ISO 27001 Audit Checklist

THE BRITISH ASSESSMENT BUREAU

✓ Ensure Commitment

The process of creating and implementing your information security management system (ISMS) and then going forward for assessment will be made easier if there is full commitment from the top to the bottom of the organisation.

✓ Assign a Project Manager

Although sole responsibility shouldn't fall on one person's shoulders, it is advised to assign a project manager as a spearhead. This needs to be someone who's orderly minded, has the authority to make decisions and has direct access to senior management team.

✓ Preparing for the Audit

It's well worth taking stock of your current situation. The best way to do this is by monitoring and measuring your current procedures and identifying any legal requirements of your ISMS.

✓ Scope of the Audit

Define the scope of your ISMS, this will help prevent you from doing unnecessary work. The scope outlines how much of the organisation the ISMS will cover. For example, an organisation may choose to implement a ISMS for just one of their sites. Section 4.3 of the ISO 27001 standard details the requirements for determining the scope.

✓ Awareness

Communication is key, there will be changes that will affect all employees, stakeholders and possibly some members of the supply chain. Everyone should be aware of the new processes and procedures contained in the ISMS. Regular updates, and in some cases training, are recommended.

✓ During the Audit

Your ISMS will introduce various procedures including:

- Information security policy
- Risk assessment
- Risk treatment plan
- Internal audit
- Security roles
- Monitoring and measuring
- Corrective actions

✓ Paperwork

You will need to compile documentation to demonstrate how your ISMS works. Our clients say that our online templates and toolkits really help them with this.

✓ Reap the Rewards

Once your ISMS is fully in place and compliant to the ISO 27001 standard, your business can then start seeing the benefits. These include, mitigation to the risk of a cyber breach, boosted client confidence and the opportunity to tender for more work.

CLICK HERE FOR THE ISO 27001 ULTIMATE GUIDE