



Certified Digital Security Level 6

Implementation Guidance Document

This document outlines the evidence required from an organization seeking to demonstrate that their System's Security meets the required criteria for Certified Digital Security Level 6.



This document may also be used to help an organization develop its security posture and is given openly to the community. An organization should never be asked to pay for any implementation guidance document issued by Certified Digital Security (CDS). They may pay for advice and consultancy to implement the various aspects of this Standard but that is for the organization to arrange with its contractors.

To meet the Certified Digital Security (CDS) Standard, an organization must provide evidence as to how they meet and comply with this guidance document (an extract of the CDS Master Standard).





DOCUMENT STRUCTURE

CDS Guidance Documents are formatted into 3 parts:

Part 1 is for Executive Level review and includes only the high level benefits and requirements of the CDS standard. It is designed to be separated from the rest of the document to form a single page submission.

Part 2 outlines what an organization should undertake to meet the target level (it is written for the system administrator or implementer of the work).

Part 3 articulates how the implementation of the CDS Level's requirements will be audited and what type of evidence will be required. Part 3 forms the core of the CDS Audit programme and as such, it is used by the CDS auditors to ensure the correct information and evidence is provided in the correct format.

Index

Introduction	3
Part 1 Executive Summary	4
Part 2 Requirements for Level 6.....	6
How Requirements are defined	9
Part 3 CDS Audit Requirements	27
Logistics for a CDS Level 6 Audit	54





INTRODUCTION

The Certified Digital Security (CDS) Levels were designed to allow an organization's IT administrative and security staffs to step-by-step improve their security along a path that their management can understand. As auditors, penetration testers and IT security consultants, we have been amazed by the number of organizations that have missed the basics. Horror stories of no Anti Virus software, every user having Administrator-level access, without the benefit of backups, are sadly still too common. Furthermore, in large organizations there appears to be a communications barrier between IT security implementers and management; CDS levels were designed to allow both to speak in common terms.

The CDS levels run from the starting point of level 1 to level 9, with each level building upon the benefits of those below it leading to a system that is progressively better managed, more secure and robust; the steps are reasonable, but the accumulation is very effective. To this end we see most organizations sitting between levels 3 and 6.

We believe that those responsible for security implementation will like the roadmap concept as it helps them justify and support their various business cases. Management like the CDS levels as they can quickly assess the increased business benefit that each level brings; they can weigh up the benefits and compare bids for fixed scope work to move from one level to another.

We have released the CDS Level Guidance Documents, supporting templates, and information to the public so that everyone can benefit. It doesn't matter if you are a small and tightly budgeted organization, we believe you and your customers can and should implement the methods, policies and procedures in CDS and make your systems more secure.

And let's face it, if everyone had a little more security we would all be at less risk from IT security incidents, both accidental and malicious.

Steve Armstrong





PART 1

EXECUTIVE SUMMARY





Certified Digital Security is about improving your system security in an incremental and staged process. It is about seeking independent external verification to ensure that you are actually doing what you claim you are doing. It's about being able to show clients and shareholders alike that you take data and system security seriously.

Note: A system that is aiming for level 6 will be required to fully implement, or will have already fully implemented, all of the Level 1, 2, 3, 4 and 5 requirements.

Specifically, Level 6 requires the organization to have the following:

Dedicated IT Security Staff provide focus and continuity across the business, ensuring that security receives its due regard. *Checks on regular Subcontractors* helps to foster confidence that required security is being maintained on information and assets passed outside the organization.

The use of *Virtual Private Networks* or other encryption on regular links helps to maintain the confidentiality and integrity of information as it transits across publicly accessible links. The use of *Application Layer Firewalls* creates an intelligent and more finely controlled mechanism to limit the movement of data to that needed by the business.

With Level 6 implemented, an organization can expect to see:

- A responsive Security team that are more proactive in protecting their system.
- Confidence that Subcontractors won't cause a PR disaster.
- Confidence the Subcontractors will meet deadlines through better uptime on their systems.
- A more secure boundary, to defend against application attacks.
- A more secure system as Vulnerability Analysis directs attention to where effort is needed.





PART 2

REQUIREMENTS FOR LEVEL 6





ABOUT THIS PART

Part 2 outlines what the organization should implement to achieve the Target Certified Digital Security (CDS) level. If the organization is not seeking an independent audit against their target level, they are able to pick and choose the elements they wish to implement. For these organizations, CDS is only a guide for their development and roadmap to improved security.

RECOMMENDED PROCESS

If the organization is not seeking a CDS audit of their security, we recommend the following process:

- Step 1. Use the CDS Rough Assessment Workbook to identify where the potential gaps in your security are centered.
- Step 2. Select your target level.
- Step 3. Read the standard for your target CDS level.
- Step 4. Examine your organization's security to assess how it currently measures against the standard.
- Step 5. Identify the gaps to calculate the amount of work required to meet your target level.
- Step 6. Put in place work packages to fill the gaps.
- Step 7. Integrate the security and ongoing reviews into normal business practice.

IF SEEKING AN AUDIT

If the organization is seeking an independent audit of their CDS implementation, the reader is strongly encouraged to use Part 3 as the guide to the production of the necessary audit evidence. Part 3 is only used for CDS Audits and is designed to communicate the type, quality, timeliness of data and structure of the evidence documents which are required to be presented for audit.

CDS Audits are speedy as, wherever possible, all evidence is simply being checked as to whether it is correct, relevant and compliant. CDS Audits are check sheet orientated (wherever possible) to remove any ambiguity/hearsay/interpretation or similarly subjective inputs which might cloud otherwise clear-cut objective assessments.





ABOUT CDS AUDITS AND LOGOS

It should be noted that even if the target level of the Standard is fully achieved, the right to claim any CDS compliance shall be withheld until such time as that compliance can be verified by an approved CDS Auditor and ratified by the Certification Body.

The CDS logo, title and rights of certification are vested solely in Digital Security Ltd who retains control and ownership of all materials.

RECOGNITION OF SOURCE

The CDS Standard is an open source, as we believe knowledge should be shared and not withheld. To this end, the CDS Standard and much of the information on the website (www.certifieddigitalsecurity.com) is open source and is given freely to the community.

However, as part of the terms associated with the release of CDS materials, Digital Security require that where this guidance document or any CDS source material is used to improve security, credit is given to the CDS Standard and documents are kept in the format provided.

To assist this, the documents are provided in a variety of formats (e.g. all Part 1s can be downloaded from the website for easy executive reading). Security is about trust and integrity, thus we hope, as security professionals, you can demonstrate these traits when using CDS information and material for your organization's benefit.

ANY FEEDBACK?

Any feedback is welcomed and is actively encouraged! If you have an idea or concept that would strengthen the CDS (or even a comment about a part of the CDS process that really annoys you), please get in touch via the website.



HOW REQUIREMENTS ARE DEFINED

Each CDS level has a number of requirements; these are numbered so they can be easily cross and externally referenced.

The requirement numbering includes the target level so that readers can see what requirements build upon previous levels' foundations.

For example: The fourth requirement on level 6 is indexed as REQ 6.4.

In Part 3 of this document, the CDS Audit evidence aspects are defined. These are similarly indexed:

For example: The evidence for level 6 requirement number four (i.e. REQ 6.4 as above) is noted under part 3 part SOE 6.4.

Thus, the reader can easily cross-refer to both requirement and evidentiary quality statements as REQ 6.4 is supported by SOE 6.4.

WHAT'S IN A REQUIREMENT?

Each requirement comprises the following components:

1. A requirement title (or short name).
2. Its unique requirement number.
3. A short overview of what the requirement is designed to achieve or introduce.
4. The user or group which is most likely to deliver, benefit or implement the requirement.
5. The details of the requirement itself.
6. The list of the potential benefits that may be realized through the implementation.
7. Whether the requirement is recurring and if so, the recurring period (e.g. annual training is required to be undertaken every 12 months or less).
8. Any notes relevant to the implementation of the recommendation.

Dedicated Security Staff

Requirement Number: REQ 6.1

Overview:

The organization must have staff whose primary role is IT security, to provide security support and promote awareness of the organizations goals, processes and ethos.

Responsible Group or Users:

Senior management must appoint suitable staff and maintain their independence from the system managers.

