroll, claims, or payment processing companies. SOC 1 reports can assure customers that their financial information is being handled securely.

A SOC 1 report can either be Type 1 or Type 2. A Type 1 report assures an organization suitably designed and placed rules in operation as of a specified date. A Type 2 report provides those assurances and includes an opinion on whether the controls operated effectively throughout a period of time.

SOC 2

SOC 2 primarily evaluates information systems’ security, availability, processing integrity, confidentiality, and privacy, making it suitable for organizations that handle sensitive data.

The two types of SOC 2 reports are Type 1 and Type 2. A Type 1 report assesses the design of a company’s security controls at a specific time. In contrast, a Type 2 SOC report assesses those controls’ effectiveness over time.

SOC 2 reports are private, which means they are typically shared only with customers and prospects under an NDA.

SOC 3

SOC 3 provides a simplified version of SOC 2. It’s a general-use report that organizations can use as a marketing tool and provide to prospective customers.

Understanding the SOC 2 Trust Service Criteria

SOC 2 is based on the Trust Services Criteria (TSC), developed by the AICPA to assess five dimensions of trust in technology-driven service organizations.

Think of the TSC as the architectural blueprint.
The Common Criteria are the structural load-bearing beams.
Your controls? They're the bricks and steel.

Security

Security forms the foundation of any SOC 2 compliance framework. It must be included and is therefore often referred to as the 'common criteria'. It focuses on protecting systems and data against unauthorized access, both physically and logically.

Robust security controls, such as multifactor authentication, encryption, and regular security assessments, ensure sensitive information's confidentiality, integrity, and availability.

Availability

Availability ensures that systems and services are accessible and usable when needed. This criterion examines an organization's ability to prevent and respond to incidents that may disrupt its operations.

Redundant infrastructure, disaster recovery plans, and monitoring tools help maintain uninterrupted services, minimizing downtime and potential financial losses.

Organizations whose customers are concerned about downtime should select this criterion.

Processing Integrity

Processing integrity guarantees the accuracy, completeness, and validity of data processing. Organizations must have controls to ensure data is processed correctly and within defined parameters.

Examples of controls include data validation, error detection, and reconciliation procedures. By maintaining data integrity, organizations build trust and confidence in their operations.

Organizations should include this criterion if they execute critical customer operations such as financial processing, payroll services, and tax processing.

Confidentiality

Confidentiality ensures that sensitive information remains protected from unauthorized disclosure. Organizations must implement strict access controls, employee training programs, and encryption methods to safeguard confidential data.

Confidentiality controls also encompass contractual agreements and non-disclosure agreements to maintain the confidentiality of client information.

Organizations that store sensitive information protected by non-disclosure agreements (NDAs) or have customers with specific requirements about confidentiality should include this criterion.

Privacy

Privacy focuses on collecting, using, retaining, and disclosing personal information. Organizations must adhere to relevant privacy laws and regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA).

Implementing privacy controls involves obtaining consent for data collection, providing individuals with the right to access their information, and implementing measures to secure personal data.

Organizations that store PII such as healthcare data, dates of birth, and social security numbers or have customers holding this type of information should include this criterion.

Key takeaway

No matter which criteria you're evaluating, auditors will look at how effectively your controls are operating, how quickly you respond to risks or incidents, and how clearly you communicate about risks, changes, and priorities within your organization.

Implementing SOC 2 Requirements

SOC 2's beauty – and its challenge – is that it doesn't tell you exactly which controls to use.

Unlike ISO 27001, which includes a predefined set of controls (Annex A), SOC 2 expects you to define and implement controls that align to the TSC and match the context of your systems.

This gives you flexibility. But it also means vagueness can kill your audit.

That's why clarity in your control structure is paramount. The auditor doesn't care if your control is fancy or innovative. They care if it's documented, implemented, monitored, and aligned to one or more Trust Services Criteria.

Here's the nuance most miss: controls are not just configurations. They are evidence-backed stories of how your systems reduce risk and fulfill your promises.

Documentation and Policies

Thorough documentation is vital to SOC 2 compliance. Clear policies and procedures enable organizations to demonstrate their data security and privacy commitment. This includes developing a comprehensive information security policy, incident response plan, data classification guidelines, and access control policies. Documenting these protocols ensures transparency and consistency in security practices

Technical Controls

Implementing robust security measures such as firewalls, intrusion detection systems, and encryption protocols helps safeguard sensitive data. Regular vulnerability assessments, penetration testing, and secure coding practices further enhance the security posture. Organizations should also ensure the proper configuration and monitoring of systems and secure network architecture

Operational Controls

Operational controls encompass the day-to-day procedures and practices that support data security. This includes employee training programs to promote security awareness, background checks, and access management protocols. Regular audits and reviews of user access privileges, system logs, and security incidents help identify and address vulnerabilities promptly. Incident response and business continuity plans are crucial for effective incident management and quick recovery.

