isms.online

# AI Management Made Easy

## The no-stress guide to ISO 42001

Public

# ISO 42001 – the world's first artificial intelligence management standard, sets out how to design, build, implement and continuously improve an Artificial Intelligence Management System that can be independently certified for assurance purposes.



**Understanding ISO 42001**



**The ISMS.online solution**

# Getting started with AI management

So, you want to unlock the benefits of ISO 42001 compliance for effective AI governance within your business?



## So, you want to unlock the benefits of ISO 42001 compliance for effective AI governance within your business?

You're probably wondering how to get started! The rapid growth of Artificial Intelligence (AI) is offering businesses fresh opportunities for innovation and growth. However, it also presents organisations with ethical, privacy, and security challenges that threaten to undermine the technology's potential benefits.

You may feel overwhelmed. That's understandable. AI is a vast topic. But don't worry. We have already helped organisations achieve and maintain their ISO 42001 certifications. We supported one of the world's first certifications to the standard, and we know how to help you unlock simple, sustainable and secure AI compliance in your business. So, let's get going!

**In this guide, we'll help you understand:**

- The basics of ISO 42001
- What a good Artificial Intelligence Management System looks like
- How you can save time and budget by learning as you build

# What is ISO 42001?

ISO 42001 is the world's first artificial intelligence management standard, published in October 2023 by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), the standard sets out how to design, build, implement and continuously improve an Artificial Intelligence Management System (AIMS) that can be independently certified for assurance purposes.



**"ISO 42001 certification helps us stand out from the crowd and proves that we are the strongest AI player in our industry."**

**Adam Wisniewski**
CTO and Co-founder, AI Clearing

## The scope of ISO 42001

ISO 42001's scope is broad, encompassing all AI systems, including machine learning, deep learning, natural language processing, and computer vision. It applies to organisations of all sizes and sectors, whether developing AI systems in-house or procuring and using third-party platforms and services.

Any organisation using AI services within their operations, such as ChatGPT 4, Google Gemini and chatbots or those developing AI products can leverage ISO 42001 to ensure they:

- Establish policies, procedures, and objectives for AI systems
- Ensure transparency, accountability, and explainability in AI decision-making
- Identify and mitigate bias in AI algorithms
- Safeguard user privacy and data security

**97%**

**97% of business owners think using ChatGPT will help their business.**

Source: Forbes

**77%**

**of companies are either using or exploring the use of AI**

Source: Exploding Topics

**69%**

**of enterprise executives believe AI will be necessary to respond to cybersecurity threats**

Source: wifitalents

**ISO 42001 doesn't just help organisations avoid adverse outcomes; it creates a foundation for long-term, sustainable growth.**

# Why is it so important?

As businesses increasingly rely on AI to drive growth and innovation, it's crucial to recognise the importance of developing and deploying AI responsibly. Trust is the cornerstone of business success, and responsible AI practices are essential for building and maintaining that trust with your customers, partners, and stakeholders.

## Taking proactive action

When you leverage ISO 42001 for AI management, you proactively address the risks facing your business, such as:

- Algorithmic biases that can lead to discriminatory outcomes
- Data privacy violations that erode customer trust
- Intellectual property loss due to inadequate security measures
- Information and financial security breaches
- Damaging regulatory fines

## Protect reputation, mitigate risk

Addressing these risks head-on demonstrates your commitment to ethical practices and protects your company's reputation. Moreover, improving AI quality through responsible practices mitigates these risks and delivers direct financial benefits to your business.

When you invest in responsible AI, you:

- **Enhance data quality, leading to more accurate insights and decision-making**. This improved accuracy can increase revenue through better-targeted and more effective business strategies.
- **Streamline processes and boost operational efficiency to achieve significant cost savings**. Efficient processes reduce waste and downtime, directly improving your bottom line.
- **Foster a culture of transparency and accountability to attract top talent and build customer loyalty**. This will enhance your workforce's productivity and stabilise revenue streams through increased customer retention.

ISO 42001 doesn't just help organisations avoid adverse outcomes; it creates a foundation for long-term, sustainable growth. By developing AI ethically, you position your business as a leader in your industry, ready to capitalise on AI's opportunities. You navigate the challenges with integrity and build a company that is resilient, trustworthy, and poised for success in the long run.



By developing AI ethically, you position your business as a leader in your industry, ready to capitalise on AI's opportunities. You navigate the challenges with integrity and build a company that is resilient, trustworthy, and poised for success in the long run.

# What are the fundamental principles of the ISO 42001 standard?

ISO 42001's primary purpose is to guide organisations in managing the unique challenges posed by AI systems. By adhering to its fundamental principles, you can ensure your AI systems are developed, implemented, and utilised in a manner that prioritises transparency, accountability and compliance.



## Ethics & Fairness

Ethics and fairness are cornerstone principles in the ISO 42001 standard, emphasising the importance of responsible AI practices to ensure equitable and unbiased outcomes.