Requirement Description:

The difference between this level and CDS Level 5 is that here IT Security is the person's primary role. Within very small organizations this may still be a role that the individual undertakes along with other duties, but IT Security is their primary focus. In medium and large organizations, the individual will be dedicated to IT Security and this will be their only role.

Ideally these staff will be internal to the organization as they will already understand the functions and ethos of the organization.

They should be aware of the organizations risks and future strategies in terms of expansion, new projects and organizational changes; this will allow them to address current risks but also plan for likely future risks.

Local administrators can fulfill the function if they are trained and dedicated to the security task, although the reporting chain of these staff should be changed to that of Security Staff and not the Network Support Team.

The requirement could be outsourced to a specialist company; however, depending upon the size of the specialist company taking on this responsibility, the list of names of the Dedicated Security Staff could be long. If it is outsourced, the following points apply:

- ❖ The same named person(s) should regularly support the organization (the specialist company should be able to produce the list of names).
- ❖ Organizations must seek a face to face meeting with the head or lead IT Security person of the specialist company and ideally induct them into the organization so they may gain an understanding of the organizations methods, risks and data moving processes.
- ❖ CDS Dispensations may be made for small and very small organizations where staff

number less than 25. Note: *Applications should be made to the CDS Certification Body ahead of any audit.*

- ❖ Large and very large organizations will require several IT Security staff.
- ❖ Multi site large organizations may require staff on each site.

The key requirement is that the same person(s) support the organization and that IT Security is their primary function (usually indicated by their Job Title).

Currently, there is no international vocational examination for staff to undertake to demonstrate a level of understanding for skills and knowledge developed, derived or researched outside the class or examination room. Whilst not ideal the following skills can only be demonstrated by showing attendance of a course which meets the requirements laid down in **REQ 6.2**.

For adherence to this standard, qualifying courses will have:

- ❖ A syllabus that meets the content requirements.
- ❖ An independent examination that tests the student has understood the content of the syllabus and that they are able to demonstrate and use the knowledge gained.
- ❖ An expiry date on the certification/examination, so that without continued evidence of use (by for example Continued Professional Development (CPD)) the skills are 'retired' and no longer valid to be claimed by the holder.

Thus for individuals to meet the skill requirements, evidence should be presented of:

- ❖ Completion of the appropriate training.
- ❖ Certification to a standard that tests the required syllabus.
- ❖ The skills must be current (i.e. not retired by the course's sponsoring body) and supported by:
 - In-date certificates.
 - CPD credits for further and ongoing personal development.
 - Where training relates to products (barriers, appliances or operating systems) the certification can be no more than two versions behind the currently deployed one.

Benefits of Implementation:

By using named IT security staff the organization gains from focused and skilled personnel dedicated to the tasks of responding to, and resolving IT security incidents, greater emphasis placed on security implementation and management during normal system operation and better opportunities for the embedding of security practices into routine system configuration.

Recurring? If so frequency:

Requirement is ongoing and continuous, although it will benefit from annual review to ensure it remains in line with the organization's growth and business goals.

Mandated IT Security Staff Training

Requirement Number: REQ 6.2

Overview:

Dedicated IT Security staff must undergo formal training to equip them with the necessary skills for their role and provide evidence of their abilities to use those skills.

Responsible Group or Users:

Senior management must ensure that formal training is provided for their IT security staff and that skills are maintained through training updates as part of their training development plan.

Requirement Description:

Within the security team (of dedicated staff), the following skills and qualifications must be held; they are split into Mandatory and Optional skills.

At least one of each Mandatory skill is to be held by someone within the team; however, if the number of supported systems is large, geographically disparate or extremely complex, more than one individual with key skills will be required. Similarly, consideration should be given to routinely training more than one individual in each skill to reduce the chances of team degradation due to absence or resignation.

Currently, there is no international vocational examination for staff to undertake to demonstrate a level of understanding for skills and knowledge developed, derived or researched outside the class or examination room. Whilst not ideal, the following skills can only be demonstrated by showing attendance of a course which meets these requirements. For adherence to this standard, qualifying courses will have:

- ❖ A syllabus that meets the content requirements.
- ❖ An independent examination that tests the student has understood the content of the syllabus and that they are able to demonstrate and use the knowledge gained.
- ❖ An expiry date on the certification/examination, so that without continued evidence of use (for example by Continued Professional Development (CPD)) the skills are 'retired' and no longer valid to be claimed by the holder.
- ❖ The required skills should be evidenced:
 - By certification.
 - By CPD following previous formal qualification.

- The skills should be current. This should be evidenced by:
 - In-date certifications.
 - Training on Operating systems no more than two versions behind the one currently deployed within the organization.
 - CPD credits for further and ongoing personal development.

Mandatory Skills

Collectively the staff should have all the following 5 skills groups:

1. Network Configuration

- ❖ The training should have covered the following:
 - How to install devices on the LAN.
 - How to optimise the traffic flows.
 - How to control access to devices across the LAN.
 - How to backup and store configuration files.
 - How to securely manage devices remotely.
 - The need and how to patch/update devices.

2. Platform Configuration

- ❖ The training should have covered the following:
 - How to install the operating system from a good source.
 - How to optimise the operating system for performance.
 - How to control access to the platform across the LAN.
 - How to backup and store configuration files (securely).
 - How to audit the running configuration of the device.
 - How to securely manage the device remotely.
 - How to add users, including what type of users to add.
 - How to limit user access.
 - How to control the times of user access.
 - How to expire an account.
 - How to set an expiry in the future for an account.
 - The need and how to patch the operating system

3. Introductory Network Security

- ❖ The Introduction to Network Security training should have covered the following:
 - The protocol stack and limitations of IPv4.
 - The Confidentiality, Integrity and Availability (CIA) security concept.
 - What a vulnerability is.
 - What an exploit is and how they can affect the organization's network.
 - The importance of patching.
 - How to control access to data/information across the LAN.
 - How to backup and store data securely.
 - How to audit the security of a network (basic level).

- The use of applications such as nMap and Nessus for identification of common configuration and security issues.
- How to report these identified issues.
- The legal aspects of scanning networks.
- How to plan a network for defence in depth. This should provide the understanding of how to:
 - Control access to public services.
 - Reduce the attack surface.
 - Harden servers.
 - Secure the internal network.
- The training material should introduce other technologies to the student including (at least 4 of the following):
 - Intrusion Detection Systems (IDS).
 - Intrusion Prevention Systems (IPS).
 - Host Based IDS.
 - Firewalls.
 - Threat Management tools.
 - Wireless Attack Detection Systems.
 - Rogue Access Point Detection Systems.
 - Network Access Control.
 - Anti Virus (Enterprise Management).
 - Secure Web Proxy Devices.
 - Secure Mail Proxy Devices.
 - Multi Factor Identification.
 - Multi Factor Authentication.
 - Encryption.

Courses known to have met the criteria

SANS 401 - SANS Security Essentials Bootcamp Style Course

4. Platform Specific Training (ie Vendor specific)

A team member should undertake an element of platform specific training, that includes how to correctly install, optimize, manage and securely configure the device. The following three headings give an idea of the sort of course content is recommended:

4.a Router/Switch/NAS/SAN/WAN Configuration

- The training should have covered the following:
 - How to install the device.
 - How to optimise the device.
 - How to control access to the device across the network.
 - How to backup and store configuration files.
 - How to audit the running configuration of the device.
 - How to securely manage the device remotely.

4.b Firewall configuration

- The training should have covered the following:
 - How to install the device.

- How to add the minimum rules necessary.
- How to control access to the device across the LAN.
- How to backup and store configuration files.
- How to audit the running configuration of the device.
- How to securely manage the device remotely.

4.c Wireless device configuration

- The training should have covered the following:
 - How to install the device.
 - How to optimise the power of the device for the environment.
 - How to control access to the device across the LAN.
 - How to backup and store configuration files.
 - How to implement Security on the device.
 - How to implement WPA and WPA2.
 - Infrastructure or Enterprise (RADIUS) with AES is preferred over Personal WPA (TKIP).
 - *WEP is not acceptable under CDS.*
 - How to audit the running configuration of the device.
 - How to securely manage the device remotely.