Continuous Monitoring and Improvement

SOC 2 compliance is an ongoing process requiring continuous monitoring and improvement. Regular internal audits and assessments help identify gaps and areas for enhancement. Organizations should establish metrics and key performance indicators to measure the effectiveness of their controls. By conducting periodic risk assessments and staying abreast of emerging threats and industry best practices, organizations can proactively adapt their controls to address evolving security challenges.

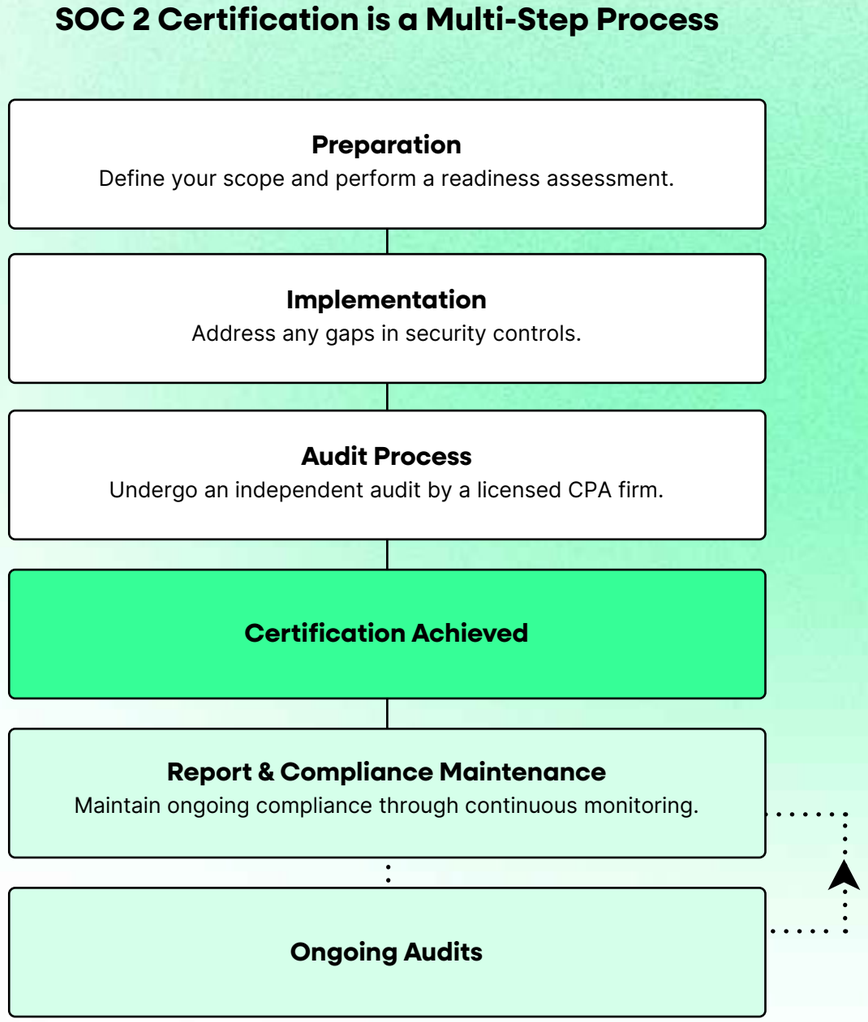
SOC 2 Audit Process

Understanding the SOC 2 audit process is crucial for organizations aiming to meet the stringent requirements of this widely recognized compliance framework.

Let’s explore the critical stages of the SOC 2 audit process and shed light on essential considerations for successful compliance.

Achieving SOC 2 certification

Achieving SOC 2 certification takes focus, consistency, and the right approach. This section outlines the essential steps to help you navigate the process smoothly and set your organisation up for long-term compliance.



Maintaining Certification

Maintaining SOC 2 compliance is an ongoing commitment beyond the initial assessment. Organizations must embrace the concept of constant monitoring and continuous improvement to ensure robust data security and adaptability in today's rapidly evolving digital landscape.