- **Ethical Guidelines**
  Organisations must develop and adhere to ethical guidelines that govern the development and deployment of AI systems. These guidelines should be aligned with universally accepted moral principles, such as respect for human rights, fairness, and non-discrimination.

- **Bias Mitigation**:
  ISO 42001 requires organisations to implement robust mechanisms to detect, assess, and mitigate biases in AI systems to ensure they do not perpetuate or amplify existing biases. Techniques such as diverse data sampling, fairness-aware algorithms, and bias correction methods should be employed.

- **Fair Decision-Making**:
  AI systems must be designed and operated to ensure fair and just outcomes. This includes providing equal treatment and opportunities across all demographic groups. Organisations should establish processes for stakeholders to report and address perceived unfairness in AI-driven decisions.

# Transparency and Explainability

A fundamental aspect of the ISO 42001 standard is fostering transparency and explainability in managing AI systems. This is crucial for maintaining trust and accountability, particularly in decisions that impact individuals and society.

- **Transparency**
  Organisations are required to ensure that the operations and outcomes of AI systems are transparent to relevant stakeholders. This involves openly sharing information about how AI systems function, the data they use, and their decision-making processes. Transparency helps stakeholders understand and trust AI systems, promoting broader acceptance and minimising resistance due to perceived opacity.

- **Explainability**
  Alongside transparency, ISO 42001 emphasises the importance of explainability. This refers to the ability to describe, in understandable terms, the mechanisms and outcomes of AI systems. Explainability is essential for validating and justifying AI systems' decisions, especially in critical applications with significant consequences.



# Security and Privacy

Security and privacy are essential components of ISO 42001, ensuring AI systems are protected against threats and personal data is safeguarded throughout the AI lifecycle. This includes:

- **Data Management**
  ISO 42001 mandates establishing secure procedures for data collection, storage, processing, and disposal. Organisations must implement data encryption, access controls, and regular security audits to protect AI systems.

- **Privacy Protection**
  Compliance with privacy laws such as GDPR is required. Organisations must anonymise or pseudonymise personal data where possible to protect individual privacy. Clear consent mechanisms and privacy notices must be communicated to data subjects.

- **Security Measures**
  Robust security measures are essential to protect AI systems from cyber threats. This includes firewalls, intrusion detection systems, regular vulnerability assessments, and incident response plans. Security protocols must be continuously updated to address evolving threats.

- **Access Control**
  Strict access control policies are necessary to ensure only authorised personnel access AI systems and data. This includes multi-factor authentication, role-based access controls, and regular access reviews.

- **Audit and Compliance**
  Regular audits and compliance checks are required to ensure the effectiveness of security and privacy measures and adherence to relevant laws and standards. These audits should evaluate technical and organisational aspects of AI security and privacy.

- **Incident Management**
  An incident management process must be established to quickly detect, respond to, and recover from security breaches or data privacy incidents. This includes clear roles and responsibilities, communication plans, and procedures for mitigating harm and preventing future incidents.

# Continuous Improvement

To ensure the AI management system remains effective and relevant, ISO 42001 emphasises constant evaluation and improvement:

- **Monitoring and Measurement**
  Regularly monitor AI system performance against set objectives and report on performance indicators.

- **Audit and Review**
  Periodic audits of the AI management system to ensure compliance with the standard and internal policies, followed by management reviews to assess overall system effectiveness.

- **Continual Improvement**
  Implement improvements based on performance evaluations, audit findings, and evolving best practices to continuously enhance the AI management system.

**“By embracing responsible AI governance, businesses can position themselves as leaders in the AI space, attracting top talent, fostering innovation, and contributing to developing and integrating AI systems that create value for all stakeholders.”**