5. Vulnerability Analysis

- ❖ The training should have covered:
 - Legal Aspects.
 - Planning and Scoping the Testing.
 - Engaging with the customer/client.
 - The stages of the testing.
 - The equipment to be used and the process of testing the equipment before the test itself.
 - Actions upon finding an ongoing incident.
 - Actions upon finding illegal content (other than child pornography).
 - Actions upon finding child pornography (both for the organization and the tester).
 - How to report the findings.
 - What to do to validate the report/findings.

Courses known to have met the criteria

SANS 504 - Hacker Techniques, Exploits & Incident Handling Course.

Optional Skills

The following two courses are optional at this point; however, their addition would strengthen the team, and prepare the organization for the higher levels, where penetration testing is required.

Optional 1: Penetration Testing

- ❖ The training should have covered:
 - Legal Aspects.
 - Planning and Scoping the Testing.

- Engaging with the customer/client.
- The stages of the Testing.
- The equipment to be used and the process of testing the equipment before the test itself.
- Actions upon finding an ongoing incident.
- Actions upon finding illegal content.
- Actions upon finding child pornography (both for the organization and the tester).
- How to report the findings.
- What to do to validate the report/findings.

Courses known to have met the criteria

SANS 560 - Network Penetration Testing and Ethical Hacking Course.

Optional 2: Wireless Security *Note this is Mandatory if wireless is deployed in the organization and replaces the Wireless Device Configuration at 4.c above.*

❖ The training should have covered:

- RF theory
- The Threat
- Wave propagation and signal strength.
- How to sniff wireless networks.
- Auditing WLANs.
- Rogue Access Points.
- The security of WEP, WPA, LEAP, WIMAX.
- Bluetooth vulnerabilities.
- Wireless segmentation on the main LAN.

Courses known to have met the criteria

SANS 617 - Wireless Ethical Hacking, Penetration Testing, and Defenses Course.

SANS 559 - Wireless Security Exposed Course.

CWSP - Certified Wireless Security Professional.

Benefits of Implementation:

IT security staff will possess a range of skills which will allow them to assist network administrators to configure the organization's network, increasing the security resilience and defensive capacity of the network.

Recurring? If so frequency:

Training requirements should be reviewed annually and care taken to ensure that where qualifications have a lapse date that re-validation of those qualifications takes place.

Checks on Regular Subcontractors

Requirement Number: REQ 6.3

Overview:

Sub-contractors who have regular access to, or who are embedded within, an organization should be subjected to checks to ensure their security accords with those of the parent organization.

Responsible Group or Users:

Senior Management should ensure that checks form part of the contract tendering or outsourcing process.

Staff responsible for contracts or outsourcing should ensure that checks of a sub-contractor's security posture are undertaken as part of the contracting or outsourcing process.

Requirement Description:

Extant and new subcontractors should be reviewed; the review should include the following (as a minimum):

- ❖ The requirement to safeguard information passed to them.
- ❖ The requirement to report the loss or compromise of their data or network.
- ❖ The requirement to take appropriate steps to protect data and information passed to them.

Subcontractors should be encouraged to adopt CDS to allow for easy review of the level of digital security that they have achieved, and allow organizations to discuss the security of their networks using common language.

Benefits of Implementation:

Organizations gain a better understanding of their sub-contractors security culture and how their data is actually protected. Both the principal and the contractor understand the strength of each other's security and are able to communicate in like terms.

Recurring? If so frequency:

Reviews should be undertaken annually or as soon as possible for organizations new to CDS. Organizations whose sub-contractors are fully integrated into CDS need only check the currency of their contractor's CDS status.

VPNs and Encryption on Regular Links

Requirement Number: REQ 6.4

Overview:

Where long standing organization-to-organization relationships exist, encryption should be implemented on communication links between the two parties.

Responsible Group or Users:

System administrators should advise senior management on the implementation of communication encryption.

Senior management must take ownership of the implementation of encryption on the organization's IT infrastructure.

Requirement Description:

Emails should be digitally signed by staff.

Mobile devices must use Virtual Private Network (VPN) links and not communicate in clear (regardless of the ISP/Telcom provider claims about private clouds).

Core business Point to Point connections should be via VPN or be Secure Socket Layer (SSL) encrypted.

VPN and SSL linking can be implemented at the router level or by firewall to firewall links.

Public Certificate Authorities (CAs) do not need to be used, internal CAs can be adopted.

Benefits of Implementation:

Data transiting across publicly accessible infrastructures or networks outside the organization's control is protected against unauthorized interception. Recipients of communications gain assurance as to their provenance.

Recurring? If so frequency:

Implementation of the technology is a one-off event, but encryption keys and certificates should be subjected to change at least annually.

Application Layer Firewalls

Requirement Number: REQ 6.5

Overview:

All connections from outside the organization must be controlled by a correctly configured Application Layer Firewall.

Responsible Group or Users:

System administrators should advise senior management on the implementation of application layer firewalls.

Senior management must take ownership of the implementation of firewalls on the organization's IT infrastructure.

Requirement Description:

- ❖ The firewall must operate at Open Systems Interconnection (OSI) Layer 3 and should be able to:
 - Track both internal outbound requests and inbound external requests.
 - Allow the returning responses to requests based upon information in its internal state table.
 - Deny a connection to a timed out or dynamically closed connection.
 - Block access from IP addresses to dynamically opened ports that are not available to that address (ie the state table entry does not match).
 - Reject packets based upon its built-in Stateful Packet filtering.
 - Silently reject or drop packets from sources not approved for connection to or through the firewall.
- ❖ The firewall must also operate at OSI Layer 7 and to the following criteria:
 - The firewall must be configured to inspect the protocols passing through it and not set in a dumb proxy mode.
 - The firewall must be configured to block protocols that are not required by the organization.
- ❖ To achieve this the organization will need to know:
 - What it needs to pass through the firewall.
 - What is approved to pass through the firewall.
 - What the approved configuration is.
- ❖ The firewall must inspect the DMZ traffic where possible and, if the technology permits,

break any SSL link to DMZ services and inspect that traffic.

- ❖ Be configured to only allow the minimum of services through.
 - This must include both inbound and outbound port filtering.
 - The firewall must control outbound communication and not allow (by default) all outbound connections.
 - Must minimise the inbound connections.
 - Firewall rules must be specific and to defined IP addresses.
 - Firewall rules must strictly limit connections into and out of DMZ servers and only to required ports.
- ❖ Must provide a DMZ function for public facing servers (by itself or in conjunction with another Stateful Firewall).
- ❖ Must be independently tested by a skilled person who confirms it is operating correctly and securely.
- ❖ The firewall must be managed from a dedicated system that is defined in the firewall rules to prevent others modifying the firewall.
- ❖ The firewall should be configured to alert the Administrator when (firewall hardware/software permitting):
 - Rules have been changed on the firewall.
 - Patches have been applied to the firewall.
 - The firewall has rebooted.
 - New updates are available for the firewall.
- ❖ Must be included in the organization's patching policy and strategy.
- ❖ See the list of approved firewalls on the CDS website.
- ❖ Large organizations (more than 100 clients on the system) should give strong consideration to implementing:
 - A standalone Web Proxy in the DMZ. This is to reduce the impact of a web based attack exploiting the clients or the internal proxy server.
 - A standalone email proxy in the DMZ. This is to reduce the impact of an email virus or other email based attacks.

Benefits of Implementation:

Implementation of improved firewall technology will improve the performance of the network by reducing the number of spurious or unnecessary connections. Network protection will be improved through more granular control of ports and services.



Recurring? If so frequency:

Firewall logs should be reviewed daily, but weekly is fine on small networks.

Configurations should be reviewed periodically to ensure they have not been changed.



Consider Further Enhanced Technologies

Requirement Number: REQ 6.6

Overview:

The organization should consider implementing additional technologies that will further enhance their overall network security profile.

Responsible Group or Users:

System administrators should advise senior management on the implementation of additional technologies within the network.

Senior management must encourage the implementation of additional technologies, producing policy as necessary.

