

IT Security Technical Assurance



Demonstrating to management, auditors and business partners that your IT infrastructure and critical business applications are secure

Effective security is now a necessity for today's businesses. For some, the drivers will be regulatory requirements such as Basel 2, Sarbanes-Oxley or Turnbull. For others, the need to demonstrate assurance to industry standards like BS7799 may be the goal.

But whatever the driver – and however good your intentions – commitment alone is no longer sufficient. Management, auditors and business partners now demand tangible evidence of the security controls you've implemented and how they'll reduce risk.

How Insight can help

Insight has drawn on its broad experience of client engagements to develop a three-stage methodology for establishing assurance in the security of an IT infrastructure. It's a proven approach that can be used as part of:

- A major change to your IT infrastructure
- Implementing a new business application
- Preparing for an internal or external audit
- Project or corporate risk assessments
- Changes in working practices
- Moving to a new office location
- A merger or acquisition.

Is it complete?

Whether it's part of a specific assurance programme – or just providing support for an existing project – Insight's Security Assurance Team will help you review your IT security policies, standards and procedures against a reference model for the industry sectors you operate in. Using

this information, we can then determine whether your IT security strategy is complete and help you compile a high-level action plan for security improvement.

Is it correct?

Having established the completeness of your strategy, a technical survey and vulnerability assessment will then establish whether your IT security infrastructure is correct. Our specialists will also compile a detailed asset report of your network, IT systems and key business applications together with short term technical recommendations and strategic planning guidelines for security.

Is it effective?

Testing is an essential, third stage that will confirm whether your strategy and infrastructure will be effective against the type of threats your organisation faces. Using a mix of automated and manual penetration testing techniques, our experts will confirm whether any of the vulnerabilities that have been identified could be exploited and used as the basis of an actual attack on your network and critical business applications.

SIEMENS

Global network of innovation

Insight Consulting

Is it effective?

Security Testing

Is it correct?

Technical Survey

Is it complete?

Security Review

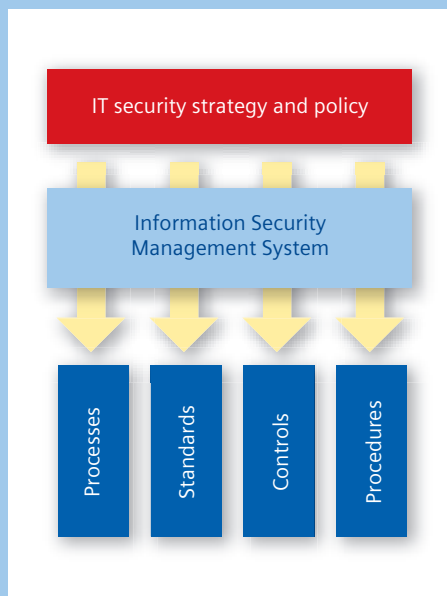
Insight's methodology for establishing assurance in the security of your IT infrastructure. We can conduct the entire process for you or work with your own specialists as part of an existing project.

Security Review

Incidents happen to all organisations – the only variation is the extent of the damage and an organisation's ability to contain it

Is your IT security strategy complete?

An Insight Security Review is an important first step in establishing whether your IT security strategy is both appropriate for the way you make use of information technology as well as being adequate for the type of risks you'll face when conducting business electronically.



Some questions to consider

- Are you confident your IT security strategy is adequate and up to date?
- Could you demonstrate compliance to BS7799 or other industry benchmarks?
- Do you have an ongoing security improvement programme?

What we'll do

- Review your IT security policies, technical standards and procedures against a relevant industry reference model
- Assess your IT infrastructure security strategy and whether it is being applied correctly.

What you'll receive

- IT security gap analysis tailored to your industry sector's compliance requirements
- High-level recommendations for security policy updates or extensions
- Advice on the most effective methods of addressing the gaps identified.

Technical Survey

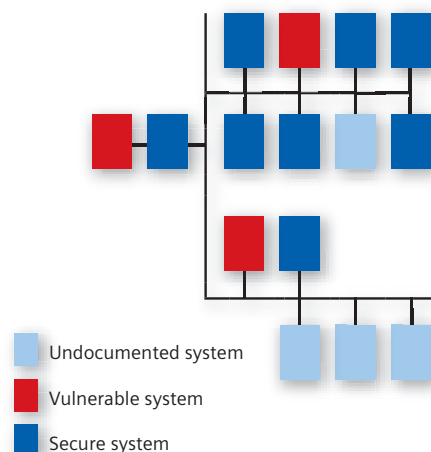
Just a single insecure or rogue system can easily compromise a carefully planned IT security strategy

Is your technical infrastructure correct?

Without a correctly documented and tested IT infrastructure, it's impossible to assess its security or the impact of change. Insight's Technical Survey service will provide you with an up-to-date inventory of your entire technical infrastructure together with its points of vulnerability.

Some questions to consider

- Can you accurately identify where your IT security vulnerabilities lie?



An up-to-date inventory of your technical infrastructure will help you determine the impact of change and identify single points of failure.