**Luke Dash**
CEO, ISMS.online



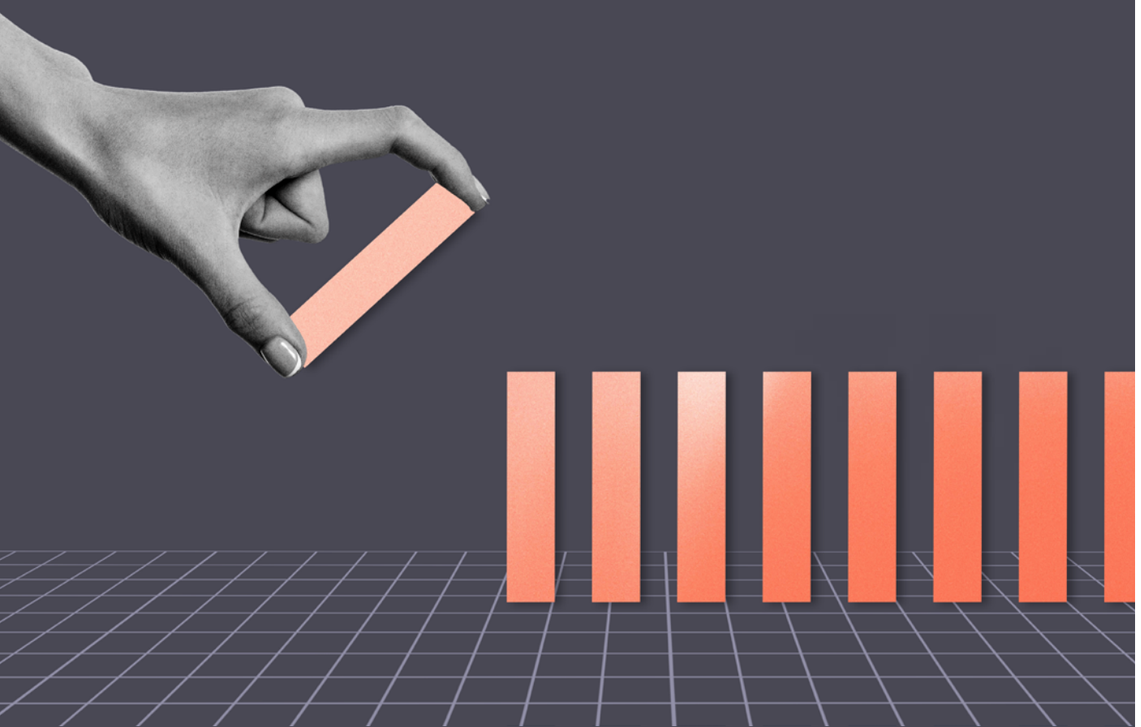
**“The AI certification validates that our AI system adheres to the latest and most rigorous standards. Our AI models undergo thorough validation and verification before release, ensuring their trustworthiness.**

**Michael Mazur,**
CEO, AI Clearing

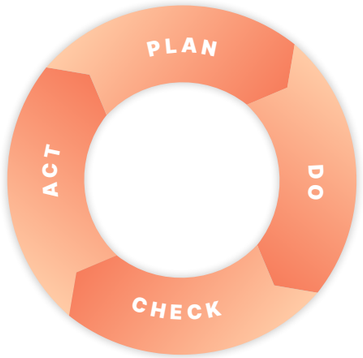
Read their story →

# How is ISO 42001 structured?

ISO 42001 is structured to ensure that organisations can develop a robust Artificial Intelligence Management System (AIMS) through a clear and systematic approach.








## Plan-Do-Check-Act

The standard employs the Plan-Do-Check-Act (PDCA) cycle, an iterative process designed to foster continuous improvement within AI systems management. This method allows organisations to achieve compliance dynamically and adaptively, accommodating the rapid evolution of AI technologies.

### Phases of the PDCA Cycle

- **Plan:** Establish AI management objectives and processes to deliver results following the organisation's AI policy.
- **Do:** Implement the processes as planned.
- **Check:** Monitor and measure processes against AI policy, objectives, legal and regulatory requirements, and report the results.
- **Act:** Take action to improve the AI management system's performance continually.

The standard was designed to be easily integrated with other management system standards, such as ISO 27001, the global information security management systems standard. As such, it follows the same structure, including identical clause numbers, titles, text, common terms, and core definitions, which are then explicitly applied to addressing AI risk.

# Clauses

The first three clauses identify the scope, normative references, and terms and conditions before proceeding to the main clauses.

Here is a breakdown of the framework requirements provided in Clauses 4 through 10, which mirror other management system standards:

| | |
|---|---|
| **Clause 4** | Context of the Organisation |
| **Clause 5** | Leadership |
| **Clause 6** | Planning |
| **Clause 7** | Support |
| **Clause 8** | Operation |
| **Clause 9** | Performance Evaluation |
| **Clause 10** | Improvement |

The framework then features four annexes providing detailed ISO 42001 AI guidance. While Annex A focuses on the controls, mirroring ISO 27001, ISO 42001 provides additional guidance beyond the scope of other management system standards in three additional annexes.

## Supportive Annexes

- **Annex A:** A comprehensive description of each of the standard's 39 controls and their objectives
- **Annex B:** Provides practical advice on implementing the various controls.
- **Annex C:** Focuses on risk management frameworks applicable to AI, detailing how organisations can identify, evaluate, and mitigate risks associated with AI deployments.
- **Annex D:** Contains sector-specific standards and recommendations to aid in contextualising the main standard, addressing unique industry needs and challenges.



**Overall, ISO 42001's structure ensures a comprehensive approach, enabling organisations to manage their AI systems effectively across all operational aspects.**

# Mastering the core controls

The standard includes 39 controls for businesses to consider, as well as some fundamental controls that all organisations must consider. These controls are integral to ensuring AI systems operate safely, ethically, and efficiently.