Regular assessments and audits play a vital role in verifying adherence to controls, identifying vulnerabilities, and assessing the effectiveness of security measures. By conducting frequent assessments, organizations can proactively address compliance gaps, strengthen their security posture, and demonstrate a continuous dedication to safeguarding sensitive data.

In addition to regular assessments, incident response and breach notification requirements are critical components of SOC 2 compliance. Prompt and efficient incident response procedures help mitigate the impact of security incidents and minimize potential damage.

Organizations should establish robust incident response plans, including clear escalation protocols, incident detection and containment mechanisms, and well-defined breach notification processes. By promptly addressing incidents and adhering to breach notification requirements, organizations can demonstrate their commitment to transparency and accountability, fostering stakeholder trust.

Another critical aspect of ongoing monitoring and continuous improvement is the proactive approach to addressing evolving requirements in SOC 2 compliance. The digital landscape constantly evolves, with emerging cybersecurity threats and changing regulations. Organizations must stay vigilant and adapt their compliance efforts to address new challenges.

Regularly reviewing and updating controls, policies, and procedures helps ensure that compliance efforts remain relevant and effective. By actively addressing evolving requirements, organizations can stay ahead of the curve, maintain compliance, and protect against emerging risks.

Trusted worldwide

SIEMENS · BDO · Panasonic · moneycorp · Entain · FLIGHT CENTRE

NHS Professionals · TUI · pladis · rightmove · Coventry University · AtkinsRéalis

Queensland Government TRADE + INVESTMENT QUEENSLAND · RICOH imagine. change. · Winckworth Sherwood · ScottishPower · accountancy insurance · orange Orange Cyberdefense

“

ISMS.online is not only an expert in their field, but they are fast, efficient, and cost-effective. Their platform takes out a lot of the hard work and as they have a proven track record delivering this certification for many clients in the past, there are very few unknowns and surprises to deal with.

