stryke.

TRANSITIONING to ISO 27001:2022

Organisations with existing ISO 27001:2013 certifications must transition to the 2022 standard by **October 31 2025**. This transition ensures that all certifications align with the latest security practices and regulatory requirements.

Let's see how it is done...

My company is certified to ISO 27001:2013, why should I starting thinking about transitioning to ISO 27001:2022 now?

STEP 1

Stay Ahead of Compliance Deadlines

Avoid Last-Minute Rush
By starting the transition early, you can avoid the stress and potential pitfalls of rushing to meet the October 31, 2025, deadline. Early planning gives you ample time to address any unforeseen challenges.

Ensure Continuous Certification
Starting now helps ensure that your organisation maintains continuous certification without any gaps, which is crucial for maintaining client trust and meeting contractual obligations of your customers.

STEP 2

Enhanced Security Posture

Updated Security Controls
The 2022 standard includes updated and more relevant security controls that address modern threats and vulnerabilities. Transitioning early helps you strengthen your security posture by implementing these enhanced controls sooner.

STEP 3

Proactive Risk Management

The new standard emphasises continuous improvement and proactive risk management, which can help you **identify and mitigate risks** more effectively, making sure you protect what matters most.

STEP 4

Market Competitiveness

Meet prospect and customer expectations
Many customers and partners expect organisations to comply with the latest standards. Transitioning to the updated ISO 27001:2022 can help you meet these expectations and enhance your reputation in the market.

Competitive Advantage
Early adoption of the new standard can set you apart from competitors who may still be lagging behind, demonstrating your commitment to the highest security standards meaning you will win more business through compliance and trust.

STEP 5

Audit Preparedness

Prepare for Audits
Transitioning early allows you to prepare thoroughly for the required audits. You can address any gaps identified during internal audits and ensure that all necessary documentation and controls are in place for the external audit

How can Stryke help?

We ensure our customers achieve and maintain ISO 27001 certification through our automated compliance platform

1. Automated Monitoring and Evidence Collection

Continuous Monitoring
Continuously your security controls and collect evidence in real-time. This automated process ensures that all necessary controls are active and functioning correctly, reducing the manual effort required to gather compliance data.

Evidence Collection
Automate the collection of evidence needed for ISO 27001 audits. This includes logs, screenshots, and configurations, ensuring that all required documentation is up-to-date and readily available for auditors.

2. Streamlined Risk Management

Risk Assessments
Conduct thorough risk assessments by identifying potential security risks and providing tools to document and manage them. This aligns with ISO 27001's requirements for regular risk assessment and treatment planning.

Risk Treatment Plans
Developing and track risk treatment plans, ensuring that all identified risks are appropriately addressed and mitigated.

3. Policy Management

Policy Templates and Customisation
Get pre-built templates for required security policies, which can be customised to fit the specific needs of your business. This helps in establishing the necessary documentation for ISO 27001 compliance.

Policy Enforcement
Ensure that all employees are aware of and adhere to the established security policies by tracking policy acceptance and enforce compliance across your business.

4. Automated Audits and Reporting

Audit Readiness
Prepare for your ISO 27001 audits by ensuring that all documentation and evidence are in place and even simulate the audit process and identify any gaps that need to be addressed before the real thing.

Reporting
Generate comprehensive reports that detail your businessses compliance status. These reports can be used during internal reviews or shared with external auditors to facilitate the audit process

Trust Centre
Provide your prospects and customers with a centralized view of live compliance status. The Trust Centre provides real-time visibility into your business's compliance status across various frameworks, including ISO 27001, SOC 2, GDPR, and more, enhancing transparency and trust to help you close new customers.

5. Integration with Existing Tools

Seamless Integration
Integrate with over 140 SaaS tool and platforms used by your business, such as cloud services, HR systems, and ticketing systems. This integration ensures that compliance processes are seamlessly incorporated into existing workflows.

Experts in all things cybersecurity and compliance

Our mission is to arm you with the right compliance and security solutions for your business. Talk to us today about how we can help make compliance easier for your business.

Let's talk