## AI Impact Assessment:
## Evaluating Influence and Implications

- **Purpose:** The AI Impact Assessment is fundamental to understanding how AI implementations can affect individuals and the broader society.
- **Process:** This involves a thorough analysis to identify potential adverse effects of AI technologies, followed by formulating strategies to mitigate identified risks.

## Lifecycle Management:
## Ensuring Comprehensive Oversight

- **Scope:** This control spans the complete lifecycle of AI systems, from their inception and design to their deployment and eventual phase-out.
- **Requirements:** It mandates sustained adherence to ethical standards and regulatory compliance at every stage, ensuring that each phase of the lifecycle conforms to established guidelines.

## Supplier Management:
## Securing the Supply Chain

- **Importance:** This is especially crucial for organisations that depend on third-party AI technologies and services.
- **Alignment:** All suppliers must conform to the organisation's AI ethics and compliance standards, safeguarding against the risks posed by external collaborations.

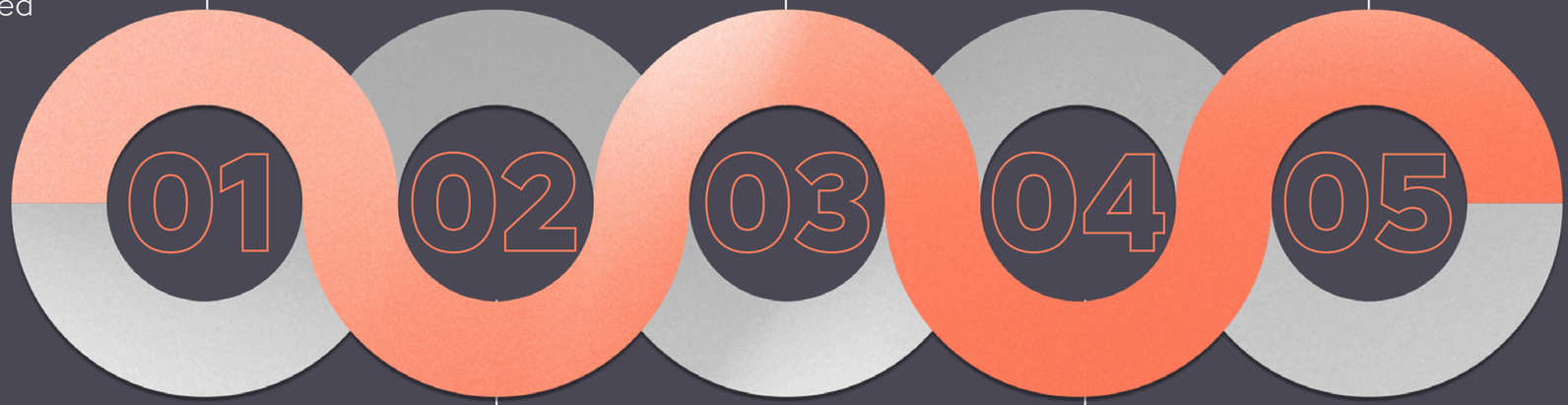
**Key takeaway**

These controls, detailed in the ISO 42001 framework, are about more than just compliance. They are strategically designed to ensure that AI systems align with broader business goals and uphold the highest ethical standards.

# How do you reach ISO 42001 compliance?

The first step is effectively implementing an Artificial Intelligence management system within your organisation's operations, which requires a structured approach. Here are the essential steps.

Working with us will significantly expedite this process. We've set up everything you need to be guided through to certification.




**Conducting a Gap Analysis**

Document current AI management practices, compare them against ISO 42001 requirements to identify gaps, and prepare a detailed report to guide your implementation strategy.

**Developing an Implementation Plan**

Establish clear objectives and priorities based on the gap analysis, allocate necessary resources, and create a timeline with specific milestones to keep the project on track.

**Training Personnel and Raising Awareness**

Conduct training sessions on ISO 42001's requirements and ethical AI usage, complemented by awareness campaigns to ensure all stakeholders understand and support the changes.

**Establishing Documentation and Record-Keeping Processes**

Develop procedures for maintaining comprehensive documentation and a secure, accessible record-keeping system regularly updated to reflect system changes.

**Conducting Internal Audits and Management Reviews**

Periodically audit the AI management system to assess its effectiveness, hold management reviews to discuss results and necessary adjustments, and continuously refine the system based on these insights.

# Achieving certification

Achieving ISO 42001 certification is the ultimate way to demonstrate your commitment to secure and ethical AI.

With our help, you'll easily pass through two rigorous external audits, after which your auditor will recommend you for certification by the relevant accreditation body. Once certified, you'll enjoy the benefits of ISO 42001 for three years, with regular internal and external audits to ensure you're always compliant.

## How long does it take?

We get asked this question a lot, and the truth is that it depends on two main factors – where you start and what approach you take.