Andrew Conway Chief Technology Officer, Xergy–Proteus

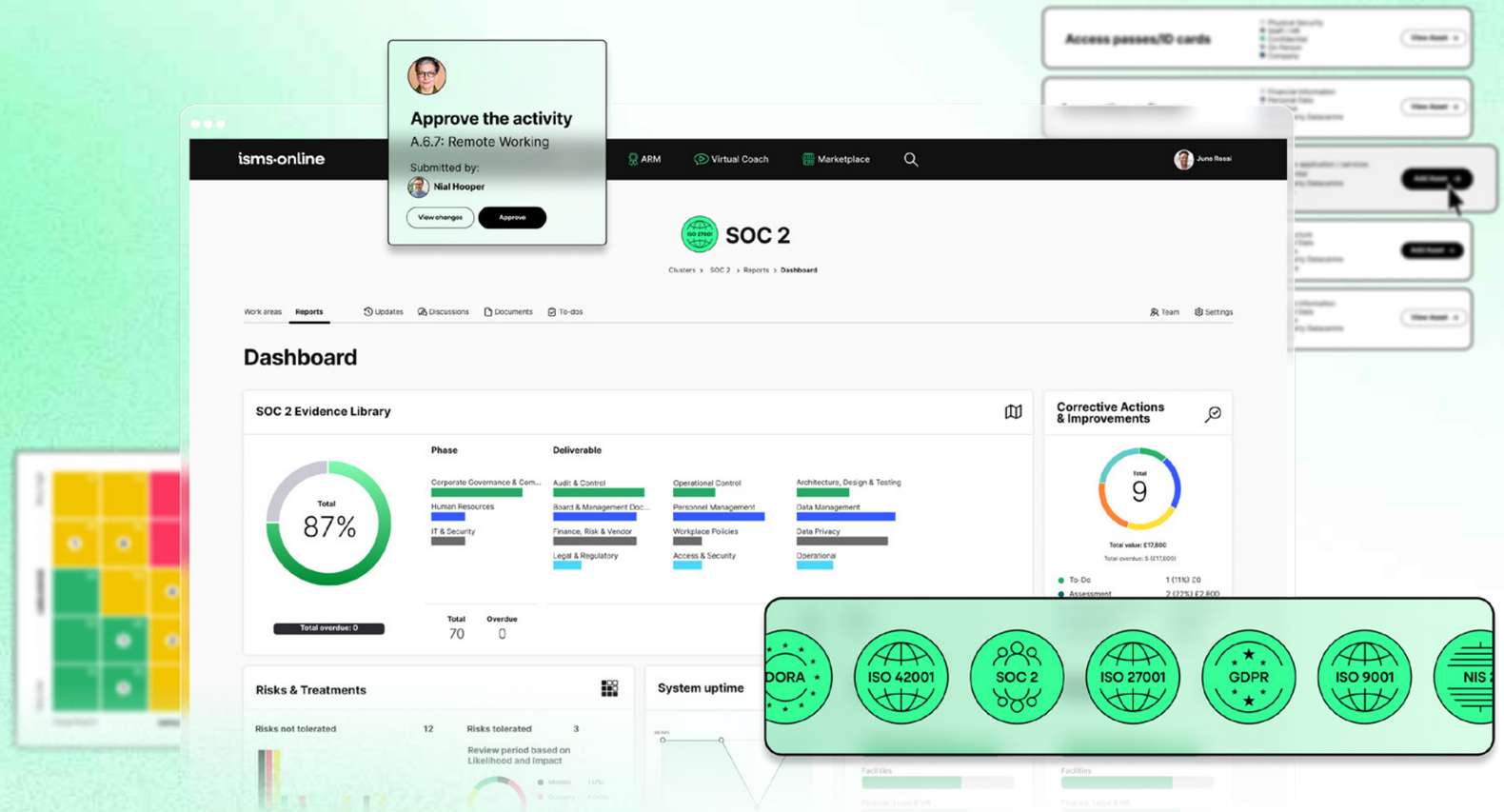
Book your platform demo today

Get started →

The ISMS.online solution

The fast lane to credible compliance

ISMS.online is packed full with all the tools, templates, and guidance you need to be compliant. And our expert support means help is always on hand when you need it.



SOC 2, Simplified.

Simplify your information security management with ISMS.online. Built with everything you need to succeed with ease, and ready to use straight out of the box – no training required!

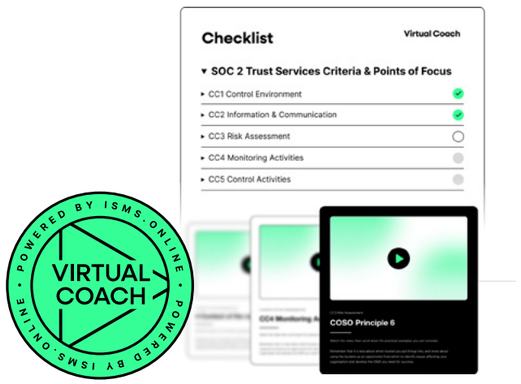
The ISMS.online software platform has been expertly designed and has all the necessary tools and features to help you achieve and maintain SOC 2 certification. With our comprehensive range of tools and content, we can assist in streamlining your SOC 2 journey and help you attain success in a shorter timeframe.

Start ahead, stay on top

With HeadStart your journey to SOC 2 is 81% complete from the moment you first log in. Simply adopt the preconfigured HeadStart content, adapt anything you need and then add in any specific policies and controls to fit your business.

No wrong turns

Stay on track to certification with ARM, your Assured Results Method for SOC 2 success. ARM takes all the SOC 2 controls and breaks them down into 11 simple steps so you can achieve certification fast without any hassle or headaches.



Your own SOC 2 coach

Virtual Coach is there when you need any guidance on how to approach any aspect of SOC 2. No need to wait for help, get your answers straight away with Virtual Coach – your always-on guide to SOC 2 certification.

Works with your existing systems

No need to double your workload.
At ISMS.online, we provide integrations with the essential systems you need to enhance your information security, seamlessly connecting with key ticketing, communications, reporting, task management, and Single Sign-On (SSO) platforms.

Fast, seamless integrations

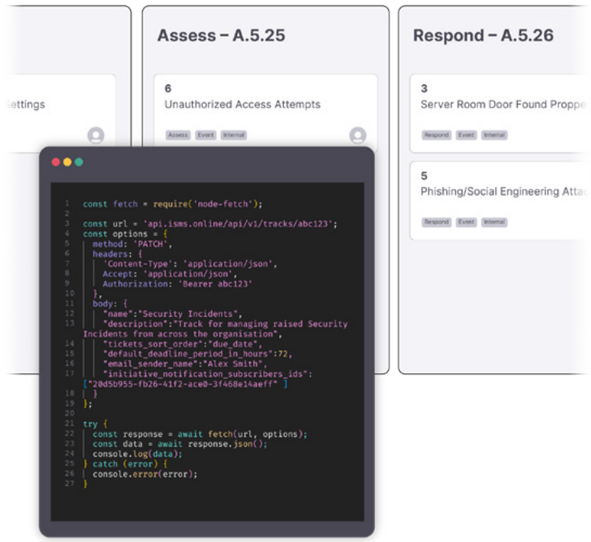
No need to double your workload. Integrate instantly with your existing setup, remove manual tasks, and let ISMS.online do the work for you.