Requirement Description:

Organizations should consider the use of the following technologies:

- ❖ Two factor authentication for remote access by clients (where VPNs are implemented). These can include Certificates, Biometrics, Tokens, and Time Sync Tokens.
- ❖ File modification alarming technology (hashing and tripwire).
- ❖ File usage control technology (white listing).
- ❖ Intrusion Detection or Prevention Systems (IDS/IPS).
 - Small organizations can implement this on client desktops (HIDS).
 - Medium sized organizations should implement on both clients (HIDS) and on the core internal LAN (NIDS).
 - Large and Very Large organizations should implement IDS on the boundary (Threat Facing), on the core LAN (NIDS) and clients (HIDS).

Benefits of Implementation:

Additional technologies will reduce the risk of successful network attack and increase the network's resilience to the effects of an attack..

Recurring? If so frequency:

An annual review should be carried out of the feasibility of employing additional technologies over and above those required of this CDS Level.

Regular Vulnerability Analysis

Requirement Number: REQ 6.7

Overview:

The system should be subjected to a Vulnerability Analysis (or Vulnerability Test).

(Note: This is not a Penetration Test.)

Responsible Group or Users:

Senior management should endorse and fund the need for a vulnerability analysis.
System Administrators should support and assist the conduct of the testing.

Requirement Description:

Where possible the vulnerability analysis should be undertaken at 12 monthly intervals.

Can be conducted with in-house resources.

All reporting and certification requirements are still required for in-house sourced resources.

Where in-house resources are provided these must routinely operate outside the organization's vertical reporting chain for the area being tested.

Significant changes to the security barriers should trigger a re-run of the VA.

Whether the VA is conducted using in-house resources or by an external specialist it must be carried out by a qualified person in the following manner:

- ❖ The VA Tester must have approved methodologies.
- ❖ The methodologies must account for the appropriate threat vectors.
- ❖ The methodology must be defined and agreed by the organization.
- ❖ The methodology must be documented and repeatable.
- ❖ The methodology should also be approved by the organization.
- ❖ The VA Tester must have policies, barriers and procedures to protect the network and data they are testing against compromise, corruption or system crashes.
- ❖ The Tester must have the correct skills and qualifications.
- ❖ The Tester must hold an in-date qualification (eg CEH, GPEN, CREST, Tiger) relevant to the conduct of the test.
- ❖ The Tester, if external, must have appropriate insurance during the testing.

- ❖ The Tester, if external, should provide a CV and statement of compliance at the audit point.

The VA must be correct and complete:

- ❖ The VA must be conducted to a Test Plan.
- ❖ The Test Plan must be available for inspection.
- ❖ The VA Report must refer to the Test Plan.
- ❖ The VA report must identify who conducted what part of the test and their qualifications/experience.
- ❖ The VA Report must demonstrate that the test plan's activities were conducted correctly.
- ❖ The Test Report must clearly identify how false positives were checked and removed.
- ❖ The VA Report must identify the issues, concerns, vulnerabilities and weaknesses in the system.
- ❖ Any instances of Trojans, root kits and ongoing hacking must be reported immediately if discovered.
- ❖ The VA Tester should have an incident response plan agreed with the tested organization.
- ❖ The plan should be available for CDS audit.

Both the target organization and the VA Tester should have a set of incident plans to ensure a rapid and measured response during the time of increased exposure.

REPORTING REQUIREMENTS

The Test Report must clearly identify how the issues found can be fixed in the immediate and medium term. report must clearly articulate the core observations to the various readers. To achieve this the report should comprise:

- ❖ **An Executive Summary**
 - No more than two facing pages for busy executive readers.
 - No technical terms unless absolutely necessary.
 - No abbreviations unless they are commonly used by most staff within the tested organization.
- ❖ **An overview of the auditing activity**
 - Detailing the dates of the audit.
 - The auditors involved.
 - The auditor's Qualifications.
 - The auditor's locations and sites visited during the audit.
- ❖ **A main body of report**
 - The detailed Auditing Results should be presented in the main body of the report and should:
 - Be broken into appropriate groups of items found.
 - Detail the source and indication of the issue.

- Explain or outline the issue in clear terms.
- Explain why this is a problem for the organization.
- Explain how to fix the problem.
- It is suggested that colour codes are used to draw the attention of the reader to the important, high impact or high risk items:
 - Red – A critical issue exists.
 - Amber – A significant issue exists.
 - Yellow – Something that could be done better.
 - Green – Good practice, a laudatory note.

❖ **Annex for additional information**

- Attach the volume of auditing output in an Annex to the main document and only distribute it to those for whom it will add value and who will use the information for the organization's benefit. This should be the raw output of auditing activity where local licensing allows.
- List all software, tools or bespoke activities/processes undertaken or used on the test. Do not include a default long list of tools, many of which are not relevant, current or applicable for the audit of the organization.
- The Annex data can be on CD or DVD.
- Hardcopy is permissible but is discouraged as it is wasteful, bulky and not easy to search for specific information.
- Any instances of Trojans, root kits and ongoing hacking must be reported immediately if discovered; details should be included in the Annex information.
- The auditing organization should have an incident response plan agreed with the audited organization.
- The plan should be available for CDS Review.
- The organization should have its own incident plan.

❖ **Secure delivery of the Report**

- The report must have been delivered in a secure manner, ie not emailed in clear to the organization. This can be achieved by:
 - Courier with encrypted removable media.
 - Encrypted email if the password is sent out of band (ie not emailed).
 - Delivered hard copy or encrypted media in person.

Follow up

The findings of the report must be addressed within 6 months of the test, with corrective action prioritized according to the severity of the issues. Thus any red and amber issues should be dealt with ahead of yellows and greens.

Organizations that have completed their first vulnerability analysis within 3 months of the date of CDS audit must produce an action plan detailing their intended corrective actions and the expected completion date.

Organizations presenting themselves for re-audit must show that the corrective actions



required from their first report have been completed.

Benefits of Implementation:

The organization will gain clearer insight as to where their areas of weakness or non-compliance exist. This knowledge will allow the development of focused plans and strategies to correct problems, develop or correct supporting policies, and allow the organization to assess their levels of risk more accurately.

Recurring? If so frequency:

Where possible, VA testing should be re-run every 12 months. Instances where this is not possible should be presented to the CDS Certification Body for consideration of a waiver notice.

Note: Waiver notices, where issued, will not be repeated for consecutive audits.





PART 3

CDS AUDIT REQUIREMENTS





ABOUT THIS PART

Part 3 outlines what the organization must demonstrate to pass the independent audit of their implementation of a chosen target Certified Digital Security (CDS) level.

IF SEEKING AN AUDIT

If the organization is seeking an independent audit of their CDS implementation, the reader is strongly encouraged to use Part 3 as the guide to the production of the necessary audit evidence. Part 3 is only used for CDS audits and is designed to communicate the type, quality, timeliness of data and structure of the evidence documents that are required to be presented for audit.

RECOMMENDED PROCESS

If the organization are seeking a CDS audit of their security, we recommend the following process:

- Step 1. Read the standard for your Target Level.
- Step 2. Go to the CDS Web Site and read the audit process as outlined in the 'Audit Requirements' pages (or Part 3 of the guidance document associated with your chosen CDS target level).
- Step 3. Examine your organization's security to assess how it currently measures against the standard.
- Step 4. Identify the gaps to calculate the amount of work required to meet your target level.
- Step 5. Put in place work packages to fill the gaps, while completing the application for CDS membership and audit.
- Step 6. Once you believe you have met the requirements for your target level of the standard, contact a CDS Auditor via the CDS Web Site and arrange an audit.
- Step 7. Integrate the security and ongoing reviews into normal business practice.
- Step 8. Generate the evidence necessary for your target level (and all levels below the target level), in the required format (see Part 3 of this document).





- Step 9. Prepare the organization for the day of the audit – ensure the room meets the standard required and that all evidence is correctly formatted, labeled and appropriate for the level targeted.
- Step 10. Support the auditor during the audit and ensure all of their questions are answered before they leave at the end of the audit.

THE AUDIT PROCESS

ABOUT THE PROCESS

CDS Audits are designed check all the evidence¹ necessary to prove the requirements² have been met. They are designed to use check sheets wherever possible to remove ambiguity, hearsay or mis-interpretation and other subjective inputs that cloud otherwise clear cut objective assessments.

TIME IS MONEY...

CDS audits are based purely upon the evidence presented to the auditor at the time of audit. CDS audits are not protracted events thus room, lighting and desk layouts are defined by CDS to ensure the maximum amount of time is spent conducting the audit.

