



Certified Digital Security Level 5

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 5.



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 5.....	6
Part 3 CDS Audit Requirements	27
Logistics for a CDS Level 5 Audit	50





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 5 will be required to fully implement, or will have already fully implemented, all of the Level 1, 2, 3 and 4 requirements.

Specifically, Level 5 requires the organization to have the following:

Nominated IT Security Staff - an organization will have a reliable group responsible for security matters as part of their duties who will understand the ethos, focus and objectives of the organization an important aspect of delivering a tailored solution. *Regular Review of Barriers by Audit* allows the organization to gain confidence from their work, whilst directing focus to areas that are weaker or that represent higher risk. The *Audit* will also reinforce and verify the implementation of the system Configuration Control.

By mandating *Encryption of all Laptops* and *Securing Mobile Devices* (PDAs, Mobile/Smart Phones) an organization can be confident that the loss or theft of these attractive items of equipment will only cost the replacement of the hardware, and not develop into a Public or Client Relations incident affecting confidence and stakeholder value in the organization. Finally, by *Locking Down USB Ports* the organization can be confident that their data is not exported or migrated without their knowledge or consent.

With Level 5 implemented, an organization can expect to see:

- A more responsive security team that are more efficient and in tune with the organization.
- Reduced risk of a PR disaster following a laptop, PDA or phone theft or loss.
- A more stable system as USB devices are blocked.
- Reduced insider threat as data export means are removed.
- An ongoing programme of auditing.



PART 2

REQUIREMENTS FOR LEVEL 5





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 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.

CDS Audits are speedy as, where possible, all evidence is simply being checked to ensure it is correct, relevant and compliant. CDS Audits are check sheet orientated (where possible) to remove any ambiguity/hearsay/interpretation and other subjective inputs that 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 that documents are kept in the format they are provided in.

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

Named IT Security Staff

Requirement Number: REQ 5.1

Overview:

The organization must have an individual or group responsible for the provision of IT Security outputs. These personnel can be either internal staff or the function can be outsourced. There is no requirement at this stage for IT Security to be their primary role.

Responsible Group or Users:

Senior management must ensure named IT security staffs are nominated and have a reporting chain independent of the system administrators.

Requirement Description:

Named IT Security Staff (either by name, role, department or position) must be nominated to provide the IT security support to the organization, promoting awareness of the organizations goals, processes and ethos.

The staff are not required to be dedicated to security (that comes at CDS: Level6), it may be an additional or secondary role they undertake. [Note: The organization may exceed this requirement; this guide only identifies the minimum that they are required to demonstrate for compliance evidence].

Ideally these staff:

- ❖ Will be internal to the organization, as they will already understand the functions and ethos of the organization.
- ❖ Should be aware of the organization's 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.

This requirement can be outsourced to a specialist company, however, depending upon the size of the company taking on this responsibility, the list of Named Security Staff could be long. If it is outsourced, the following apply:

- ❖ The same named person(s) should regularly support the organization (the specialist company should be able to produce the list of names).

- ❖ Organizations should seek (at the very least) a face to face meeting with the head or lead IT Security person from the company.
- ❖ Ideally outsource staff (or at least their lead IT security person) should be inducted into the organization so they may gain an understanding of the organization's methods, risks and data moving processes.

The suggested sizes of staff pools are (note these are not necessarily full time staff):

- ❖ 1-3 persons - organization 1-50 systems.
- ❖ 3-5 persons - organization 50-200 systems.
- ❖ 5-10 persons - organization 200-1000 systems.
- ❖ 10-20 persons - organization 1000-5000 systems.

Benefits of Implementation:

By using named IT security staff the organization gains from more focused and skilled personnel able to quickly respond to, and resolve security incidents, greater emphasis placed on security implementation 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.

Security Staff Training

Requirement Number: REQ 5.2

Overview:

The organization must provide appropriate training for the staff responsible for the provision of IT security. This requirement includes security staff whether they are in-house or outsourced.

Responsible Group or Users:

Senior management must ensure that the named security staff either receive training or are already qualified in the skills detailed under the mandatory section of this requirement.