In our recent State of Information Security Report, over 39% of organisations stated that it took them over one year to achieve certification.

**Key takeaway**

In comparison, you can achieve success more quickly by using a pre-configured AIMS rather than by building your own, with the average time to complete sitting at less than six months (25%) and between 6–12 months (21%).

## Typical certification process

# The building blocks for an effective AIMS

If your AIMS doesn't have these characteristics as an absolute baseline, you'll end up with a less effective platform and work much harder than you need to.

### Easy to use

Keep it simple – complicated management systems are costly to use and encourage noncompliance.

### A single source of truth

Make sure you choose a single software solution that's futureproofed for your ongoing compliance needs.

### Security confidence

You'll hold some very sensitive information in your aims, so avoid software solutions with weak security.

### Works with your existing systems

Utilise integrations to streamline data collection and seamlessly connect with the software you already use daily.

### Always accessible

Your AIMS should be available to authorised parties securely when and where they want it, with backup and

### Joined up

Choose a solution with easy navigation and clear linking to help stakeholders find their way.

### Transparent

Impress your auditor with an AIMS that shows your work as it evolves, making it easy to record and track changes.

### Collaborative

Go for built-in collaboration tools to avoid duplication and help demonstrate continual improvement.

### Insightful & actionable

An AIMS with pre-configured reporting and reminders will help you and your stakeholders make better decisions.

### Affordable

Prove your return on investment with an AIMS that's cost-effective to implement and operate.

isms.online

# TRUSTED WORLDWIDE

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

NHS Professionals · pladis · Coventry University · AtkinsRéalis · AI Clearing · Orange Cyberdefense

Trade + Investment Queensland · TUI · accountancy insurance · ScottishPower

**ISMS.online are 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 free platform demo today

Get started →

# AI Management, Simplified.

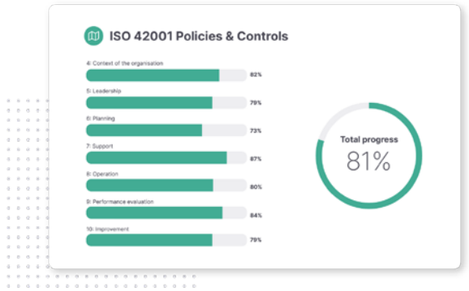
Simplify your AI management with ISMS.online. It is built with everything you need to succeed easily and is ready to use straight out of the box — no training required!

The ISMS.online software platform has been expertly designed and has all the necessary tools and features to help you achieve and maintain ISO 42001 certification. With our comprehensive range of tools and content, we can assist in streamlining your ISO 42001 journey and help you attain success in a shorter timeframe.

**Key takeaway**

Adopting the ISMS.online platform to achieve ISO 42001 compliance helps you mitigate risks, improve transparency and accountability, and maintain a competitive edge by ensuring compliance with international standards.



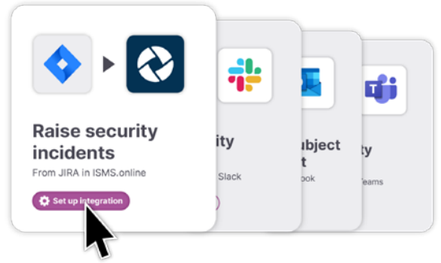


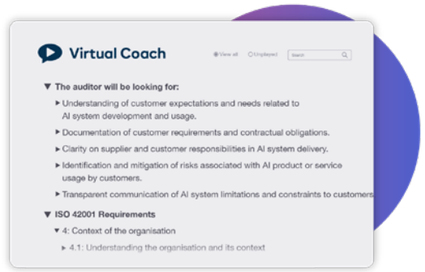

## Start ahead, stay on top

With Headstart, your journey to ISO 42001 is 80% complete from the moment you log in. Simply adopt the pre-configured HeadStart content, adapt anything you need, and then add any specific policies and controls to fit your business.

## Works with your existing systems

No need to double your workload. Connect with over 5,000 apps and leverage the benefits of automating compliance by integrating ISMS.online with your existing tech stack. Integrate instantly, remove manual tasks, and let ISMS.online do the work for you.




## Your own ISO 42001 coach

Virtual Coach is there when you need guidance on approaching any aspect of ISO 42001. There is no need to wait for help; get your answers immediately with Virtual Coach, your always-on guide to ISO 42001 certification.

