



# Certified Digital Security Level 4 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 4.*



*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 4..... 6

Part 3 CDS Audit Requirements ..... 22

Logistics for a CDS Level 4 Audit..... 43





## INTRODUCTION

The Certified Digital Security (CDS) Levels were designed to allow an organization's IT administrative and security staff to improve their security, step by step, 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 having no Anti Virus software or of 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 and leading to a system which is progressively better managed, more secure and ultimately, more robust. The steps are reasonable but the accumulation is very effective. With this in mind, 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 which 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 whether or not 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 in order to make your systems more secure.

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

Level 4 represents the first of the **Enhanced** CDS Levels; here the focus switches to controls that are more technical. Specifically, Level 4 requires the organization to have the following:

By *Hardening the Public Facing Servers* the organization reduces the attack surface and potentially vulnerable software. Replicating the Lock Down process on the internal servers will reduce the risk of an internal attacker being able to take control of servers and the data or resources they control. By *Controlling Remote Access* and blocking users from connecting personal or external systems by VPN to the corporate LAN, the export of data risk is significantly reduced.

By adopting *Increased Levels of System Logging*, the organization is better able to identify and stop attackers whilst providing greater post incident information for analysis. *Configuration Control* will ensure this effort is maintained and sustained, by keeping the systems in the known state.

The *Risk Register* will allow management and technical staff to share visibility of the risks one group is managing and the other group is defending against. It is intended that this will allow the organization to communicate better the importance and criticality of the IT Systems to the organization. *USB Auditing* will deter users from using non-approved or external USB Devices in the organization, reducing both data leakage risks and USB based attacks. Finally, the mandating of WPA and WPA2 ensures that the highest level of Wi-Fi encryption is implemented, protecting the network from eavesdropping and attack. With Level 4 implemented, an organization can expect to see:

- Fewer defacements and better uptime of public servers.
- Better performing Internal Servers through service and software minimization.
- Better control of their Configuration.
- A greater understanding of the Risk they are carrying.
- Greater control of where their data goes.
- Improved security where Wireless is used.



## PART 2

# REQUIREMENTS FOR LEVEL 4



## 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](http://www.certifieddigitalsecurity.com)) is also open source and is given freely to the community.

However, as part of the terms associated with the release of CDS materials, Digital Security Ltd 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 1s can be downloaded from the website for easy executive reading). Security is about trust and integrity; thus we hope that, 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 is comprised of 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 that 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. If the requirement is recurring and if so the recurrence period (eg annual training is required to be undertaken every 12 months or less).
8. Any notes relevant to the implementation of the recommendation.

# ***Harden Public Facing Servers***

**Requirement Number:** REQ 4.1

**Overview:**

The organization must secure all public facing servers and base-line them ie their configuration defined, recorded and the system backed up fully to read-only media (DVD/Blu-Ray).

**Responsible Group or Users:**

System administrators must securely configure the servers in line with the instructions contained in this requirement and measured against the organization's business need. Administrators are also responsible for the recording and backing up of the defined secure configuration.

**Requirement Description:**

The **documented** hardening process should include, cover or ensure:

- ❖ The servers should be patched to the highest level possible (as per CDS:REQ 2.3).
- ❖ The servers are backed up in the secure configuration.
- ❖ Removing all unnecessary services or ensuring that they are disabled.
- ❖ Ensuring that Public Facing servers do not have any internal network credentials entered, stored or cached.
  - For example, the policy should ensure:
    - That the server has never been added to the internal domain.
    - That the administrator/root account and password used in the installation are not used on the internal domain/administrator account.
  - Public Servers must never:
    - Be (or have been) members of the internal domain.
    - Be used as general systems.
    - Be used to browse the internet.
    - Be used to read publicly received email.
- ❖ Any new server that is to be public facing should be built securely.
- ❖ The server must be built from a known good data source.
- ❖ The server must be patched before being connected to the internet.
- ❖ The server must be hardened before being exposed to the internet. Not installed in the DMZ and then built in place.
- ❖ The server administrator accounts must not be using the same names or passwords as for internal LAN servers.

- ❖ Where possible, and for all new servers to be installed after a CDS Audit to level 4, the HDD must be wiped to ensure no internal LAN credentials are stored on it. Every sector of the HDD must be overwritten rather than formatted (where the flags to the data are removed, but the data itself remains), before being used.

**Benefits of Implementation:**

External servers will be more resistant to attack. In the event of a successful attack, post-incident recovery can be more readily achieved through use of the backed up configuration disks.

**Recurring? If so frequency:**

The configuration should be reviewed at least annually by the system administrators to ascertain whether the servers could be further hardened or whether additional business functionality requires some relaxation of the secure configuration. The review should include checking that the read only configuration disks are still current.

This review could be conducted in conjunction with the annual review of the Business Continuity and Disaster Recovery Plan in accordance with REQ 3.5.