Requirement Description:

Within the security team (including the Named 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.

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:

By providing formal training for IT security staff the organization gains a workforce qualified to advise on, and implement, secure network features, respond appropriately to security events and develop further security enhancements in support of the organization's growth and change.

Recurring? If so frequency:

Training needs should be reviewed annually, perhaps as part of staff development reviews,

together with the continued relevance of the training courses attended. Further training, revalidation of qualifications and the obtaining of CPD credits also need to be reviewed annually.

Regular Review of Barriers by Audit

Requirement Number: REQ 5.3

Overview:

The organization must carry out regular technical audits of their security barriers to ensure they are still being operated, managed and supported in line with their approved configuration. Security barriers are defined as any device or software which, when operating correctly, control or prevent unauthorised or unwanted access to the IT system (examples include firewalls, IDS/IPS, anti-virus software, smartcards, biometrics).

Responsible Group or Users:

Senior management must ensure that the audits are undertaken on a regular basis. Appropriately qualified in-house IT security staff can undertake the audits and produce a report on their findings for senior management review, or the process can be outsourced to a specialist service provider.

Requirement Description:

- ❖ The auditing is to specifically cover and review:
 - The current 'controlled' configuration.
 - The industry best practice for each barrier device.
 - The common criteria guidelines (if the device is common criteria evaluated).
 - The configuration that best meets the organization's needs.
 - The current threats against the organization.
 - The manufacturer's guidelines (including any work-a-rounds for current issues).
- ❖ Where possible this should be undertaken at 6 monthly intervals.
- ❖ It can be conducted with in-house resources.
- ❖ Where in-house resources are used these must routinely operate outside the vertical reporting chain for the area being tested (ie they should not be expected to audit their boss).
- ❖ Significant changes to the barriers or network should trigger a re-run of the audit.
- ❖ The audit must be conducted by a qualified person and/or credible organization.
- ❖ The auditor must have the correct skills and qualifications.
 - The auditor must hold appropriate in date qualifications or professional body memberships (eg GSEC, CISA).
 - The auditor must be appropriately insured during the audit.
 - The auditor should provide a CV and statement of compliance for inspection at the audit point.
- ❖ All reporting and certification requirements are still required for in-house sourced resources.

The Audit must be correct and complete

- ❖ The audit must be conducted to an Audit Plan which must be available for inspection.
- ❖ The subsequent Audit Report must:
 - Refer to the Audit Plan.
 - Identify who conducted what part of the audit and their qualifications/experience.
 - Demonstrate that the audit plan's activities were conducted correctly.
 - State clearly if any false positives were found and, if so, how they were checked and removed.
 - Identify the issues, concerns, vulnerabilities and weaknesses in the system.
 - Clearly identify how the issues found can be fixed in the immediate and medium term.
- ❖ The organization carrying out the audit must have approved methodologies.
- ❖ The methodologies must ensure all aspects of the system are included and covered by the audit (as per the audit plan).
- ❖ The methodology must be:
 - Defined by the organization.
 - Documented and repeatable.
 - Approved by the organization being audited.

- ❖ The auditor must use licensed tools and software (i.e. legally owned and operated by the auditor).

Reporting requirements

The post audit 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.

Benefits of Implementation:

By carrying out regular reviews of security barriers the organization will gain assurance that they are configured and operating as expected. The audit report will give the organization the opportunity to develop and refine their protective measures in line with their business aspirations and goals.

Recurring? If so frequency:

Annually.

Laptop Encryption

Requirement Number: REQ 5.4

Overview:

The loss of even a single laptop has the potential to seriously embarrass the organization. Depending on the organization's location, line of business or regulatory requirements, the resulting public disclosure of the fact has measurable impact upon the reputation, value and

commercial standing of the organization. Furthermore, the potential loss of valid user credentials, stored passwords, wireless and VPN passwords and general network intelligence make the impact to the overall security posture severe.

Responsible Group or Users:

Senior management must ensure that the requirement for laptop encryption is included and endorsed in the organization's security policy.

IT support staff responsible for the configuration and issue of laptops must ensure that suitable encryption (as defined in this requirement) is installed in accordance with the manufacturer's instructions.

