

BS7799 Compliance and Certification



Step by step guidance to achieving BS7799 compliance or certification and maximising the business benefits

BS7799, the British Standard for information security management, affords a proven framework for organisations to improve the effectiveness of their information security processes.

Achieving compliance or certification requires a methodical approach, careful consideration of scope and a thorough understanding of your information security needs.

As one of the first organisations to achieve full BS7799 certification, Insight is well placed to advise you on the steps required to ensure that your information security practices conform to those identified in the Standard. Our experts are able to:

- Help you determine the areas of your business that should seek compliance
- Provide advice on interpreting the standard
- Identify the improvements required to your existing security processes

- Provide expertise in specialist areas such as risk assessment, business continuity, penetration testing and security awareness
- Interpret auditor requirements and negotiate with them during certification.

Scoping the project

Correctly scoping a BS7799 project is a crucial first step in any compliance initiative, and we'll help you identify the business processes critical to your organisation and which would be best targeted for initial compliance to the Standard.

We can also advise you on the merits of certification versus compliance, assist you in selecting a certification body and help you to identify, and articulate, the benefits of BS7799 so that a robust business case can be presented to your board or senior management.

And, with complex organisations, Insight has proven expertise in identifying successful, progressive compliance programmes based around an initial ISMS scope.

SIEMENS

Global network of innovation

Insight Consulting

Identifying the gaps

Undertaking a gap analysis is an essential next step and our consultants will perform a thorough assessment of your existing security arrangements and compare them against those required by the Standard.

We'll then develop a comprehensive report identifying the work required to become compliant as well as an action plan that includes prioritised and costed actions for security improvement.

Addressing the risks

Risk assessment is a mandatory component of BS7799 and we'll help you analyse the levels of information security risk inherent in your business processes. Assessments can be performed using tools such as CRAMM, or by manual methods.

Following the assessment, a risk treatment plan can be created which defines the outstanding security controls required to counter the risks identified. This allows you to demonstrate – to an auditor, for instance – that you've taken actions to reduce your residual risk to an acceptable level.

Introducing improvement

By rationalising the actions from the gap analysis and the recommended controls from the risk assessment, a formal Security Improvement Programme can now be developed.

Insight can provide whatever level of support you require to implement the required security improvements and is able to suggest practical solutions in each of the different areas of the Standard.

Our consultants can additionally help you create a Statement of Applicability (SoA) – a key reference document that explains the relevance of each security control and how it has been implemented within your organisation.

Importantly, the format adopted by Insight for an SoA introduces proven business benefits. It can act, for example, as a high-level policy document, as a baseline for internal audit or as the basis for service level agreements with other departments or third party organisations.

Preparing for certification

If you've chosen to seek certification to BS7799 – and our consultants will explain both the benefits and the relatively minor, additional costs involved – Insight can prepare you for certification and help you implement any final changes necessary to your ISMS.

Finally, we can assist during the audit process itself by dealing with a certification body on your behalf and addressing any audit observations that arise. Interpreting the Standard is often a complex process and many Insight clients have found our involvement to be highly beneficial during this final, crucial stage.

Key features

- All levels of support from complete outsourcing of a compliance project to agreed levels of guidance
- Proven experience in reviving 'stalled' compliance programmes
- Structured approach combines achieving compliance whilst maximising business benefits
- Scheduled or onsite training courses provide expertise to manage internally resourced BS7799 projects.



Insight Consulting is the specialist security, compliance and continuity unit of Siemens Communications and offers a complete, end-to-end portfolio encompassing:

- Research
- Consultancy
- Testing
- Implementation
- Training
- Recruitment
- Managed services

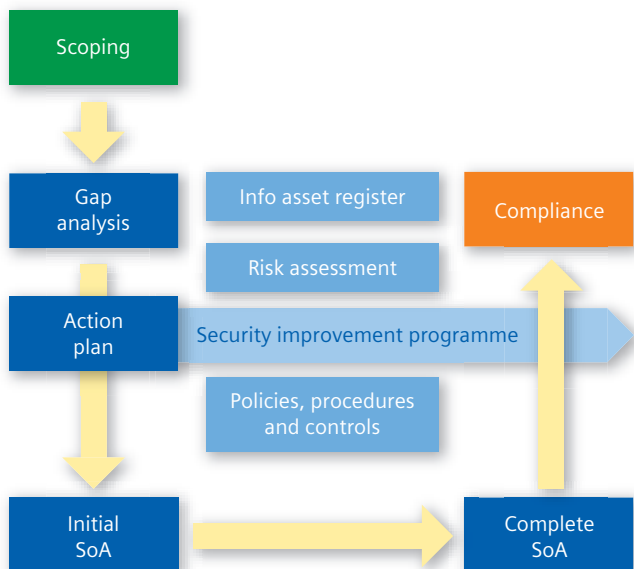
Insight is BS7799 certified, is a GCat and S-Cat (Category 7) supplier and subscribes to the CESG Listed Advisor Scheme (CLAS) and CHECK services.

If you'd like to discuss how Insight could help you manage risk in your organisation, email us at insight@insight.co.uk or visit our web site at www.siemens.co.uk/insight

Insight Consulting

Churchfield House
5 The Quintet
Churchfield Road
Walton on Thames
Surrey KT12 2TZ
United Kingdom

Tel: +44 (0)1932 241000
Fax: +44 (0)1932 244590
www.siemens.co.uk/insight



Insight's proven methodology for achieving BS7799 compliance and certification