Integrating compliance management tools into your business operations can streamline the compliance journey and achieve audit readiness.

With ISMS.online, businesses can go beyond simply outlining tasks and leverage the platform's automation capabilities to organise, remind, and capture corrective actions against each task continuously and in an audit friendly manner.

By leveraging our Zapier integrations, you can connect with over 5,000 other software platforms, enabling you to simplify the compliance journey from start to audit-ready and beyond. Moreover, ISMS.online is built and supported by security and compliance experts, assuring that the platform can handle compliance challenges effectively. By automating compliance management, businesses can simplify their security and compliance posture and confidently meet regulatory requirements.

Drive · Teams · Office · freshdesk · SharePoint · Namely
bambooHR · zendesk · ClickUp · asana · OneDrive · monday.com
slack · salesforce · Jira · HubSpot · Gmail · servicenow



Take complete control with our Public API

With our Public API, you're in control, allowing you to integrate data from the platforms essential to your business operations and information security.

Looking to streamline your security incident management process by sending security incidents from Jira into ISMS.online? How about receiving a continuous feed of threats and vulnerabilities directly as track items? With the ISMS.online Public API, you can effortlessly connect these systems and many more while turning ISMS.online into your single point of truth for information security.

Our API is designed for simplicity, ensuring your development team can hit the ground running in minutes and enabling you to advance your information security initiatives with ease. Whether you prefer Python, JavaScript, Ruby, or other coding languages, we've got you covered. Our documentation has working code snippets in multiple languages, so you can play around and interact with the API easily.

Your complete compliance toolkit

ISMS.online provides a dynamic and comprehensive toolset, built by experts to simplify every aspect of your SOC 2 compliance journey.

If managing SOC 2 requirements is draining your time instead of streamlining your process, it's time to switch to ISMS.online. Our secure, intuitive, and scalable platform is designed to help you efficiently maintain compliance, provide clear audit-ready evidence, and give your customers and stakeholders the assurance they need.

Easy Asset Management
Select assets from the Asset Bank and create your Asset Inventory with ease

Dynamic Risk Management
Effortlessly address threats & opportunities and dynamically report on performance

Perfect Policies & Controls
Easily collaborate, create and show you are on top of your documentation at all times

Mapping & Linking Work
Shine a light on critical relationships and elegantly link areas such as assets, risks, controls and suppliers

Fast, Seamless Integrations
Out of the box integrations with your other key business systems to simplify your compliance

Public API
Seamlessly integrate with key platforms to simplify your compliance by using ISMS.online's Public API

Evidence Library
Easily collect, organise, and access compliance evidence in one secure, audit-ready repository.

Staff Compliance Assurance
Engage staff, suppliers and others with dynamic end-to-end compliance at all times

Supply Chain Management
Manage due diligence, contracts, contacts and relationships over their lifecycle

Clear Reporting
Make better decisions and show you are in control with dashboards, KPIs and related reporting

Audits, Actions & Reviews
Reduce the effort and make light work of corrective actions, improvements, audits and management reviews

Specialist support

As an ISMS.online customer you have access to a Live Support Team of platform experts and a Customer Success Manager who has a stake in your success.

You're busy and SOC 2 is a big subject, so you may experience gaps in your capability, capacity or confidence. During your onboarding we help you identify what you currently have, what you may be missing and how quickly you're looking to achieve your goals. The outcome is a personalised roadmap that you can reference to ensure you're staying on track. If at points you have trouble staying on target, our team of in-house specialists can step in to lighten the load.

> ***The support team has been invaluable. They helped us migrate data, answered our everyday functionality questions, and their Information Security Experts were on hand to give us one-to-one support.***

Dean Fields IT Director, NHS Professionals

Ace your audits

Our platform ensures you can create, communicate, control and collaborate with ease – exactly the things your auditor will look for.

With ISMS.online your compliance becomes ‘business as usual’ with all your activity creating clear audit trails. This means you’ll approach every audit with confidence; knowing you’ve removed the risk of error while saving time and reducing cost.

“Our auditor loves it”

★★★★★

“Our auditor LOVES it! Our initial certification audit was a breeze because ISMS.online made it easy to show her everything was in place.”