Requirement Description:

To reduce the damage the loss of a laptop device will incur all such devices must be encrypted.

The following types of encryption algorithm can be used, the difference being the performance versus security trade off:

- ❖ 3DES (also known as Triple DES).
- ❖ AES128
- ❖ AES256
- ❖ FIPS140-2
- ❖ FIPS140-3
- ❖ AES256

Check the website (www.certifieddigitalsecurity.com) for details of the standards of encryption as well as reliable products.

File level encryption is not acceptable by itself, although it may be used to add privacy to certain data while the system is running; only Whole Disk Encryption (WDE) or Full Disk Encryption (FDE) will prevent customer or system data from being accessed.

Benefits of Implementation:

With laptop encryption implemented, organizations will reduce the impact of a loss. This will allow for resource to be focused on investigation of the circumstances of the loss and the implementation of measures to prevent recurrence rather than on emergency damage limitation activities to protect reputation or legal position.

Recurring? If so frequency:



Once implemented encryption products and keys should be updated periodically in line with the manufacturers' recommendations.



Mobile device lockdown

Requirement Number: REQ 5.5

Overview:

Personal Digital Assistants (PDAs) have evolved into smart/camera phones with a wide array of capabilities (3G, GPRS data, Memory slots and mega pixel cameras), they are now vital business assets and extensions of the organizational LAN.

As many devices store, email, web history, corporate contact lists, cached network accounts and passwords; their loss will be embarrassing and place the organization at risk.

Responsible Group or Users:

Senior management must issue endorsed policy requiring that all mobile devices capable of being connected to the organization's network (including mobile telephones, personal organisers and USB data storage devices) are locked down.

The network administrators are to produce a configuration document detailing the lockdown measures to be applied to any device able to connect to the organization's LAN.

Requirement Description:

The following measures must be implemented for mobile devices:

- ❖ BlackBerry and other mobile devices should be encrypted where solutions are available.
- ❖ A locking code (PIN) must be implemented that prevents access to the stored data or functions (not including phone answering capabilities).
- ❖ Devices which cannot support the use of a PIN should be prevented from connecting to the organization's LAN.
- ❖ The device should wipe its internal volatile memory in the event that:
 - The user fails to enter the correct PIN/code 5 times (in a row). Where possible this number should not be reset by either a 'cooling off' period or by switching off and restarting the device.
 - The organization initiates a Remote Wipe upon receiving information that the device

is lost or compromised.

Benefits of Implementation:

As with laptops, mobile device lockdown minimises the impact of a loss, protects corporate data and reduces the need for emergency response measures.

Recurring? If so frequency:

Devices should be updated in line with their manufacturers' patches and updates. Where methods are found to lock down existing devices which previously could not be locked down, those methods are to be implemented.

USB Lockdown

Requirement Number: REQ 5.6

Overview:

USB ports and devices represent significant data export and system attack vectors, the USB ports are to be controlled or lockdown to only allow the organization's owned, known and approved devices the ability to connect.

Responsible Group or Users:

Senior management must issue endorsed policy requiring that USB ports be controlled or locked down.

The network administrators are to produce a configuration document detailing the lockdown measures to be applied to USB ports, and are to configure the organization's LAN in accordance with the document.

Requirement Description:

The organization must have a policy governing the use of USB.

All USB Devices connected to the system should be audited i.e. the details of all connected devices is to be recorded by the system (manufacturer, device type, device instance ID, serial number). Where the device is connected during a user's active session, the log should include the user's ID (where possible) or at least the system it was connected to.

Only approved devices should be able to logically connect to the system.

The system must be able to block access to USB devices not authorised by the organization.

Strong consideration should be given to encrypting external removable USB media.

The system should alert security staff when an unauthorised device is connected to the system.

See the CDS website www.certifieddigitalsecurity.com for 3rd Party software known to meet



these requirements.

The organization should be able to examine **any** USB devices including:

- ❖ When items are brought onto site.
- ❖ When items are taken off site.