CDS audits have been designed to be very cost effective. By following the information listed in Part 3 of the guidance document, an organization can guarantee that only the information required for **that** audit is actually presented to the auditor. This will ensure the audit is conducted within the planned and quoted timeframe.

NO HANDS ON!

CDS audits do not require the auditor to connect any system to your network and as such the auditor should not be offered any connection or system for review purposes. Any such offering is not supported or condoned by CDS or Digital Security Ltd. The Audit process was specifically designed to prevent the auditor from attacking or affecting the system being reviewed.

LOWER LEVELS ARE INCLUDED TOO

Remember CDS levels are cumulative – to pass level 5 you must present the necessary evidence for levels 1 through 4 unless one of the following is true;

¹ Identified in the Part 3 of the guidance document for the Target CDS Level

² Identified in the Part 2 of the guidance document for the Target CDS Level





The organization has either a waiver from CDS detailing which items or evidence or levels are not required to be audited.

or

The organization presents an audit pass certificate from the last 4 months for the lower level

Note: both of these exclusions must be confirmed at the time of scheduling the audit, and not on the day of the audit.

ON THE DAY OF AUDIT

The auditor will arrive and review the documents that have been presented for audit³. If all items of evidence are correct and appropriate, the auditor will complete their audit forms and issue their recommendation and a copy of their report to the organization in the form of a quick on-site quick debrief.

The auditor will forward their report to the Certification Board (Digital Security).

The certification board will review the auditor's report and if satisfactory will endorse the reports recommendation. The certification board will inform the organization of the result within 4 working days (usually 1-2 days) of the receipt of the report.

The organization will be asked to retain the auditor's report in a secure location as the Certification Board will destroy their copy within 10 working days (for security reasons).

The organization will be asked to confirm the level of publicity they would like and this will be adhered to by CDS and the Certification Board; options include:

1. Listing on the CDS website with achieved level - either a level number or the level grouping eg Standard, Enhanced or Advanced.
2. Their organization identified on the CDS website with 'Independently Verified CDS Adopter'.
3. No listing on the CDS website.

Regardless, all organizations that pass a CDS level will be issued a unique reference that can be given to clients or external 3rd parties. This can be quoted to CDS staff to receive a verification and validation of the organization's achievement.

³ In the format required of the target CDS level and displayed in layout or desk plan as defined by that target level





IF THE EVIDENCE IS NOT CORRECT OR IS INCOMPLETE

In the event that your audit findings result in a fail, a non-compliance report will be provided to you for rectification prior to a re-audit.

Where your audit findings result in a pass, upon ratification of the results your organization will be granted the right to claim the CDS Target Level and display the appropriate logo on corporate communications.

HOW REQUIREMENTS ARE MET

Each CDS level has a number of requirements that must be evidenced as being met during a CDS Audit; these are numbered so they can be easily cross and externally referenced.

The requirement numbering includes the target level so that readers can see what requirements build upon previous levels foundations. Requirements are prefixed with 'REQ' (for requirement)

For example: The fourth requirement on level 6 is indexed as REQ 6.4.

Audit evidence aspects are defined as being 'Statements of Evidence' or SOE's for short. These are similarly indexed:

For example: The evidence for level 6 requirement number four (ie REQ 6.4 from above) is noted under Part 3, SOE 6.4.

Thus, the reader can easily cross-refer to both requirement and evidentiary quality statements as REQ 6.4 is supported by SOE 6.4.

WHAT'S IN A STATEMENT OF EVIDENCE (SOE)?

Just as each requirement is comprised of several components, SOEs are also made up of different fields and labels:

1. The Statement of Evidence (SOE) title.
2. The related requirement title (or short name) - if different from SOE title.
3. Its unique requirement number.
4. A short overview of what the requirement is designed to achieve or introduce.
5. The details of the evidence required (the numbers, percentages or other details relating to the quality and type of evidence needed). This can be further broken down and may link to the CDS website for current information.



6. The list detailing how the evidence can be generated.
7. The details of the pass/fail Criterion – if known.
8. Any notes relevant to the SOE.

Dedicated Security Staff

Statement of Evidence (SOE) Number: SOE 6.1

Overview:

The organization must provide evidence that it has staff whose primary role is IT security, providing security support and promoting awareness of the organization's goals, processes and ethos.

Statement of Evidence (SOE) Description:

SOE 6.1.a

The organization must present details of their IT security staff. If the function is outsourced, the organization must provide details of the company in addition to the names of the individuals.

SOE 6.1.b

The organization must provide terms of reference for the IT security staff detailing their responsibilities. Responsibilities must include:

- ❖ Providing advice to the organization
- ❖ Auditing IT security within the organization
- ❖ Promoting the organization's security ethos and practices
- ❖ Involvement in discussions on current and future IT risks and network development (manager only).

SOE 6.1.c

Where the IT security function is outsourced, the organization must show that at least the lead individual from the company has undergone the organization's induction training.

SOE 6.1.d

The organization must show that IT security staff have undergone initial or refresher training in accordance with **SOE 6.2**

How this can be generated:

The details of IT security staff and their terms of reference can be produced as printed output in the form of a nominal roll or other type of document, such as a contract for any outsourced provision. Training records should be produced to demonstrate attendance on induction courses.

Details of the pass or fail criteria for SOE 6.1:

SOE 6.1 Will be deemed to have been failed if any of the fail criteria are met or are outstanding at the end of the audit period:

Fail Criterion 1:

The organization does not have dedicated IT security staff as defined by **SOE 6.1.a**.

Fail Criterion 2:

The organization fails to produce details of the IT security staff as defined by **SOE 6.1.a**.

Fail Criterion 3:

Any outsourced IT security support is not provided by named individuals; i.e. support is ad hoc.

Fail Criterion 4:

The organization fails to show that IT security staff pool does not undergo initial or refresher training in accordance with **SOE 6.2**

Mandated IT Security Staff Training

Statement of Evidence (SOE) Number: SOE 6.2

Overview:

The organization must provide evidence that IT Security staff undergo formal training to equip them with the necessary skills for their role and provide evidence of their abilities to use those skills.

Statement of Evidence (SOE) Description:

To meet the evidence requirements the organization must:

SOE 6.2.a.

The organization must present a statement of their training regime, either in-house or outsourced, for their IT security staff. The statement must include provisions for the mandatory and optional training requirements of this standard.

SOE 6.2.b

The organization's statement must show that the optional elements (Wireless Security and Penetration Testing (See **REQ 6.2**)) of the CDS training requirements form part of their IT security staff development plans.

SOE 6.2.c

The organization must present details of the staff responsible for IT security by name. If the function is outsourced, the organization must provide details of the company in addition to the names of the individuals.

SOE 6.2.d

The organization must produce details of the training undertaken by their IT security staff, including names, training dates, venues and training providers.

SOE 6.2.e

The organization must provide evidence that the following skills are available among their IT security staff:

1. Network Configuration

The training should have covered the following:

- ❖ How to install devices on the LAN.
- ❖ How to optimise the traffic flows.
- ❖ How to control access to devices across the LAN.

- ❖ How to backup and store configuration files.
- ❖ How to securely manage devices remotely.
- ❖ The need and how to patch/update devices.

2. Platform Configuration

The training should have covered the following:

- ❖ How to install the operating system from a good source.
- ❖ How to optimise the operating system for performance.
- ❖ How to control access to the platform across the LAN.
- ❖ How to backup and store configuration files (securely).
- ❖ How to audit the running configuration of the device.
- ❖ How to securely manage the device remotely.
- ❖ How to add users, including what type of users to add.
- ❖ How to limit user access.
- ❖ How to control the times of user access.
- ❖ How to expire an account.
- ❖ How to set an expiry in the future for an account.
- ❖ The need and how to patch the operating system

3. Introductory Network Security

The Introduction to Network Security training should have covered the following:

- ❖ The protocol stack and limitations of IPv4.
- ❖ The Confidentiality, Integrity and Availability (CIA) security concept.
- ❖ What a vulnerability is.
- ❖ What an exploit is and how they can affect the organization's network.
- ❖ The importance of patching.
- ❖ How to control access to data/information across the LAN.
- ❖ How to backup and store data securely.
- ❖ How to audit the security of a network (basic level).
- ❖ The use of applications such as nMap and Nessus for identification of common configuration and security issues.
- ❖ How to report these identified issues.
- ❖ The legal aspects of scanning networks.
- ❖ How to plan a network for defence in depth. This should provide the understanding of how to:
 - Control access to public services.
 - Reduce the attack surface.
 - Harden servers.
 - Secure the internal network.
- ❖ The training material should introduce other technologies to the student including (at least 4 of the following):
 - Intrusion Detection Systems (IDS).
 - Intrusion Prevention Systems (IPS).

