

# Security Operations Audit

*Secure your operations with one quick, expert, fixed-price engagement*

*Concerned whether you are meeting your data protection obligations?  
Worried about the data you hold on your customers leaving your business?  
Suspect you have vulnerabilities but don't know where to go for advice?*

Virtuous Networking's Security Operations Audit has been designed to answer these questions. With one short, sharp engagement, our security experts will analyse your processes, procedures and technology, and provide you with clear, actionable, prioritised advice for how you should secure your business against insider and external threats.



The Audit has been designed specifically with small and medium businesses in mind, concentrating all on-site effort into two days of expert analysis. By using the best people in the industry, we do the job quickly and quietly, limiting the impact on you and your team.

You will get a comprehensive report listing the vulnerabilities found, the impact of those vulnerabilities, and what to do about them. This can be used by management to balance investment decisions against risk, by Operations to create safe, secure operating procedures, and by IT to close dangerous holes in your security net.

Virtuous Networking's Security Operations Audit gives you the information you need to manage information security risks in an increasingly complex and inter-connected world.

***Understand your risks***  
***Meet your legal obligations***  
***Demonstrate commitment to securing customer data***

## Security Operations Audit - 3 Step Process

### Step 1: Interview and Inspection Review

Review admin methods, access controls, documentation, change control and logging.  
Interview IT staff to assess existing procedures and technical counter-measures.  
Interview sample non-IT staff to assess their security awareness and behaviour.  
Benchmark against best practice.

### Step 2: Internal Network Discovery and Penetration Test

Map internal network and attempt to identify relevant devices, including routers, switches, servers, workstations, printers and access points.  
Test sample routers and switches for secure configuration.  
Examine a sample of other devices offering management interfaces, including printers, backup units, wireless access points and IP telephony.  
Anonymous Windows testing: conduct penetration test, attempting to gain access to business-sensitive information, technical configuration information and user credentials.  
Authenticated Windows testing: Examine the security of Windows domains and standard desktop build, using a desktop PC and a non-privileged Windows account.  
Evaluate controls designed to protect business-sensitive information, technical configuration information and user credentials.

### Step 3: Report Findings

*Management Summary:* Each report contains a plain English management summary. It summarises the vulnerabilities present and an overall assessment of the environment.  
*Recommendations Section:* Details the vulnerabilities discovered, categorised by risk. Provides information on each vulnerability, why it matters, and mitigation. Mitigations may include changes to responsibilities, reporting mechanisms, awareness education, procedural changes, contractual changes and technical changes.  
*End of Project Teleconference:* At the end of the review an end of project teleconference is held, providing an opportunity to review the project and ensure clear actionable conclusions can be drawn.

The Virtuous Networking Security Operations Audit is available for businesses of up to £10M turnover for a fixed cost of £3,750 (plus VAT). Larger businesses may well also qualify at this price.

**Virtuous**  
Networking

Virtuous Networking Ltd  
4th Floor, Bush House, 72 Prince St, Bristol, BS1 4QD, UK  
+44 (0)117 328 1483 | info@virtuousnetworking.com | www.virtuousnetworking.com