- Pre-site Inspection
  - Introduction
    - Testing organisation history and background.
    - Authority to test i.e. Request from company, corporate headquarters or potential buyer of company.
    - Detailed Proposal of test and services that are proposed to be carried out.
    - Capability Statement of the testing organisation i.e Core competencies/ limitations/ timescales etc.
    - Tools to be utilised if requested.
  - Accreditation Status
    - Interim
    - Re-accreditation
    - Full
  -

Scope of Test

- Stage of Lifecyle
  - Interim Operating Capability i.e. Development build/ beta stage.
  - Final Operating Capability i.e. Project at customer acceptance stage.
  - Major upgrade i.e. Software/ hardware update.
- Test Type
  - Compliance Test
    - Basically an audit of a system carried out against a known criterion. A compliance test may come in many different forms dependant on the request received but basically can be broken down into several different types:
      Operating Systems and Applications: A verification that an operating system and/or applications are configured appropriately to the companies needs and lockdown requirements, thus providing adequate and robust controls to ensure that the Confidentiality, Integrity and Availability of the system will not be affected in its normal day to day operation.
      Systems in development: A verification that the intended system under development meets the configuration and lockdown standards requested by the customer.
      Management of IT and Enterprise Architecture: A verification that the in-place IT management infrastructure encompassing all aspects of system support has been put in place. This is to ensure effective change control, audit, business continuity and security procedures etc. have been formulated, documented and put in place.
      Interconnection Policy: A verification that adequate security and business continuity controls governing the connection to other systems, be they Telecommunications, Intranets, Extranets and Internet etc. have been put in place, have been fully documented and correspond to the stated customer requirements.
      - Full credentials Supplied
      - Full access to Network diagrams and schematics
      -

- Full access to Configuration scripts and files
- Compliant with:
  - Customer Defined
  - Government Assurance Pack
  - HIPAA
  - ISO27001
  - Microsoft Lockdown
  - NSA Lockdown
  - Sorbanes Oxley
  - Etc.

- Vulnerability Assessment
  - Vulnerability assessment is a process of identifying and analysing a system or network for any potential vulnerabilties, flaws or weaknesses that could leave it open to exploitation.
    - Full credentials Supplied or limited to basic user credntials dependant on level of test
    - Full access to Network diagrams and schematics
    - Full access to Configuration scripts and files
- Penetration Test

A Penetration Test is essentially an evaluation of a system or networks current state of security and its likelihood to be susceptible to a successful attack by a malicious hacker or nefarious user. The process involves enumeration and scanning for any technical flaws or vulnerabilities. After such flaws are found, attempts are then made to penetrate inside the network and gain a foothold. Once this has been established, attempts are then made to utilise trusts and relationships to gain further ingress into the domain.

- Type of Test
  - White-Box
    - The testing team has complete carte blanche access to the testing network and has been supplied with network diagrams, hardware, operating system and application details etc, prior to a test being carried out. This does not equate to a truly blind test but can speed up the process a great deal and leads to a more accurate results being obtained. The amount of prior knowledge leads to a test targeting specific operating systems, applications and network devices that reside on the network rather than spending time enumerating what could possibly be on the network. This type of test equates to a situation whereby an attacker may have complete knowledge of the internal network.
  - Black-Box
    - No prior knowledge of a company network is known. In essence an example of this is when an external web based test is to be carried out and only the details of a website URL or IP address is supplied to the testing team. It would be their role to attempt to break into the company website/ network. This would equate to an external attack carried out by a malicious hacker.
  - Grey-Box
    - The testing team would simulate an attack that could be carried out by a disgruntled, disaffected staff member. The testing team would be supplied with appropriate user level privileges and a user account and access permitted to the internal network by relaxation of specific security policies present on the network i.e. port level security.
- Exclusions
  -

- Social Engineering Attacks
- Denial of Service Attacks etc.
- See also Exemptions from test section.