- Do you have rogue servers, redundant firewalls or poorly located intrusion detection systems?
- Do you know where you should be focusing your security testing effort?

What we'll do

- Technical infrastructure mapping exercise
- On-site vulnerability assessment including server and application configuration reviews
- Assess the suitability of your IT security architecture and whether it delivers ROI.

What you'll receive

- Detailed IT infrastructure topology and vulnerability assessment report
- Technical improvement plan including recommended security architecture changes
- Strategic planning guidelines identifying longer term security initiatives.

Are your network, IT and application controls effective?

Vulnerability scanning identifies weaknesses in your network but won't confirm their exploit potential. Insight's Security Testing service uses a variety of penetration testing techniques to identify vulnerabilities that could be exploited and the real impact they could have on your IT systems and critical business processes.

Some questions to consider

- Can you demonstrate to auditors that old or new exploits couldn't be used against you?
- Could you detect an insecure wireless network that was operating in your office?
- Are your developers conversant with secure coding techniques and do they apply them?

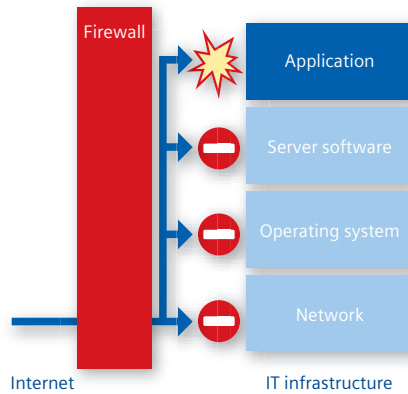
What we'll do

- Internal or external penetration testing using zero- or full-knowledge approach
- Testing of applications using specific techniques such as XML or SQL injection

- Review of your application development and database configuration standards.

What you'll receive

- Prioritised recommendations for closing exploitable IT or application vulnerabilities
- Advice on how your security testing strategy could be improved
- Secure application coding and database configuration improvement plan.



Most vulnerability scanning tools are unable to identify application layer problems – especially those that may exist in bespoke applications.

Security Testing

A combination of testing methods – tailored to an organisation's threat model – will provide the most effective results

Ongoing assurance

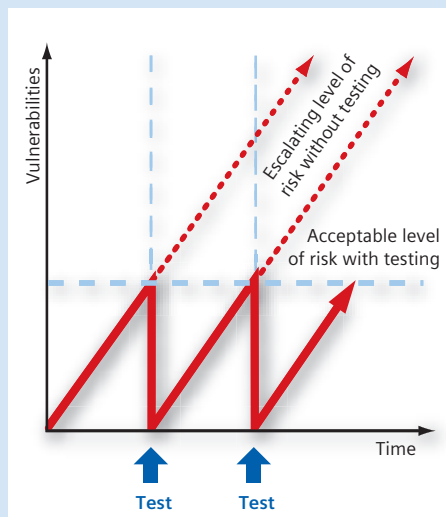
Change is a constant in any discussion of security. Just consider the changing nature of threats, for example.

Whilst network-level attacks are still common – and clearly need to be guarded against – hackers are increasingly turning their attention to application-level vulnerabilities. Unfortunately, because these exploits often masquerade as legitimate traffic, traditional blocking or detection methods are often ineffective against them.

Managing your level of risk

Whilst any investment in reviews, surveys and testing will help to reduce risk, without regular ongoing activity, new threats and vulnerabilities will invariably be discovered or introduced which will progressively increase the level of risk your business faces.

Insight offers a range of ongoing security assurance service options which will help you to regularly re-establish an acceptable risk threshold for your IT infrastructure and business systems.



A regular security review and testing programme will reduce the risks your organisation faces to a commercially acceptable level.

Insight can advise you on the optimum review frequency based on factors such as the use you make of IT and the nature of your business.

Using a partner

Without the correct tools and expertise, conducting a security review or testing programme can be a resource-intensive and time consuming activity.

That's why, despite increased awareness and IT security budgets, most organisations still find it more cost effective to work with a security services partner when undertaking a review of their technical infrastructure.

Why Insight?

With a client base of over four hundred different UK organisations, Insight has an enviable reputation for delivering practical solutions that are both business-driven and cost-effective.

Our security assurance team regularly conducts assignments for both public and private sector organisations and has established a proven track record of:

- Delivering projects on time and to agreed cost and quality objectives
- Maintaining broad and up-to-date experience of the risks and threats facing specific industry sectors
- Developing reports that are focused and tailored for the audiences involved
- Providing the correct mix of tactical and strategic advice for security improvement.

For more information or advice on Insight's IT Security Assurance services, visit www.insight.co.uk/assurance

Key features

- Structured approach to demonstrating assurance in your IT infrastructure and application security controls
- Access to specialist resources with knowledge of the latest tools, techniques and security exploits
- Clear recommendations for tactical and strategic security improvement
- Improved return on investment from your security strategy.



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 Consulting has one of the most respected security assurance teams in the UK. Many of our consultants subscribe to the Government's CESG Listed Advisor Scheme (CLAS) and all of our testing specialists subscribe to the CESG CHECK service.



Insight is also fully certified to the BS7799 standard for information security.