Benefits of Implementation:

With USB ports controlled or locked down, an organization will reduce the number of possible means of introducing malicious software and exploit tools, and close another avenue for the surreptitious removal of data.

Recurring? If so frequency:

USB lockdown forms a security barrier which should be included in the Review of Barriers by Audit requirement (**REQ 5.3**)





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.

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





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;

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.

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





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.

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.

Named IT Security Staff

Statement of Evidence (SOE) Number: SOE 5.1

Overview:

The organization must provide evidence that they have an individual or group responsible for the provision of IT Security outputs. These personnel can be either internal staff or the function can be outsourced. There is no requirement at this stage for IT Security to be their primary role.

Statement of Evidence (SOE) Description:

SOE 5.1.a

The organization must present details of the staff nominated as responsible for IT security (by name, role, department or position). If the function is outsourced, the organization must provide details of the company in addition to the names of the individuals.

SOE 5.1.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 5.1.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 5.1.d

The organization must show how they have based the size of their IT security provision (see the guidance provided in **REQ 5.1**).

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 5.1:

SOE 5.1 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 named IT security staff as defined by **SOE 5.1.a**.

Fail Criterion 2:

The organization fails to produce details of the nominated IT security staff as defined by **SOE 5.1.a**.

Fail Criterion 3:

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

Fail Criterion 4:

The size of the IT security staff pool is unjustified, undefined or is 50% or less of the minimum number suggested in **REQ 5.1**.

Security Staff Training

Statement of Evidence (SOE) Number: SOE 5.2

Overview:

The organization must provide evidence that appropriate training is provided for the staff responsible for IT security. This requirement includes whether they are in-house or outsourced staff.

Statement of Evidence (SOE) Description:

SOE 5.2.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 5.2.b

The organization's statement must show that the optional elements (Wireless Security and Penetration Testing (See **REQ 5.2**)) of the CDS training requirements form part of their IT security staff development plans.

SOE 5.2.c

The organization must present details of the staff nominated as responsible for IT security (by name, role, department or position). If the function is outsourced, the organization must provide details of the company in addition to the names of the individuals.

SOE 5.2.d

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

SOE 5.2.e

The organization must provide evidence that at each of the primary 5 requirements listed below are covered by its staff. The optional Wireless security skills are considered mandatory if wireless is deployed in the organization; this can replace the 4.c Wireless device configuration requirement (so only 5 are still required)

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 5.1.f

The organization must produce the certificates and qualifications held by their administrators which support the requirements of **SOE 5.2.e**

SOE 5.1.g

Certificates and qualifications presented under **SOE 5.2.f** must be in-date.

SOE 5.2.h

The organization must produce copies of the syllabi of all training courses undertaken to support the requirements of **SOE 5.2.e** and **SOE 5.2.f**.

SOE 5.2.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 5.2.h** must be those produced by the training provider of the course in question.

Details of the pass or fail criteria for SOE 5.2:

SOE 5.2 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 5.2.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 5.2.e** and **SOE 5.2.f**

Fail Criterion 7:

Certificates and qualifications presented under **SOE 5.2.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 5.2.e** and **SOE 5.2.f**.

Fail Criterion 9:

The syllabus evidence in **SOE 5.2.h** fails to cover 2 or more elements of any one of the mandatory training courses detailed in **SOE 5.2.e**.

Regular Review of Barriers by Audit

Statement of Evidence (SOE) Number: SOE 5.3

Overview:

The organization must demonstrate the conduct of regular technical audits of their security barriers to ensure they are still being operated, managed and supported in line with their approved configuration.

Statement of Evidence (SOE) Description:

SOE 5.3.a

The organization must produce evidence that security barriers are reviewed by regular audits as part of the organizational security policy. The policy must require that:

- ❖ Audit reports fulfil the evidence requirements of **SOE 5.3.c**
- ❖ Audit s are conducted 6 monthly where feasible, or justification be given as to why this cannot be achieved.
- ❖ The audit covers:
 - The current 'controlled' configuration.
 - The industry best practice for each barrier device.
 - The common criteria guidelines (if the device is common criteria evaluated).
 - The configuration that best meets the organization's needs.
 - The current threats against the organization.
 - The manufacturer's guidelines (including any work-a-rounds for current issues).
 - Significant changes to the barriers or network should trigger a re-run of the audit.
 - The audit must be conducted by a qualified person and/or creditable organization.