- Host Based IDS.
- Firewalls.
- Threat Management tools.
- Wireless Attack Detection Systems.
- Rogue Access Point Detection Systems.
- Network Access Control.
- Anti Virus (Enterprise Management).
- Secure Web Proxy Devices.
- Secure Mail Proxy Devices.
- Multi Factor Identification.
- Multi Factor Authentication.
- Encryption.

4. Platform Specific Training

4.a Router Configuration

The training should have covered the following:

- ❖ How to install the device.
- ❖ How to optimise the device.
- ❖ How to control access to the device across the LAN.
- ❖ How to backup and store configuration files.
- ❖ How to audit the running configuration of the device.
- ❖ How to securely manage the device remotely.

4.b Firewall configuration

The training should have covered the following:

- ❖ How to install the device.
- ❖ How to add the minimum rules necessary.
- ❖ How to control access to the device across the LAN.
- ❖ How to backup and store configuration files.
- ❖ How to audit the running configuration of the device.
- ❖ How to securely manage the device remotely.

4.c Wireless device configuration

The training should have covered the following:

- ❖ How to install the device.
- ❖ How to optimise the power of the device for the environment.
- ❖ How to control access to the device across the LAN.
- ❖ How to backup and store configuration files.
- ❖ How to implement Security on the device.
- ❖ How to implement WPA and WPA2.
 - Infrastructure or Enterprise (RADIUS) with AES is preferred over Personal WPA (TKIP).
 - *WEP is not acceptable under CDS.*
- ❖ How to audit the running configuration of the device.
- ❖ How to securely manage the device remotely.

5. Vulnerability Analysis

The training should have covered:

- ❖ Legal Aspects.
- ❖ Planning and Scoping the Testing.
- ❖ Engaging with the customer/client.
- ❖ The stages of the testing.
- ❖ The equipment to be used and the process of testing the equipment before the test itself.
- ❖ Actions upon finding an ongoing incident.
- ❖ Actions upon finding illegal content (other than child pornography).
- ❖ Actions upon finding child pornography (both for the organization and the tester).
- ❖ How to report the findings.
- ❖ What to do to validate the report/findings.

Optional Skills

Optional 1: Penetration Testing

The training should have covered:

- ❖ Legal Aspects.
- ❖ Planning and Scoping the Testing.
- ❖ Engaging with the customer/client.
- ❖ The stages of the Testing.
- ❖ The equipment to be used and the process of testing the equipment before the test itself.
- ❖ Actions upon finding an ongoing incident.
- ❖ Actions upon finding illegal content.
- ❖ Actions upon finding child pornography (both for the organization and the tester).
- ❖ How to report the findings.
- ❖ What to do to validate the report/findings.

Optional 2: Wireless Security (This is Mandatory if wireless is deployed in the organization)

The training should have covered:

- ❖ RF theory
- ❖ The Threat from wireless attackers
- ❖ Wave propagation and signal strength.
- ❖ How to sniff wireless networks.
- ❖ Auditing WLANs.
- ❖ Rogue Access Points.
- ❖ The security of WEP, WPA, LEAP, WIMAX.
- ❖ Bluetooth vulnerabilities.
- ❖ Wireless segmentation on the main LAN.

SOE 6.1.f

The organization must produce the certificates and qualifications held by their administrators which support the requirements of **SOE 6.2.e**

SOE 6.1.g

Certificates and qualifications presented under **SOE 6.2.f** must be in-date.

SOE 6.2.h

The organization must produce copies of the syllabi of all training courses undertaken to support the requirements of **SOE 6.2.e** and **SOE 6.2.f**.

SOE 6.2.i

The mandatory training requirements must be met by the contents of the syllabi presented. Evidence of any mandatory element can be met by the content of separate courses attended by the same individual (e.g. a particular Network Security course does not cover Host Based IDS or Secure Web Proxy Devices, however another course (which does not include the limitations of IPv4) does. Providing an individual attends and passes both courses the organization can claim all elements of that CDS training requirement).

How this can be generated:

The training statement can be produced as a written document or extract from a parent document within the organization.

Certificates and Qualifications can be produced as originals or certified photocopies.

To be valid, course syllabi presented under **SOE 6.2.h** must be those produced by the training provider of the course in question.

Details of the pass or fail criteria for SOE 6.2

SOE 6.2 Will be deemed to have been failed if any of the fail criteria are met or are outstanding at the end of the audit period:

Fail Criterion 1:

The organization fails to produce a training policy statement for IT security staff.

Fail Criterion 2:

The training policy statement does not include provision of optional, as well as mandatory training.

Fail Criterion 3:

The organization does not produce a list of IT security staff names.

Fail Criterion 4:

The organization does not produce records of training undertaken by IT security staff.

Fail Criterion 5:



The training provided to IT security staff does not include the mandatory courses detailed in **SOE 6.2.e**.

Fail Criterion 6:

The organization fails to produce the certificates and qualifications held by their IT security staff which support the requirements of **SOE 6.2.e** and **SOE 6.2.f**

Fail Criterion 7:

Certificates and qualifications presented under **SOE 6.2.f** are out-of-date or invalid.

Fail Criterion 8:

The organization fails to produce copies of the syllabi of all training courses undertaken to support the requirements of **SOE 6.2.e** and **SOE 6.2.f**.

Fail Criterion 9:

The syllabus evidence in **SOE 6.2.h** fails to cover 2 or more elements of any one of the mandatory training courses detailed in **SOE 6.2.e**.



Checks on Regular Subcontractors

Statement of Evidence (SOE) Number: SOE 6.3

Overview:

The organization must show that sub-contractors who have regular access to, or who are embedded within, the organization are subjected to checks to ensure their security accords with those of the parent organization.

Statement of Evidence (SOE) Description:

SOE 6.3.a.

The organization must provide a list of all sub-contractors annotated with their status within the organization (i.e. have frequent access or embedded function).

SOE 6.3.b.

The organization must demonstrate that reviews of sub-contractors are carried out.

SOE 6.3.c.

The organisation must produce a written account of the review which includes their assessment of their sub-contractors' capability to:

- ❖ Safeguard information passed to them.
- ❖ Report the loss or compromise of their data or network.
- ❖ Take appropriate steps to protect data and information passed to them.

This requirement can also be met by identifying that the sub-contractor holds a current CDS certificate for organization's preferred CDS Level.

How this can be generated:

Lists and review proceedings can be produced as printed hard copy; sub-contractors who hold CDS status should be identified by their CDS membership number.

Details of the pass or fail criteria for SOE 6.3

SOE 6.3 Will be deemed to have been failed if any of the fail criteria are met or are outstanding at the end of the audit period:

Fail Criterion 1:



The organization fails to present a hard copy list of its sub-contractors.

Fail Criterion 2:

The organization fails to include the status of its sub-contractors in the list

Fail Criterion 3:

The organization fails to produce a written account of their reviews of sub-contractors

Fail Criterion 4:

The review account does not contain assessments of the elements required by **SOE 6.3.c**.



VPNs and Encryption on regular links

Statement of Evidence (SOE) Number: SOE 6.4

Overview:

This will confirm that the organization has implemented VPNs and other encryption on links it uses regularly to communicate with internal and external business entities.

Statement of Evidence (SOE) Description:

SOE 6.4.a.

The organization must present a list of the links it uses to communicate both inside and outside the organization. These links must include, but are not limited to, remote access connections for home workers or 'road warriors' and point to point communications to business partners, clients or service providers (for example frequent sending or posting of reports to a client).

SOE 6.4.b.

For each link the organization must provide a statement, signed by the IT manager, detailing:

- ❖ How VPN or encryption is implemented.
- ❖ What encryption is used.

SOE 6.4.c.

