bsi.

● ISO/IEC 27001 Transition Guide

A leap forward in ISMS effectiveness

ISO/IEC 27001, Information Security Management and ISO/IEC 27002, Controls for Informations Security standards have been updated to reflect the global digital evolution and new business practices becoming more cloud and digitally reliant. The new standards will require you to implement changes to ensure you not only remain compliant but align your infosec posture with the digitalization of business practices and the accompanying threats.

Step 1 - Understand the changes

Buy a copy of the ISO/IEC 27001:2022 and ISO/IEC 27002:2022 standards and train your team to help them understand and apply the changes as necessary. Our training and resources page can help support you on your learning journey.

Skills updated

By taking the new BSI Understanding and auditing the changes training course you and your team will be prepared to go through the transition journey.

Step 2 - Check the impact on your organization

Do a Gap Analysis against the changes in ISO/IEC 27001:2022 using your learnings from the BSI training and ISO/IEC 27002 to help you, and take a look at your risk assessment. Is it aligned with your organization's objectives and context? Ensure that it is.

Update-ready

By this point, you're almost ready to update your ISO/IEC 27001 certificate.

Step 3 - Implement the changes

Take a look at the evidence and justification for the inclusion or exclusion of necessary controls, and update your SOA accordingly. Be sure to implement the applicable changes based on your risk treatment plan and new controls, and validate the changes through an internal audit. Have they been implemented effectively? Make sure you have implemented the changes effectively. This step will help you reduce the likelihood of failing. Contact us for a **Readiness review**.
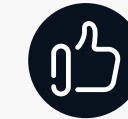
See the benefits

Even this early in the process, you'll begin to see the benefits of the changes you've identified based in your understanding on how your current business practice and associated risks has evolved.

Step 4 - Transition you certificate

Get in contact and schedule your transition audit with your BSI representative. To transition to ISO/IEC 27001:2022, your Auditor will confirm the implementation of any new necessary controls that you have chosen and their alignment with your ISMS. Get your audit report, take a look at your auditor's feedback and act based on the results.
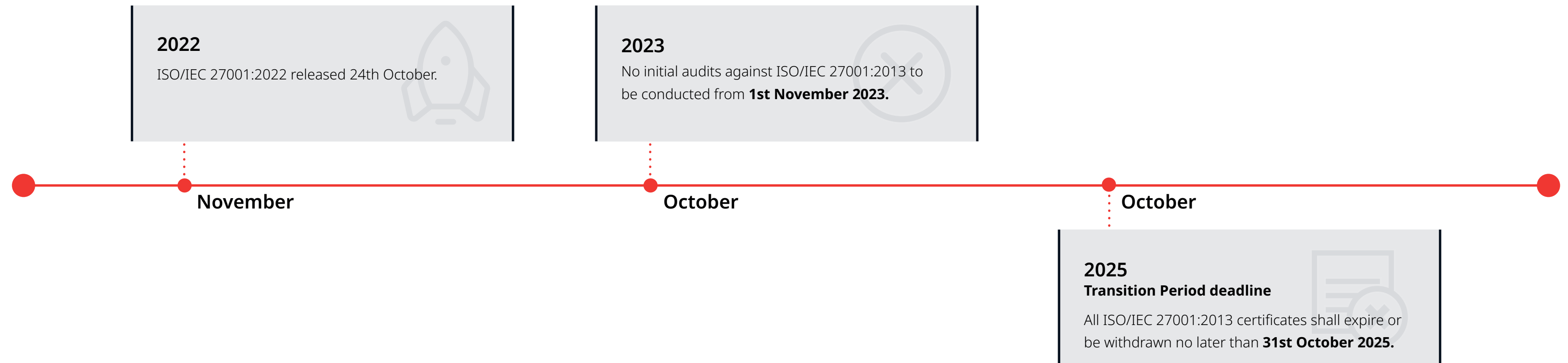
Congratulations!

You've made it, get your updated ISO/IEC 27001:2022 certificate

Ongoing conformance and improvement

Keep your process improvement cycle and embed information resilience within your organization.

bsi.

ISO/IEC 27001:2022 Transition Timeline

1st November 2022 start of 3 years transition period to 31st October 2025

2022
ISO/IEC 27001:2022 released 24th October.

2023
No initial audits against ISO/IEC 27001:2013 to be conducted from **1st November 2023.**

November

October

October

2025
Transition Period deadline

All ISO/IEC 27001:2013 certificates shall expire or be withdrawn no later than **31st October 2025.**

When to transition

During a routine surveillance audit

At your re-certification audit

Special audit

Notes

- All audits require additional time to complete
- Additional time calculated on an individual basis, based on size and complexity of your scope.

bsi.