- Purpose of Test
  - Deployment of new software release etc.
  - Security assurance for the Code of Connection
  - Interconnectivity issues.
  - Deployment of wireless networks on wired LAN.
  - ISO27001/HIPAA etc. Compliance

- Obtain appropriate Network details (dependant on level of test.)
  - Peer to Peer, Client-Server, Domain Model, Active Directory integrated
  - Number of Servers and workstations
  - Operating System Details
  - Major Software Applications
  - Hardware configuration and setup
  - Interconnectivity and by what means i.e. T1, Satelite, Wide Area Network, Lease Line Dial up etc.
  - Encryption/ VPN's utilised etc.
  -

- Role of the network or system

- Obtained signed Authority to Test
  - CEO
  - Risk Manager
  - System Manager
  - Data Owners
  - Security Officer
  - Relevant ISP

- Non-Disclosure Agreement
  - Full i.e. All information in relation to this task cannot be distributed/ used in research, training, marketing etc.
  - Limited i.e. Certain information can be used in marketing/ training and research scenarios after agreement has been sort from the customer.
  - None i.e. All information is freely distributable and not under any restrictions whatsoever.

- Special Clearances required
  - Government vetting
  - CHECK Team qualified
  - Mastercard certified

-

Known waivers/exemptions

- Known to Risk Manager
- Risk Assessments completed
- Exemptions from test
  - Development builds
  - Joint-owned equipment
  - Laptops
  - Trial Applications
  - Unstable Hosts
  - Supplied Network infrastructure for the test only

- Contractural constraints
  - Are there any Service Level Agreement in place that may affect the scope of the test
  - Waiver letter required for test from contractural partners (this document is required in conjunction with Authority to test above.)

- Local equipment requirement
  - CAT5 taps and speed
  - Fibre taps/converter requirement
  -

- Local Internet access
  - Filtered
  - Unfiltered
  - Downloads/exports allowed
- Office space
- Power available
- Refreshments

- Local manpower requirement
  - Application administrators
  - Database administrators
  - Network administrators
  - Operating System administrators

- Points of Contact
  - Risk Manager
  - Database Administrator
  - Local Security Officer
  - System Administrator
  -

- Networking Administrator
- ISP
- Note: - All should be named and have appropriate 24/7 contact numbers provided.

- Reporting Timescales
  - During Test
    - Normal
      - Daily Brief
      - Interim Brief
      - End of Test verbal debrief
    - Exceptional
      - Upon identifiying Critical vulnerabilities/ exploits
      - Upon identifying previous Intrusion
      - Upon finding child pornography/ other activities legally bound to report.
  - Post Testing
    - Normal timescale
    - Local requested timescale
    -

Privacy/Commercial Protective Marking required

- Distribution List

- Access to Previous tests & reports
  - Compliance Test
    - Reason for test
    - Who carried out
    - When carried out and if any rectification work was completed.
    - Release timescale
      - Start of test - This is important for a Compliance test as previous failings can immediately be re-tested and verified as secured or still vulnerable to exploit etc.
      - During test
      - End of test
  - Vulnerability Assessments
    - Reason for test
    - Who carried out
    - When carried out and if any rectification work was completed.
    - Release timescale

- Start of test
- During test
- End of test
- This can be important during a vulnerability assessment as it can be used as a guide of how the network has progressed during the time of the last test to the current period. Release of this by the customer may not be in there best interests as it is best to have an independant team to assess all vulnerabilties. The customer can then also assess the overall performance of the testing team and thus its value for money in conducting the test.

- Penetration Tests
  - Reason for test
  - Who carried out
  - When carried out and if any rectification work was completed.
  - Release timescale
    - Start of test
    - During test
    - End of test
    - Appropriate comment to be made in final report reference receipt of these documents and at what point during the test. This provides mitigation points as the information gained is privileged and was used to gain an unfair advantage in potentially accessing the network. Obviously if the documents were made available after the test, the less weight would be stressed in the final report as they would only be used for reference. This can severly disadvantage the customer as they are potentially disclosing exploitable holes within their network infrastructure. An opposite point of view is the fact that the testing team will verify any fixes that have taken place or that the exploitable hole still exists and still needs attention to mitigate or close. From the customer perspective if an exploitable hole is not discovered it can give an indication that the exploit could possibly be risk assessed and managed.

- Physical inspection
  - Major work areas where the majority of users would utilise the equipment.
  - Network equipment room where all routing infrastructure is housed and secured.
  - Server room if different from the Network equipment room.
  - Testing teams planned area of work.