SOE 5.3.b

The organization must produce copies of their audit reports covering the previous 12 months unless they have joined the CDS scheme during the last 6 months.

SOE 5.3.c

The organization must provide evidence that the audit was conducted correctly and completely.

SOE 5.3.d

The organization must produce the audit plan used for their audits.

SOE 5.3.e

The organization must provide copies of the audit methodology used to carry out their audit. The methodology must be defined such that it can be repeated as necessary and approved by the organization.

SOE 5.3.f

The organization must certify in writing that a check was carried out at the time of audit to verify that the auditor used licensed tools and software (i.e. legally owned and operated by the auditor).

SOE 5.3.g

The organization must provide copies of their Audit Report, which must:

- ❖ Refer to the Audit Plan.
- ❖ Identify who conducted what part of the audit and their qualifications/experience.
- ❖ Demonstrate that the audit plan's activities were conducted correctly.
- ❖ State clearly if any false positives were found and, if so, how they were checked and removed.
- ❖ Identify the issues, concerns, vulnerabilities and weaknesses in the system.
- ❖ Clearly identify how the issues found can be fixed in the immediate and medium term.

SOE 5.3.h

The audit report must contain the following elements:

- ❖ An Executive Summary
- ❖ 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.
- ❖ Annex for additional information

- Additional information should include the volume of auditing output; 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.

SOE 5.3.i

The organization must present the incident response plan they agree with the auditing organization

SOE 5.3.j

The organization must produce its own incident response plan.

SOE 5.3.k

The audit report must contain a section for senior management comments and endorsement.

SOE 5.3.l

Issues that have been outstanding for 2 consecutive audit reports must have an action plan against them for corrective action before the next scheduled audit. Issues which remain uncorrected for 2 CDS audits will result in the award of a fail.

SOE 5.3.m

Where in-house resources are used for audit, the organization must show that these resources routinely operate outside the vertical reporting chain for the area being tested.

SOE 5.3.n

The organization must provide evidence that the auditor had the correct skills, qualifications and professional indemnity in accordance with **REQ 5.3**

SOE 5.3.o

The organization must provide evidence that the auditor was appropriately insured during the audit.

How this can be generated:

The audit policy should form part of the organization's security policy and be produced in hard copy.

Audit reports should be produced as photocopies of the signed original.

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

Details of the pass or fail criteria for SOE 5.3:

SOE 5.3 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 produce an audit policy statement.

Fail Criterion 2:

The audit policy does not contain all the statements in **SOE 5.3.a**

Fail Criterion 3:

The organization fails to produce audit reports covering the last 12 months unless exempt by virtue of them joining CDS in the last 6 months.

Fail Criterion 4:

The audit report has 2 or more of the content elements from **SOE 5.3.g** missing.

Fail Criterion 5:

The audit report has 2 or more of the content elements from **SOE 5.3.g** missing.

Fail Criterion 6:

The audit report has not been reviewed by senior management

Fail Criterion 7:

There are issues that have been outstanding for 2 consecutive audit reports without an action plan against them for corrective action before the next scheduled audit.

Fail Criterion 8:

There are issues which have remained uncorrected since the last CDS audit.

Fail Criterion 9:

The organization fails to provide evidence that the auditor had the correct skills, qualifications and professional indemnity in accordance with **REQ 5.3**

Fail Criterion 9:

The organization fails to provide a copy of the auditor's CV.

Laptop Encryption

Statement of Evidence (SOE) Number: SOE 5.4

Overview:

Laptop computers (including notebooks and similar smaller portable IT) must have their hard drives encrypted. The organization must produce evidence that laptop encryption is enforced within its security policies, IT configuration documentation and is installed on all its laptops.

Statement of Evidence (SOE) Description:

SOE 5.4.a

The organization must produce an updated security policy mandating the use of whole disk encryption on all its laptop assets.