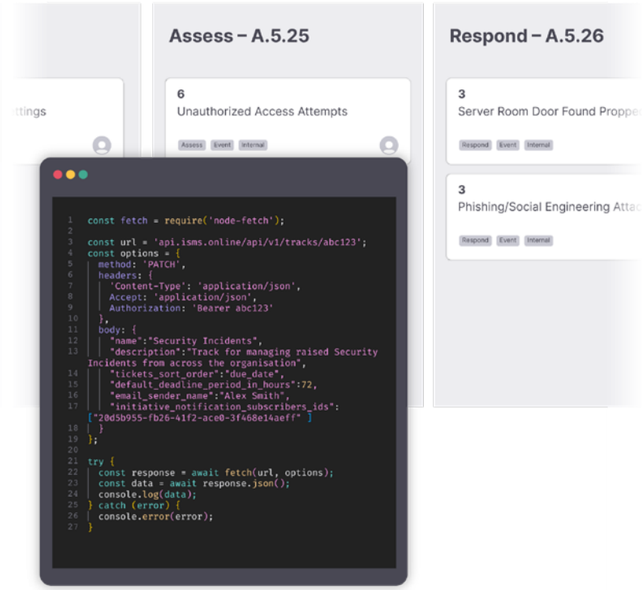
# Fast, seamless integrations

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 solutions like 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.




## Take complete control with our Public API

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

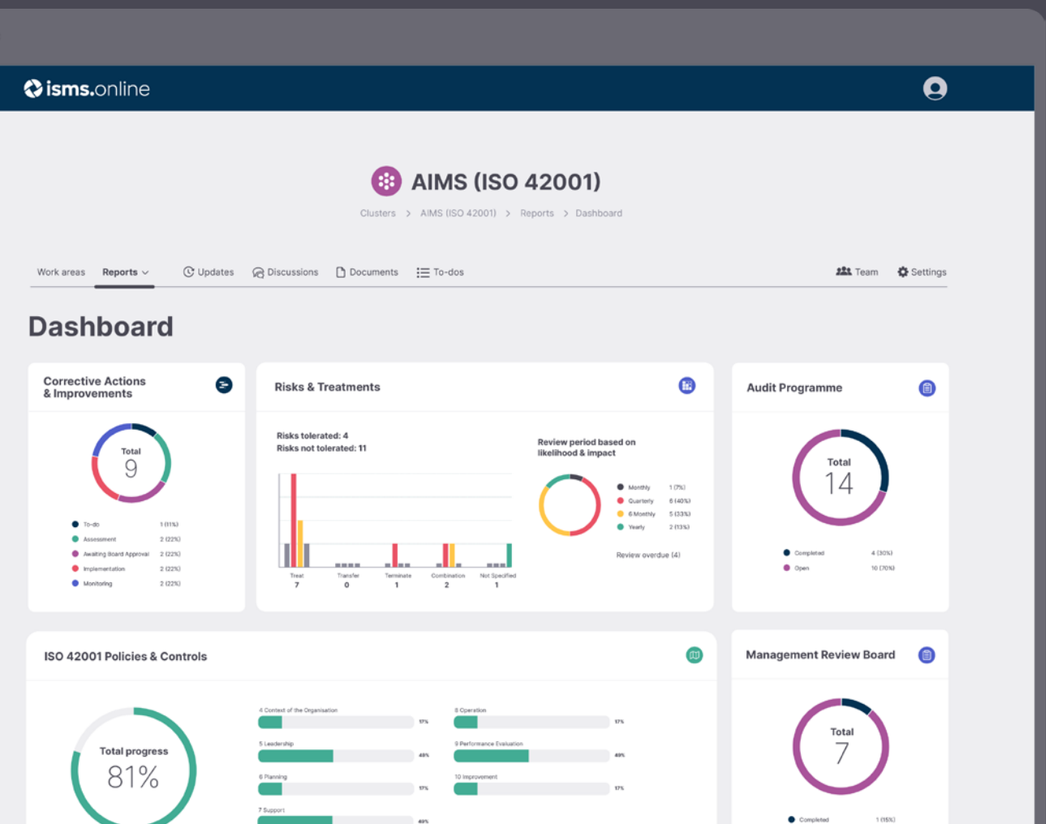
Looking to streamline your security incident management process by sending security incidents from Jira into ISMS.online? How about receiving a continuous feed of threats and vulnerabilities directly as track items? With the ISMS.online Public API, you can effortlessly connect these systems and many 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 features a dynamic and comprehensive toolset built by experts to simplify every requirement of your AIMS build and maintenance.

If your AIMS costs you time instead of saving it, it's time to move to ISMS.online. Every aspect of our simplified, secure, sustainable platform is designed to help you reclaim your time while giving you and your interested parties maximum assurance.




## Create your AIMS

### Dynamic risk management

Effortlessly address threats & opportunities and dynamically report on performance.

### Perfect policies & controls

Easily collaborate, create, and show that you are always on top of your documentation.

### Fast, seamless integrations

Out-of-the-box integrations with your other critical business systems to simplify your compliance.

### Mapping & linking work

Shine a light on critical relationships and elegantly link areas such as risks, controls and suppliers.

## Manage your AIMS

### 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.

### Audits, actions & reviews

Reduce the effort and make light work of corrective actions, improvements, audits and management reviews.