The statement must also assert that emails are required to be digitally signed within the organization by the user before it is sent.

SOE 6.4.d.

The organization must provide a copy of their mobile device configuration document.

SOE 6.4.e.

The configuration document must show that mobile devices can only communicate with the organization's network via VPN.

How this evidence may be generated:

The list of business links can be provided from either network architecture or information management documents. The key requirement is for the document to show all business links where information enters or leave the organization.

The statement of conformity for **SOE 6.4.b** and **SOE 6.4.c** can be a list of the criteria signed by the IT Manager.

Details of the pass or fail criteria for SOE 6.4

SOE 6.4. Will be deemed to have been failed if any of the following criteria are met:

Fail Criterion 1:

The organization fails to present the list of links it uses to communicate both inside and outside the organization.

Fail Criterion 2:

The organization fails to provide a statement for how links are implemented for each link listed in support of **SOE 6.4.a**.

Fail Criterion 3:

The link implementation statements are not signed by the IT Manager.

Fail Criterion 4:

The link implementation statements do not assert that users must digitally sign their emails.

Fail Criterion 5:

The organization does not provide a copy of their mobile device configuration document.

Fail Criterion 6:

The mobile device configuration document does not show that mobile devices can only communicate with the organization's network via VPN.

Application Layer Firewalls

Statement Of Evidence (SOE) Number: SOE 6.5

Overview:

This is to confirm that the organization has implemented application layer firewalls on the boundaries of their network.

Statement of Evidence (SOE) Description:

SOE 6.5.a.

The organization must present a list of all firewall devices connected to their network together with a list of network servers in accordance with **SOE 2.3.c** showing all public facing servers.

SOE 6.5.b.

The organization must present printed output of the ruleset for each firewall device, showing:

- ❖ Source IP addresses
- ❖ Destination IP addresses
- ❖ Port numbers and Protocols
- ❖ Allows and Deny rules

SOE 6.5.c.

The organization must provide details of the firewall manufacturer's datasheet regarding the functional capabilities of the device.

SOE 6.5.d.

The firewall manufacturer's datasheet must show that the device carries out the following functions:

- ❖ Operates at Open Systems Interconnection (OSI) Layer 3.
- ❖ Able to track both internal outbound requests and inbound external requests.
- ❖ Allows the returning responses to requests based upon information in its internal state table.
- ❖ Denies a connection to a timed out or dynamically closed connection.
- ❖ Blocks access from IP addresses to dynamically opened ports that are not available to that address (ie the state table entry does not match).
- ❖ Rejects packets based upon its built-in Stateful Packet filtering.

- ❖ Silently rejects or drops packets from sources not approved for connection to or through the firewall.
- ❖ The firewall must also operate at OSI Layer 7.

SOE 6.5.e.

The organization must produce a firewall configuration document which contains details of:

- ❖ What protocols are required to pass through the firewall.
- ❖ What data types are approved to pass through the firewall.
- ❖ The approved firewall configuration.

SOE 6.5.f.

The firewall configuration document must show that:

- ❖ The firewall is configured to inspect the protocols passing through it and not set in a dumb proxy mode.
- ❖ The firewall is configured to block protocols that are not required by the organization.
- ❖ Where possible the firewall inspects the DMZ traffic and, if the technology permits, break any SSL link to DMZ services and inspect that traffic.
- ❖ The firewall is configured to only allow the minimum of services through, including both inbound and outbound port filtering.
- ❖ The firewall controls outbound communications and does not allow (by default) all outbound connections.
- ❖ The firewall minimises the inbound connections.
- ❖ Firewall rules are specific and to defined IP addresses.
- ❖ Firewall rules strictly limit connections into and out of DMZ servers and only to required ports.
- ❖ The firewall provides a DMZ function for any public facing servers (by itself or in conjunction with another Stateful Firewall).
- ❖ The firewall is managed from a dedicated system that is defined in the firewall rules to prevent others modifying the firewall.
- ❖ The firewall is configured to alert the Administrator when (firewall hardware/software permitting):
 - Rules have been changed on the firewall.
 - Patches have been applied to the firewall.
 - The firewall has rebooted.
 - New updates are available for the firewall.

SOE 6.5.g.

The organization must provide a written report showing that firewalls have been independently tested by a skilled person who confirms they are operating correctly and securely in accordance with the configuration document and published ruleset.

SOE 6.5.h

The organization must provide copies of the qualifications held by the skilled person performing their independent test in accordance with **SOE 6.5.g**.

SOE 6.5.h.

The organization must provide their patching policy and strategy in accordance with **SOE 2.3.a**.

SOE 6.5.i.

The patching policy and strategy must show that the patching and updating of the firewall(s) is(are) included.

How this evidence may be generated:

Policy and configuration documents should be produced as printed documents. Firewall rule sets can be output from the firewall management console if possible, or as a printed document. Independent testing reports should provide clear cross-referencing to the configuration and rule set documents against which compliance was checked.

Details of the pass or fail criteria for SOE 6.5

SOE 6.5 The organization will be deemed to have been failed if any of the fail criteria are met or are outstanding at the end of the audit period:

Fail Criterion 1:

Failure to present a full hard copy of the list of firewalls and servers.

Fail Criterion 2:

Failing to produce the firewall rule set containing all the elements of **SOE 6.5.b**

Fail Criterion 3:

Failing to produce the firewall configuration document.

Fail Criterion 4:

The firewall configuration document does not contain 2 or more of the evidence elements from **SOE 6.5.d**.

Fail Criterion 5:

The firewall configuration document does not contain 2 or more of the evidence elements from **SOE 6.5.f**.

Fail Criterion 6:



The organization fails to provide an independent test report for the firewall(s)

Fail Criterion 7:

The report does not verify that the firewall is operating in accordance with the configuration document and rule set presented to meet **SOE 6.5.b** and **SOE 6.5.e/SOE 6.5.f**.

Fail Criterion 8:

The organization does not provide their patching policy and/or strategy.

Fail Criterion 9:

The patching policy or strategy does not include the firewall(s).





Consider Further Enhanced Technologies

Statement of Evidence (SOE) Number: SOE 6.6

Overview:

The organization should consider implementing additional technologies which will further enhance their overall network security profile.

Statement of Evidence (SOE) Description:

This Requirement is an advisory which Certified Digital Security strongly recommends is given consideration. However, the requirement is not audited.



Regular Vulnerability Analysis

Statement Of Evidence (SOE) Number: SOE 6.7

Overview:

This is to confirm that the organization conducts regular vulnerability analysis tests and uses the results to maintain secure network operation.

Statement of Evidence (SOE) Description:

SOE 6.7.a.

The organization must present a report showing that a vulnerability analysis was conducted in the preceding 12 months.

Where the organization is unable to carry out the vulnerability analysis or has been a member of the CDS scheme for less than 6 months a waiver may be applied for from the CDS Certification Body. The waiver must be presented at the CDS audit.

SOE 6.7.b.

The organization must produce a test plan for the conduct of the vulnerability analysis.

SOE 6.7.c.

The test plan must include:

- ❖ The scope of the system or network being tested.
- ❖ The testing methodology to be used in the test.
- ❖ A step-by-step breakdown of the methodology to show that it is repeatable.
- ❖ How the methodology accounts for the threat vectors identified for the tested system.
- ❖ The extent of testing, i.e. whether any attempts will be made to exploit or quantify any vulnerability found during testing.
- ❖ The intended protection and recovery strategies and procedures in the event of the test causing a system failure.
- ❖ An incident response plan to deal with any immediate problems such as evidence of an attack in progress, or the discovery of illegal material or incriminating evidence on the system.

SOE 6.7.d.

The test plan must be signed as being agreed and approved by both the tester and the organization under test. The signature must also be annotated as binding both parties to

the conduct of the test in accordance with the plan.

SOE 6.7.e.

The test plan must be signed by the person conducting the vulnerability analysis, or team leader if there is more than one tester, and a senior representative of the organization being tested.

SOE 6.7.f.

The organization must present copies of the tester's qualifications. The qualifications must be:

- ❖ Relevant
- ❖ Appropriate
- ❖ In-date

SOE 6.7.g.

The organization must provide a copy of the tester's CV.

SOE 6.7.h.