SOE 5.4.b

The organization must produce copies of their IT configuration control documentation as per **REQ 4.3**.

SOE 5.4.c

The organization's configuration control documentation must show that whole disk encryption forms part of the standard configuration for all laptops.

SOE 5.4.d

The organization must provide details of the encryption product they use.

SOE 5.4.e

The organization must demonstrate that the encryption product is compliant with one of the following algorithm types:

- ❖ 3DES (also known as Triple DES).
- ❖ AES128.
- ❖ AES256.
- ❖ FIPS140-2.
- ❖ FIPS140-3.

SOE 5.4.f

The organization must produce an in-use laptop for demonstration of its encryption when requested to do so. This must be a laptop selected, by the auditor, from the organization's asset list.

Note: The auditor will not require access to the machine, a demonstration of function is all

that is required.

How this can be generated:

The policy and configuration documents should already exist as part of earlier CDS requirements and can be produced in hard copy.

Details of the pass or fail criteria for SOE 5.4:

SOE 5.4 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 an updated security policy statement.

Fail Criterion 2:

The security policy does not include a requirement for whole disk encryption on all laptops.

Fail Criterion 3:

The organization fails to produce a configuration control document.

Fail Criterion 4:

The configuration control document does not show that whole disk encryption is part of the standard configuration of all laptops.

Fail Criterion 5:

The organization fails to produce a laptop computer when requested to do so.

Fail Criterion 6:

The laptop produced does not have whole disk encryption installed on it.

Fail Criterion 7:

The whole disk encryption product used by the organization does not use a CDS approved algorithmic standard.

Mobile Device Lockdown

Statement of Evidence (SOE) Number: SOE 5.5

Overview:

Organizations must show that they have implemented measures to protect mobile devices from unauthorised access to their data.

Statement of Evidence (SOE) Description:

SOE 5.5.a

The organization must produce an updated security policy mandating that all mobile devices must be locked down to prevent unauthorised access to them.

SOE 5.5.b

The organization must produce copies of their IT configuration control documentation as per **REQ 4.3**.

SOE 5.5.c

The organization's configuration control documentation must show that mobile devices have a locked down configuration prior to issue to a user.

SOE 5.5.d

The configuration control document must show that mobile devices are encrypted where possible.

SOE 5.5.e

The configuration control document must show that the following features are implemented:

- ❖ A locking code (PIN) is implemented that prevents access to the stored data or functions (not including phone answering capabilities).
- ❖ The internal volatile memory of the device will be wiped if:
 - The user fails to enter the correct PIN 5 times (in a row). Where possible this number should not be reset by either a 'cooling off' period or by switching off and restarting the device.
 - The organization initiates a Remote Wipe upon receiving information that the device is lost or compromised.

SOE 5.5.f

The organization must produce an in-use mobile device for demonstration of its lock down features when requested to do so. This must be a device selected, by the auditor, from the organization's asset list.

Note: The auditor will not require access to the device, a demonstration of function is all that is required.

How this can be generated:

The policy and configuration documents should already exist as part of earlier CDS requirements and can be produced in hard copy.

Details of the pass or fail criteria for SOE 5.5:

SOE 5.5 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 an updated security policy statement.

Fail Criterion 2:

The security policy does not include a requirement for mobile devices to be locked down.

Fail Criterion 3:

The organization fails to produce a configuration control document.

Fail Criterion 4:

The configuration control document does not show that a lock down is applied to all mobile devices before they are issued to a user.

Fail Criterion 5:

The organization fails to produce a mobile device when requested to do so.

Fail Criterion 6:

The mobile device produced does not have a locked down configuration as per **REQ 5.5**.

USB Lockdown

Statement of Evidence (SOE) Number: SOE 5.6

Overview:

Organizations must show that they have implemented measures to lock down or control access to the USB functionality on their LAN.

Statement of Evidence (SOE) Description:

SOE 5.6.a

The organization must produce an updated security policy. The policy must make clear statements on the following topics:

- ❖ The policy governing the use of USB devices.
- ❖ Mandating that personally owned USB devices are prohibited from being connected to the corporate network.
- ❖ Whether or not it has chosen to use encrypted USB devices and the rationale for the decision.
- ❖ The policy on examination of any USB device brought onto, or removed from, its site(s).