### Clear reporting

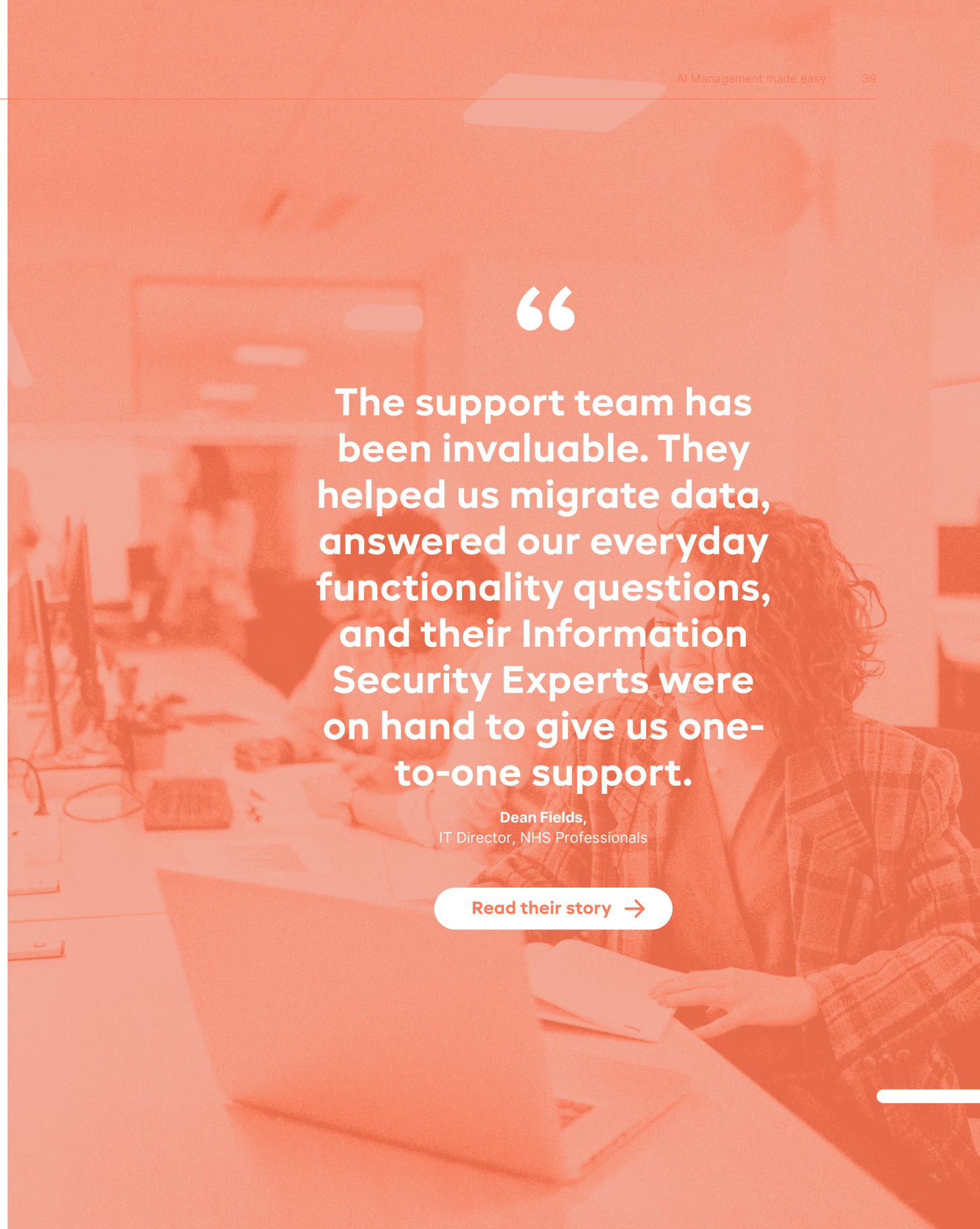
Make better decisions and show you are in control with dashboards, KPIs and related reporting.

# Specialist support

As an ISMS.online customer, you can access a Live Support Team of platform experts and a Customer Success Manager with a stake in your success.

You're busy, and ISO 42001 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

Read their story →

“

**We admire the clarity and structure of ISMS.online. It positions our ISO procedures and processes as the focal point of our organisation rather than just being shelved documentation.**

**Dariusz Ciesla**
VP of Product & Strategy, AI Clearing

Read their story →

# Ace your audits

Our platform ensures you can easily create, communicate, control, and collaborate with ease — exactly what your auditor will look for.

With your AIMS all-in-one-place and instantly accessible, you’re perfectly placed to demonstrate the “process of continual improvement” required by the foundational ISO 42001 standard.

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

**Read ISO 42001 customer stories**

If you want to hear from real customers who have gone through the process with us, check out our **case study with AI Clearing**, which achieved the world’s first ISO 42001 certification using our platform!

