



Using External Security Specialists  
Good Practice Guide

September 2004

# Good Practice Guide on Using External Security Specialist

Document History	Version	Date of Issue
	01	24 September 2004

## DISCLAIMER

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

NISCC shall also accept no responsibility for any errors or omissions contained within this document. In particular, NISCC shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

**National Infrastructure  
Security Co-Ordination Centre**  
PO Box 832  
London  
SW1P 1BG

Tel: 020 7821 1330 Ext 4511  
Fax: 020 7821 1686  
Email: [enquiries@nisc.gov.uk](mailto:enquiries@nisc.gov.uk)  
Web: [www.nisc.gov.uk](http://www.nisc.gov.uk)

## **USING EXTERNAL SECURITY SPECIALISTS**

The primary focus of NISCC is protecting the UK CNI from the threat of electronic attack. Within that remit NISCC can provide direct assistance to CNI partners by providing access to specialist expertise in a range of Government departments, but companies will often need to use external security specialists for a variety of work including consultancy and IT Health Check.

NISCC does not endorse any particular products or services, but this note attempts to assist in the choice of a reputable provider for this work, by raising awareness of a range of information security qualifications that consultants may possess. Obviously these will only be one factor in the choice of consultant. (Most certifications are vendor-neutral, which gives the holders the necessary broad background, and knowledge of vendor-specific technologies will not be covered.) More detailed information can be obtained from the organisations concerned.

We also offer some guidance on handling contracts with external security specialists.

### **DTI Study on Information Security Consultancy**

In 2001 the DTI commissioned a study to look at existing and emerging issues impacting on the confidence users may have in the supply of information security services. (This was occasioned by the debate surrounding the issue of whether the Private Security Industries Act should encompass information security consultants). Views were collected from a range of providers and buyers of information security consultancy and services, and other interested bodies. The study concluded that there were no perceived problems with the integrity of providers in the UK who focus on information security issues, but did suggest that users of these services needed to be better informed on the scope of the services and how to procure them. The resulting report makes a number of recommendations to address the issues raised.

(See [www.dti.gov.uk/industry\\_files/pdf/psirep.pdf](http://www.dti.gov.uk/industry_files/pdf/psirep.pdf))

## **Information Security Accreditation Schemes and Qualifications**

### **BCS (British Computer Society)**

[www.bcs.org](http://www.bcs.org)

BCS offers certificates in various areas of IT, including Information Security, and also maintains a register of its members who can provide advice and expertise as security specialists.

### **ISEB (Information Systems Examinations Board) - Information Security Management Certificate**

This is designed to prove that the holder has a good knowledge and basic understanding of the wide range of subject areas making up IS management.

Requirements:

- Minimum of 12 months experience in IT
- Accredited training course or six months experience in a security control activity
- Exam pass

ISEB also offer a certificate in IS Consultancy Practice.

#### BCS Professional Advice Register – Security

Requirements:

- Professional member of BCS or affiliated
- Six years experience in Information systems/ three years in Information Systems Security
- Assessment by written application and interview
- Annual renewal

A list of registrants can be viewed on the BCS website.

#### **CESG – CESG Listed Advisor Scheme (CLAS)**

([www.cesg.gov.uk/site/clas/index.cfm](http://www.cesg.gov.uk/site/clas/index.cfm))

Through CLAS, CESG has accredited a pool of high quality Information Assurance Consultants on which HMG and the wider public and CNI sectors can draw for a range of Information Assurance related services. Candidates applying for CLAS membership must satisfy a CESG panel that they have the right mix of formal qualifications and experience. Once accepted on to the Scheme, members must attend regular training events to ensure that they are aware of and fully understand all relevant government policy.

Requirements:

- Evidence of professional qualifications, membership of professional bodies and relevant experience - these demonstrate that the consultant has the right level and mix of knowledge
- Evidence against a Core Competency Framework - this demonstrates that the consultant has the ability to put that knowledge into practice effectively.
- CLAS consultants are also required to provide good quality references from two previous clients

Details of CLAS consultants are listed on the CESG website.

#### **CISSP (Certified Information Systems Security Professional)/SSCP (Systems Security Certified Professional)**

[www.isc2.org](http://www.isc2.org)

The International Information Systems Security Certificate Consortium, or (ISC)<sup>2</sup>, was established in 1989 to develop a certification program for information systems security practitioners. These are becoming recognised as international security qualifications.

CISSP

Requirements:

- At least four years full-time security professional work or three years + degree
- CISSP exam pass (250 multiple-choice questions in 10 topic areas)
- Endorsement by another CISSP

- Re-certification every three years – accomplished through continuing professional education.

Individuals holding CISSP certification are entitled to be listed in the CISSP Directory

## SSCP

### Requirements

- At least one year's work experience in one of the information security test domains
- SSCP exam pass (125 multiple-choice questions in seven topic areas)
- Re-certification every three years – accomplished through continuing professional education

## **Degree Courses – MSc in Information Security**

There are three MSc courses in Information Security in the UK, one at Royal Holloway College, University of London and the others at Westminster University and University of Glamorgan, all requiring the equivalent of a year's full-time study. Royal Holloway College also offers a diploma course.

[www.isg.rhul.ac.uk](http://www.isg.rhul.ac.uk)

[www.wmin.ac.uk](http://www.wmin.ac.uk)

[www.glam.ac.uk](http://www.glam.ac.uk)

## **Penetration Testing/IT Health Checks**

### CESG – CHECK scheme

[www.cesg.gov.uk](http://www.cesg.gov.uk)

CESG has developed a special partnership with industry to approve companies for work on systems processing some protectively marked material. To apply for membership a company must submit

- details of company methodology
- at least two examples of Health Check reports
- two independent references from companies for whom it has done work
- CVs of team members

And at least one member of the Health Check team must pass the CHECK 'assault course'

(At the time of writing no other similar schemes exist.)

## **Contracts with External Security Specialists**

It is vital that relationships with any third party organisations that have access to your information are managed effectively. Ensure that any contracts you have include relevant clauses outlining information security responsibilities. A common practice is to request third parties to agree to abide by your information security policy.

Examples of some of the areas that such a contract may cover include

- the general policy on information security
- a description of the service provided
- target levels of service
- the respective liabilities of parties
- responsibility with respect to legal matters (data protection legislation and IPR)
- access control agreements