SOE 5.6.b

The organization must produce copies of their IT configuration control documentation as per **REQ 4.3**.

SOE 5.6.c

The organization's configuration control documentation must show that USB devices are managed and controlled.

SOE 5.6.d

The organization must be able to demonstrate the following features of their USB lockdown:

All USB Devices connected to the system are audited by the system (manufacturer, device type, device instance ID, serial number and, where possible, the user session responsible for connection of a device).

Only approved devices are able to logically connect to the system.

The system is able to block access to USB devices not authorised by the organization.

Where used, removable media encryption meets the same standard as laptop encryption **REQ 5.4**.

Note: The auditor will not require access to the LAN, a demonstration of function is all that

is required.

The system alerts security staff when an unauthorised device is connected to the system. **Alternatively a log is made of the activity for later investigation – this method will require a waiver certificate from the CDS Certification Body prior to the audit.**

How this can be generated:

The policy and configuration documents should already exist as part of earlier CDS requirements and can be produced in hard copy.

Details of the pass or fail criteria for SOE 5.6:

SOE 5.6 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 an updated security policy statement.

Fail Criterion 2:

The security policy does not include all the statements as per **SOE 5.6.a**

Fail Criterion 3:

The organization fails to produce a configuration control document.

Fail Criterion 4:

The configuration control document does not show that USB devices are managed and controlled.

Fail Criterion 5:

The organization fails to provide access to the LAN when requested to do so.

Fail Criterion 6:

The LAN configuration does not possess all the functionality as per **SOE 5.6.d** or is not covered by a valid waiver certificate issued by the CDS Certification Body.



LOGISTICS FOR A CDS LEVEL 5 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 5 audits.

DURATION

A CDS Level 5 audit should take no longer than the following, depending upon the size of the organization:

Tiny – Small	-	2 day
Medium	-	3 day
Large	-	4 days

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, or to have specific features of your IT system demonstrated; 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 their 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 5 Audit.

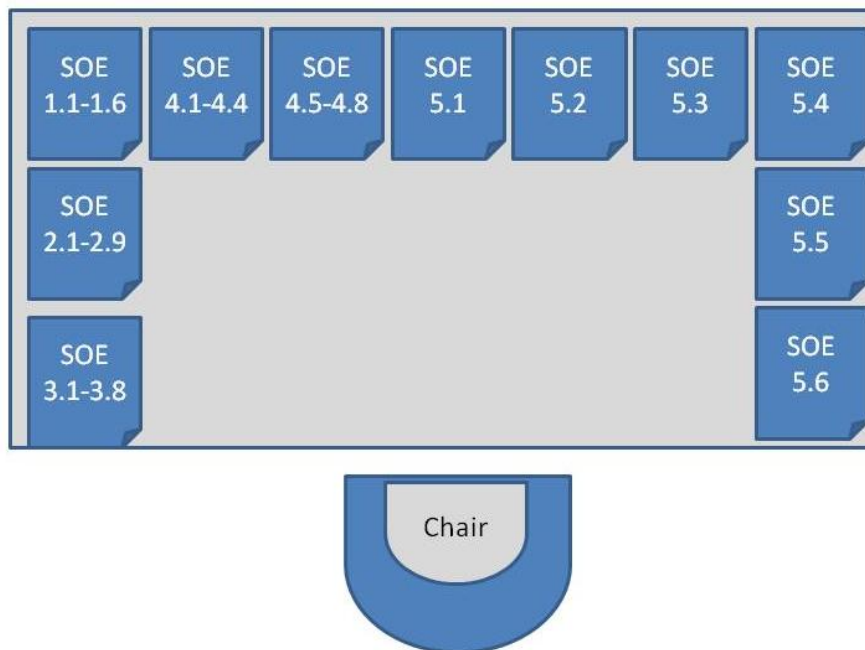


Figure 1 - CDS Level 5 SOE arrangement

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



Certified Digital Security Level 5
Implementation Guidance Document

