

Penetration testing and vulnerability assessment

How robust is your network?

The answer may surprise you. Using sophisticated penetration testing techniques, our expert team can help you to identify security weaknesses in your organisation's information systems, and suggest ways to strengthen your defences.

Comprehensive testing services

Penetration testing is an invaluable way to test the resilience of your network, pinpointing vulnerable areas and identifying ways to protect your information more effectively. By simulating a malicious attack on your systems, we can conduct penetration testing in three different ways:

- **Full disclosure ('white box') testing**
Testers have complete knowledge of the infrastructure to be tested – often including network diagrams, source code and IP addressing information
- **Partial disclosure ('grey box') testing**
Testers are provided with limited information about the infrastructure to be tested
- **Blind ('black box') testing**
Testers have no prior knowledge of the infrastructure to be tested

Experienced consultants

All QCC penetration testing and vulnerability assessment consultants are trained to the highest standards, holding qualifications such as:

- CREST
- CHECK
- CEH

All these qualifications are backed up with many years of industry experience in testing, assessment and report writing.

Vulnerability testing services

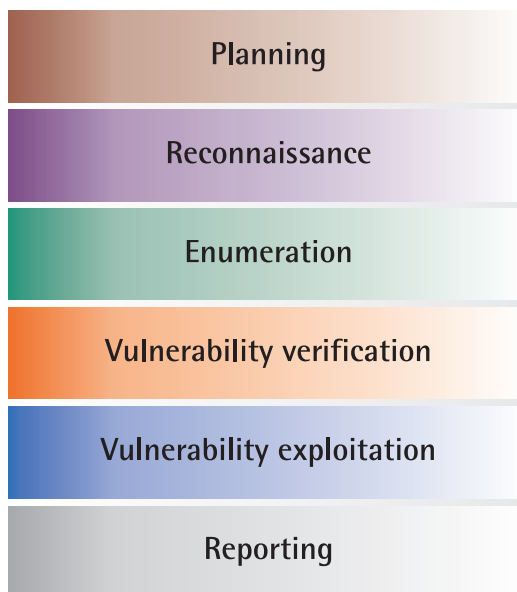
Along with comprehensive penetration testing, QCC also offers vulnerability scanning and remediation services. QCC is well positioned to deliver detailed reports on vulnerabilities found within the network architecture, utilising industry standard tools such as:

- GFI Languard
- Nessus
- Burp Suite

Proven approach

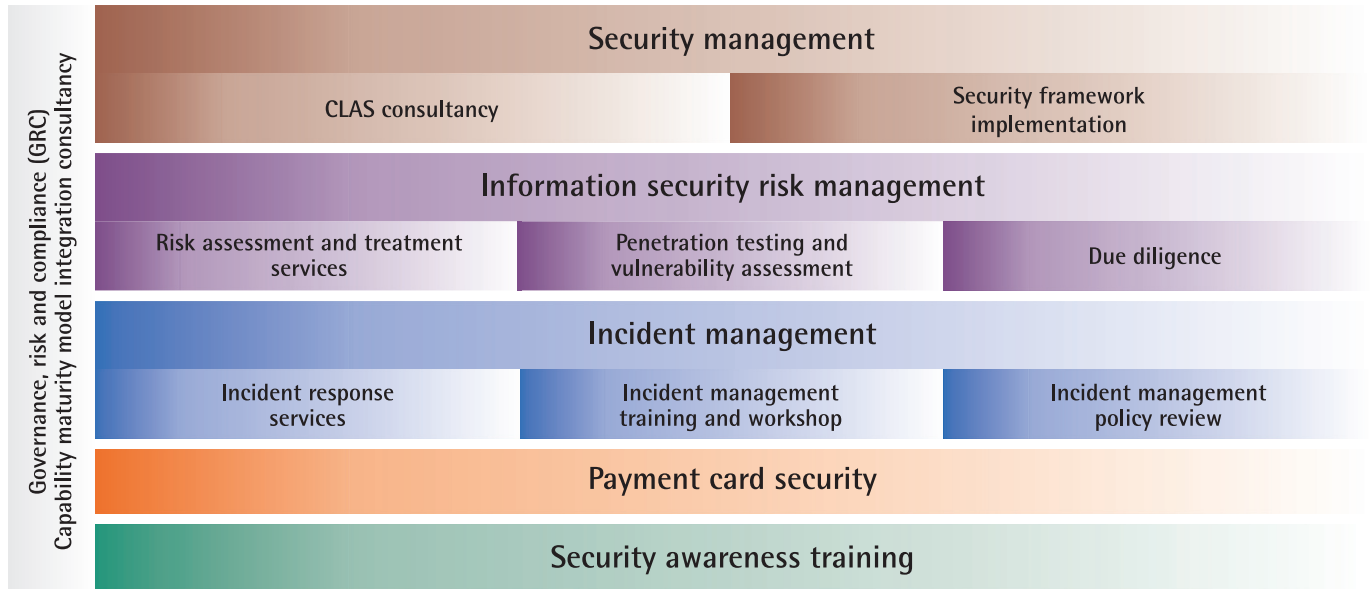
Using our tried and trusted approach, QCC's experienced testers will identify and quantify your technical vulnerabilities, establishing key areas of concern and making recommendations about how best to address them. Key stages are as follows:

- **Planning**
Acceptable timeframes, agreed target systems, methods of operation and, most importantly, the system owner's consent are just a few of the many items that need to be addressed before a test can commence
- **Reconnaissance**
Testers attempt to gain as much knowledge as possible about the target network
- **Enumeration**
The tester will attempt to identify the open ports and services available on the systems of the target network
- **Vulnerability verification**
Sophisticated scanners are used to identify vulnerabilities on the target network
- **Vulnerability exploitation**
Using a combination of automated and manual techniques, our testers begin the process of exploiting vulnerabilities in order to establish their extent
- **Reporting**
We provide a report detailing both findings and recommendations



QCC security and risk management services

Our comprehensive portfolio of security and risk management services provides support across every aspect of information security.



About QCC

Established in 1996 as one of the first independent information security companies in Europe, QCC has a strong reputation across all areas of proactive and reactive security and risk management services. These include security management consultancy, risk assessment and digital forensics, as well as payment card security and security awareness training.

With considerable experience working in the public and private sector, our highly-skilled consultants are uniquely placed to help you develop a clear and robust information security strategy for your organisation.

Identify. Quantify. Fortify.

Contact us

For further information on any QCC services and products, call us on +44 (0)20 7353 9000, email us on info@qccis.com, or visit www.qccis.com.



**QCC Information Security Ltd • Buchanan House
24-30 Holborn • London EC1N 2LX • UK**

Tel: +44 (0)20 7353 9000

Email: info@qccis.com

Web: www.qccis.com

This publication is for general guidance only and information in it is subject to change without notice. Please contact QCC Information Security Ltd for latest information on QCC products and services. No part of this publication may be reproduced or transmitted, in any form or by any means, or stored in any retrieval system of any nature, without prior written permission of QCC Information Security Ltd, except for fair dealing under the Copyright, Designs and Patents Act.

© Copyright QCC Information Security Ltd. 2011. All Rights Reserved.

QCC-MKTG110813a-MS-Info Sheet Penetration Testing-v2