# ***Harden Internal Servers***

**Requirement Number:** REQ 4.2

**Overview:**

The organization must secure all internal servers and base-line them (ie their configuration defined, recorded and the system backed up fully to read-only media (DVD/Blu-Ray))

**Responsible Group or Users:**

System administrators must securely configure the servers in line with the instructions contained in this requirement and measured against the organization's business need. Administrators are also responsible for the recording and backing up of the defined secure configuration.

**Requirement Description:**

The documented hardening process should include, cover or ensure:

- ❖ That all unnecessary services and software items are disabled or removed (unnecessary means any service not required for operational role of the server).
- ❖ The servers should be patched to the highest level possible (as per CDS:REQ 2.3).
- ❖ The servers must be backed up in the secure configuration, so a baseline is held, should the system need to be reverted to its initial configuration.
- ❖ The servers must not be used as general-purpose systems.
- ❖ The servers must not be used to browse the internet.
- ❖ Internal servers must never have been part of the organization's DMZ (as they could be importing Trojans, root kits or other software to assist an attacker).

**Benefits of Implementation:**

Internal servers will be more resistant to attack. In the event of a successful attack, post-incident recovery can be more readily achieved through use of the backed up configuration disks.

**Recurring? If so frequency:**

The configuration should be reviewed annually by the system administrators to ascertain whether the servers could be further hardened or whether additional business functionality requires some relaxation of the secure configuration. The review should include checking that the read only configuration disks are still current.

This review could be conducted in conjunction with the annual review of the Business Continuity and Disaster Recovery Plan in accordance with REQ 3.5.

## ***Configuration Control Implemented & Enforced***

**Requirement Number:** REQ 4.3

### **Overview:**

Configuration control ensures that only approved and recorded changes happen to the system. This prevents illegal, unstable or dangerous software from being installed.

### **Responsible Group or Users:**

The Senior Management must support the enforcement of configuration control by the system administrators. System administrators must have a process for preventing unauthorized configuration changes to the system and for controlling those that are authorized.

### **Requirement Description:**

The organization should nominate and empower a person or group to approve changes to the system. This person does not need to be technical; the decision to install software or hardware is more a business-orientated decision than a technical one.

This person or group can then work with both the IT and business groups to manage new system requirements, ensuring their implementation is controlled and managed.

Linked to account security and the REQ.1.4 whereby users do not use Administrator level accounts for day-to-day activities:

- ❖ Users must not be able to install software.
- ❖ Users must not be able to uninstall software.
- ❖ Users must not be able to disable any security product.

The organisation should have a system by system inventory of the software installed:

- This is usually in a database.
- This is often held and used (if not generated) by the helpdesk staff.
- This can be as simple as a spreadsheet with 'x' against software using a line for each PC or user group.

### **Benefits of Implementation:**

Systems will be more stable resulting in fewer helpdesk calls, less downtime and reduced support costs.

Changes to system configuration will be managed; ensuring that post incident recovery can be achieved quickly and easily from “known good” backups of the approved configuration.



**Recurring? If so frequency:**

The agreed configuration should be reviewed at least annually. Periodic checks of the actual configuration should be conducted at random intervals throughout the year with configuration change meetings being held as required to meet the business need.

**Notes:**

No configuration changes should take place without the approval of the configuration control body. Unapproved changes are a sign that control is not implemented.



# Create a Board level Risk Register

**Requirement Number:** REQ 4.4

**Overview:**

The organization must create and maintain a Register of Risks relating to or potentially impacting upon the organization or its IT.

**Responsible Group or Users:** System administrators should advise on security risks to a board level manager. Board level management must take ownership of risks to the organization's IT infrastructure.

**Requirement Description:**

The Risk Register should record at least the following:

- ❖ The serial number (so all items are referenced and unique).
- ❖ The source of the risk.
- ❖ A short description of the risk.
- ❖ A full description of the risk.
- ❖ The potential impact.
- ❖ A simplified Red/Amber/Green status of the risk.
- ❖ The event deemed to trigger the risk becoming an issue.
- ❖ The likelihood of the event occurring.
- ❖ The potential cost of rectification.
- ❖ The person that owns the risk.
- ❖ The chosen rectification method.
- ❖ The date the decision was made.
- ❖ The resulting risk after the action has been implemented.
- ❖ The date of review.

The Risk Register should be presented at regular intervals to the organizations senior staff (eg board of directors). The risk register should be presented in an easily readable and understandable format.

**Benefits of Implementation:**

The Management Board gain visibility of security-related risks and are better placed to make decisions based upon the needs of the business and the current level of risk. Active involvement of the Management Board in security risks will ensure appropriate funding and support for risk reduction strategies in line with the prevailing business conditions.

**Recurring? If so frequency:**

The Risk Register must be included in the agenda of senior staff meetings at least quarterly.