The organization must present a vulnerability analysis test report.

SOE 6.7.i.

The report must contain the following elements:

- ❖ Cross-reference to the test plan against which the testing was carried out.
- ❖ A statement that the test was carried out in accordance with the referenced test plan.
- ❖ Clear identification of who conducted each part of the test and a note of their qualifications/experience.
- ❖ An explanation of how false positives were checked and removed.
- ❖ An explanation of the issues, concerns, vulnerabilities and weaknesses discovered during the test.
- ❖ Where appropriate, any instances of Trojans, root kits and ongoing hacking and the action taken at the time in accordance with the test plan.

SOE 6.7.j.

The organization must present the test report in the following format:

Note: This will be easier if the report format forms part of the tester's deliverables for the task.

❖ ***An Executive Summary.***

- No more than two facing pages for busy executive readers.
- No technical terms unless absolutely necessary.
- No abbreviations unless common within the tested organization.

❖ ***An overview of the testing activity.***

- Detailing the dates of the testing.
- The Tester(s) involved.
- The Tester(s) Qualifications.
- The location(s) where testing was carried out.

❖ **The Detailed Testing Results:**

- The technical detail relating to each issue identified in the test.
- Graphical demonstration of the problems (screen shots) where appropriate.
- An explanation of why this is a problem for the organization.
- An explanation of how to fix the problem.
- Use should be made of Red, Amber, Yellow and Green codes to indicate risk:
 - Red - Exploitable issue.
 - Amber - Vulnerability exists.
 - Yellow - Unnecessary service running or something that could be done better.
 - Green - Good practice, a laudatory note.
- A list and description of the tools actually used during the test.

❖ **Additional Information Annex.**

- All supporting and supplementary information should be placed in this Annex, including but not limited to:
 - The testing output such as the raw data from the tools where the licence allows.
 - Screenshot or banner-grabbed evidence where it adds value.
 - Client software or licensing information where issues have been found.

SOE 6.7.k.

The organization must provide a statement, signed by the IT manager, confirming that the test report was delivered or produced securely and not sent by normal email to the organization. The means of delivery must conform to the acceptable methods listed in **REQ 6.7.**

SOE 6.7.l.

The organization must present evidence that the findings of the report have been addressed within 6 months of the test. This evidence can take the form of either:

- ❖ An action plan detailing their intended corrective actions and the expected completion date, **only for organizations that have completed their first vulnerability analysis within the preceding 3 months of the date of CDS audit.**

Or

- ❖ Two audit reports showing that issues present in the first report have not been identified in the subsequent one.

SOE 6.7.m.

The action plan must be endorsed, in writing, by senior management committing to undertaking the corrective actions it contains.

How this evidence may be generated:

All plans and reports should be produced as printed documents, with the exception of the test report's Additional Information Annex. The annex can be produced on CD or DVD and accompany the report. Evidence of qualifications and the tester's CV can be provided as certified copies of the original documents.

Details of the pass or fail criteria for SOE 6.7

SOE 6.7 The organization will be deemed to have been failed if any of the fail criteria are met or are outstanding at the end of the audit period:

Fail Criterion 1:

Failure to provide a copy of the latest vulnerability analysis report or a waiver issued by the CDS Certification Body.

Fail Criterion 2:

Failing to produce a test plan for the conduct of the vulnerability analysis.

Fail Criterion 3:

The test plan does not contain all the elements in **SOE 6.7.c**.

Fail Criterion 4:

The test plan is not signed as being agreed and approved by both the tester and the organization under test.

Fail Criterion 5:

The test plan is not signed by the person conducting the vulnerability analysis, or team leader, and a senior representative of the organization being tested.

Fail Criterion 6:

Failing to present copies of the tester's qualifications.

Fail Criterion 7:

Failing to present a vulnerability analysis test report.

Fail Criterion 8:

The report does not include all the elements of **SOE 6.7.i**.

Fail Criterion 9:

Failing to provide a statement, signed by the IT manager, confirming that the test report was delivered or produced securely in accordance with **SOE 6.7.k**.



Fail Criterion 10:

Failing to provide either an action or 2 audit reports in accordance with **SOE 6.7.I.**

Fail Criterion 11:

The action plan is not endorsed, in writing, by senior management.





LOGISTICS FOR A CDS LEVEL 6 AUDIT

The audit process for CDS has been designed to be extremely efficient in terms of time for both Auditor and the organization. The following outline the requirements for CDS Level 6 audits.

DURATION

A CDS Level 6 audit should take no longer than the following, depending upon the size of the organization:

Tiny – Small	-	3 day
Medium	-	3 day
Large	-	4 days (*possibly 5)

ROOM REQUIREMENTS

The room provided for the Auditor must have a desk no smaller than 1.8m wide and 0.6m deep (ideally the desk would be 2 - 2.2m long and 0.8 - 1.0m deep). The desk must comply with all national safety requirements in terms of height, stability and surface finish. The room must be a correctly heated, quiet and well lit space designed and appropriate for normal human occupation and administrative working (i.e. a small desk in a cold and noisy server room is not appropriate).

Remember, the Auditor does not require access to your IT system but may require access to staff or other documents; do not place them where general talking is frowned upon (e.g. a call center operations floor).

Fresh water should be provided (ideally, not on the table with all the documents).

A local safe power outlet should be provided should the Auditor require it for his IT. A telephone is not mandatory but may assist the organization if the Auditor is not being escorted throughout their visit and they find a problem with the evidence provided.



DESK AND DOCUMENT LAYOUT

Possibly one of the most important elements is the layout of the desk for the Auditor as it will also serve as a check list for those preparing for the audit. The following diagram shows the location of the various sections for the CDS Level 4 Audit.

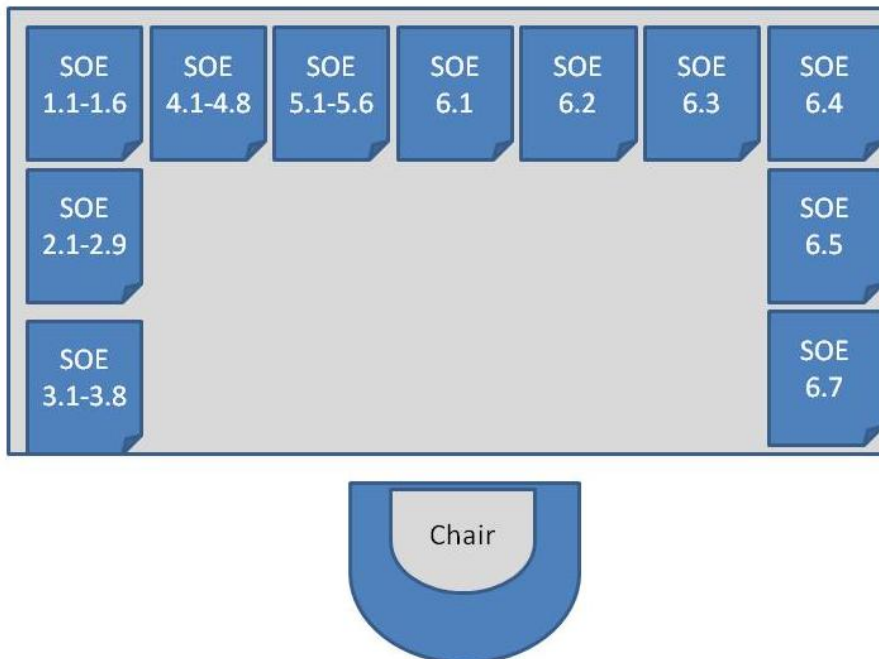


Figure 1 - CDS Level 6 SOE arrangement

Each collection of evidence generated to meet a particular SOE requires a cover sheet to allow the Auditor to quickly see which SOE it pertains to. Sheets can be locally produced and need only have the SOE number printed/written on the front. Advanced cover sheets will be available from the CDS website⁴ and these will include a series of checkboxes to ensure that the organization has not omitted any evidence.

Thus, if the Auditor arrives and observes a missing or thin pile, they can raise a query with the organization, who will then have time to remedy the situation. If any SOE is completely missing, the organization will fail the audit.

The blank paper is for the Auditor to make notes upon and the rest of the area is provided for them to read and work on.

⁴ www.certifieddigitalsecurity.com