# “OUR AUDITOR LOVES IT”


★★★★★

**“ISMS.ONLINE IS A GAME CHANGER. MAKES MANAGING THE SYSTEM A BREEZE AND HELPS WITH STAYING CURRENT AND COMPLIANT.”**

MATTHEW F.
DIRECTOR OF COMPLIANCE

★★★★★

**“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

★★★★★

**“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

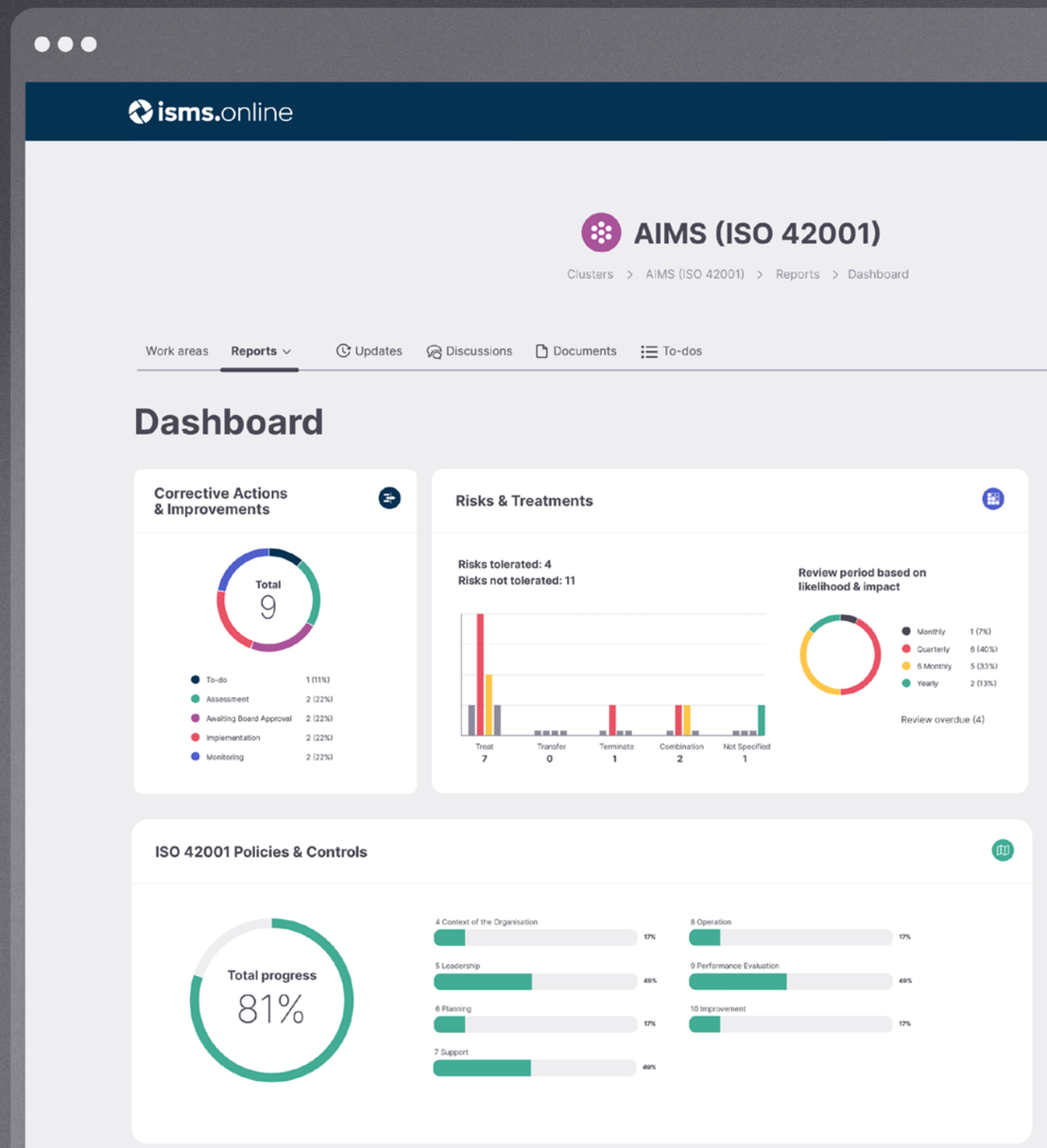
★★★★★

**“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

## Book your free platform demo today

Get started →



# 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. We can also help you integrate many other ISO and non-ISO standards into your system. In fact, we currently support over 100 standards, frameworks, and regulations.

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


### A framework to manage and protect personal data

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


### 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.


### 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.


### Ensure the privacy of health records and personal information

HIPAA is a law that requires organisations
managing protected health 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.

isms.online

# Ready to get started with ISO 42001?

Book a chat with our team today and see how ISMS.online can improve your business

Get started →