Mark W.
Chief Technology Officer

★★★★★

“ISMS.online is a game changer. Makes managing the system a breeze and helps with staying current and compliant.”

Matthew F.
Director of Compliance

★★★★★

“Turns the daunting task of ISMS compliance and certification into a surmountable one. I can’t see how we would have achieved certification without it!”

L.K.
Project Manager

★★★★★

“ISMS.online has been vital to our success. The Assured Results Method is a neat and efficient system to keep track of our progress and has been instrumental to our success.”

Vincent G.
Head of Compliance

Get started today

Book a demo →

A solution that grows with your business

With ISMS.online you can integrate any management systems that share common elements.

Easily compatible standards include ISO 27001, ISO 27701, ISO 9001, ISO 22301 and ISO 14001 and we can also help you bring together many other ISO and non-ISO standards into your system. In fact, we currently support over 50 standards, frameworks and regulations.

If we don't already cover what you're looking for, we can quickly and easily add them to our simple, secure and sustainable platform.

View all frameworks →

The only truly global information security standard

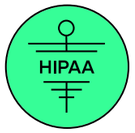
Manage the security of consumer data by implementing an information security management system.

Protect and manage your customer data

SOC 2 outlines standards for the management of data with regards to: security, availability, processing integrity, confidentiality, and privacy.

A framework to manage and protect personal data

ISO 27701 provides guidelines for the implementation of a privacy information management system.

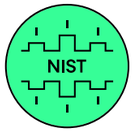


Ensure the privacy of health records and personal information

HIPAA is a law that requires organisations managing protected health information to keep it secure and protected.

Data protection and privacy in the EU and EEA

GDPR is an EU law establishing rules for the collection, use, and storage of personal data and individual rights related to their personal information.



Reduce cybersecurity risk and protect networks and data

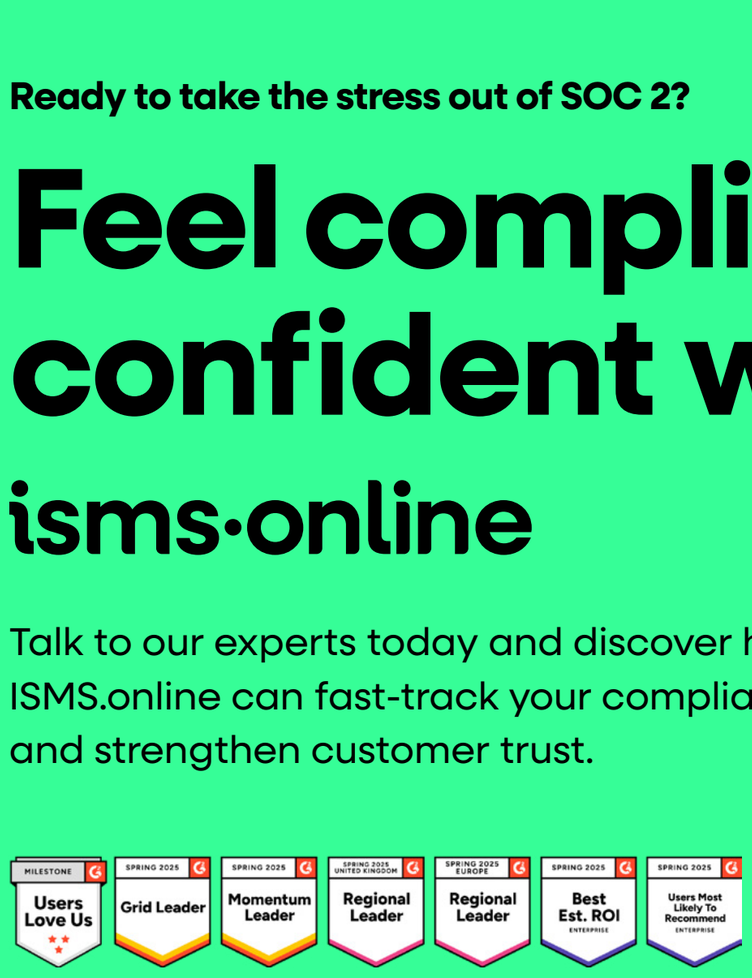
NIST is a US government standard that outlines the security requirements for protecting controlled unclassified information (CUI) in non-federal systems and organisations.

Ready to take the stress out of SOC 2?

Feel compliance confident with

isms·online

Talk to our experts today and discover how ISMS.online can fast-track your compliance and strengthen customer trust.



Start your compliance journey today

Get started →