





# We spend over **1 million hours** each year improving the performance of businesses around the world



This experience allows us to see first-hand how ISO/IEC 27001 can help organizations to continually improve and deliver real benefits.

Business issue	How ISO/IEC 27001 helps	Benefit to your organization
 <p><b>Reputation</b></p>	<ul style="list-style-type: none"> <li>• Helps you identify risks to your information and put in place measures to manage or reduce them</li> <li>• Helps you put in place procedures to enable prompt detection of information security breaches</li> <li>• Requires you to continually improve your Information Security Management System (ISMS)</li> </ul>	<ul style="list-style-type: none"> <li>• Improved reputation and stakeholder confidence</li> <li>• Better visibility of risk amongst interested parties</li> <li>• Builds trust and credibility in the market to help you win more business</li> </ul>
 <p><b>Engagement</b></p>	<ul style="list-style-type: none"> <li>• Requires you to identify all internal and external stakeholders relevant to your Management System ISMS</li> <li>• Requires you to communicate the ISMS policy to and ensure that the workforce understands how they contribute to it</li> <li>• Top management need to define ISMS roles and ensure individuals are competent</li> </ul>	<ul style="list-style-type: none"> <li>• Improved information security awareness amongst all relevant parties</li> <li>• Reduces likelihood of staff-related information security breaches</li> <li>• Shows commitment to information security at all levels of the business</li> </ul>
 <p><b>Compliance</b></p>	<ul style="list-style-type: none"> <li>• Gives you a framework which helps you to manage your legal and regulatory requirements</li> <li>• Makes you review and communicate your regulatory requirements to other interested parties</li> </ul>	<ul style="list-style-type: none"> <li>• Reduces the likelihood of fines or prosecution</li> <li>• Helps you comply with relevant legislation and helps make sure you keep up-to-date</li> </ul>
 <p><b>Risk management</b></p>	<ul style="list-style-type: none"> <li>• It makes you assess risks to information security so you can identify potential weaknesses and respond</li> <li>• Requires you to put in place controls that are proportionate to the risks</li> <li>• Requires you to continually evaluate risks to your information security and make sure the controls you put in place are appropriate</li> </ul>	<ul style="list-style-type: none"> <li>• Helps you protect your information so you can continue business as usual and minimize disruptions</li> <li>• Gives cost savings by minimizing incidents</li> <li>• Ensures information is protected, available, and can be accessed</li> </ul>

# Top tips on making **ISO/IEC 27001** effective for you

Every year we have interactions with tens of thousands of clients. Here are their top tips.

**Top management commitment** is key to making implementation of ISO/IEC 27001 a success. They need to be actively involved and approve the resources required.

Think about how **different departments work together** to avoid silos. Make sure the organization works as a team for the benefit of customers and the organization.

**Review systems, policies, procedures and processes** you have in place – you may already do much of what's in the standard, and make it work for your business. You shouldn't be doing something just for the sake of the standard – it needs to add value.

**Speak to your customers and suppliers.** They may be able to suggest improvements and give feedback on your service.

**Train your staff to carry out internal audits of the system.** This can help with their understanding, but it could also provide valuable feedback on potential problems or opportunities for achievement.

And finally, when you gain certification celebrate your achievement and use the **BSI Assurance Mark** on your literature, website and promotional material.



"The earlier that organizations talk to senior managers, the better it will go for them so have those discussions early".

John Scott, Overbury, leading UK fit-out and refurbishment business



"The key to implementing the standard lay in getting staff to think about information security as an integral part of the daily business and not as an additional burden".

Mr. Thamer, Ibrahim Ali Arab, Assistant General Manager I.T.



"Don't try and change your business to fit the standard. Think about how you do things and how that standard reflects on how you do it, rather than the other way around".

Paul Brazier, Commercial Director, Overbury



"This certification allows us to go one step further by offering our customers the peace of mind that we have the best controls in place to identify and reduce any risks to confidential information".

Jitesh Bavisi, Director of Compliance, Exponential-eBavisi



"The course was loaded with practical exercises and real-case scenarios and was structured in a way that it encouraged participants to be interactive and share their experiences in information security".

Nataliya Stephenson Manager, Information Security, NSW Attorney General's Department