## *Increased Level of Logging*

**Requirement Number:** REQ 4.5

**Overview:**

Building upon the logging implemented in REQ 2.6, this requirement demands enhancements to logging. As the system is more complex, the level of fidelity and number of logging points should be increased.

**Responsible Group or Users:** System Administrators

**Requirement Description:**

As the level of logging has been increased, the network should have synchronized timeservers. Where the LAN is small, this could have all servers looking to internet time or other authoritative server. Where the organization is large, the timeserver should be an owned time server/appliance.

Logging must occur in the following places:

- ❖ All firewalls and boundary devices.
- ❖ All servers.
- ❖ All authentication points.
- ❖ All applications that require any authentication.
- ❖ All physical access to the servers or server rooms (not necessarily a digital log file).
- ❖ Where digital access control is implemented in a building that protects the servers or data stores.

For Operating System authentication and applications that use or require authentication, the logging should include:

- ❖ The time of the event.
- ❖ The server or node the event was recorded on.
- ❖ The event.
- ❖ The importance of the event.

The following events should be logged:

- ❖ User account creation, modification and deletion (both successful and unsuccessful attempts).
- ❖ Any changes of permissions (both successful and unsuccessful).
- ❖ Any logon attempt, local or remote (both successful and unsuccessful).
- ❖ The remote connection of any user to the LAN or RAS type node (both successful and unsuccessful attempts).
- ❖ Any attempt to change any security policy (both successful and failed attempts).

- ❖ Any reboot of any server.
- ❖ Any restart of any service on any server.
- ❖ Insertion or removal of any USB Storage device

**Benefits of Implementation:**

Implementation of enhanced logging will improve the performance of network troubleshooting through the provision of additional system information, as well as helping to detect and respond to attacks or other unauthorized user activity.

**Recurring? If so frequency:**

Logs should be:

- ❖ Constantly updated.
- ❖ Archived (ideally) weekly and at most monthly.
- ❖ Reviewed daily, but weekly is acceptable on small networks (with limited staff).

In large organizations with dedicated Systems Administrators, these logs should be reviewed and archived on a daily basis.

**Notes:**

With the increased logging requirements there is a risk that the amount of information will become unmanageable and therefore have no practical value. It is recommended that a software tools be used to interpret the logs and provide trend analysis.

# ***Auditing of USB devices***

**Requirement Number:** REQ 4.6

**Overview:**

All USB Devices connected to the system should be audited.

**Responsible Group or Users:**

Audit should be supported by a policy sanctioned by senior management.  
System Administrators should conduct checks of log files for USB device usage.

**Requirement Description:**

The organization should have a policy governing the use of USB devices. This should be incorporated as an update to the CDS: Level1 Security Policy (REQ 1.4).

Implementation of Auditing must include:

- ❖ Recording of the insertion of a device
- ❖ Recording of the filenames of data that is moved on and off the device.

The organisation should also have a process to examine all USB devices:

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

The organization should have a policy that allows them to deny a user/staff/visitor the right to bring a personal USB device onto site.

**Benefits of Implementation:**

The organization will be able to control the presence and use of USB devices; thus reducing the risk of unauthorized data copying / theft. Auditing will provide a deterrent to their unauthorized use.

**Recurring? If so frequency:**

The records of USB usage should be checked at the same time as the inspections of system logs in accordance with REQ 4.5.

# Control Remote Access

**Requirement Number:** REQ 4.7

**Overview:**

Only the organization's assets are permitted to connect to the network. Access away from the organization's premises must not break this rule.

This requirement is to prevent the organizations data being removed or the system being attacked by the use of external assets.

**Responsible Group or Users:**

Remote Access must be supported by a policy sanctioned by senior management. System Administrators should configure network services to control remote access.

**Requirement Description:**

The provision and use of remote access should be included in the organization's Security Policy (REQ 1.1)

Remote access may be implemented by:

- ❖ Having machine level passwords and not user level VPN passwords (ie the machine connects and authenticates to connect to the VPN before the user authenticates).
- ❖ Installing non-exportable certificates on the mobile assets.
- ❖ Use of 3rd party software (eg agent or 802.1x based).

Any implementation must prevent users from connecting their own laptops and systems to the organization's network, thus the use of standard commercial software with only a user level password that is given to the user is not secure (against an insider threat).

**Benefits of Implementation:**

The organization will be able to control connections from outside their premises without unnecessarily limiting the flexibility of mobile or remote workers. The preclusion of non-organizationally owned assets will prevent personal assets that do not meet the organization's secure configuration requirements presenting a means of attacking the network.

**Recurring? If so frequency:**

Provision of remote access should be reviewed annually by the management board.

## ***WiFi connecting to the LAN must use WPA***

**Requirement Number:** REQ 4.8

### **Overview:**

All wireless connectivity to the organization's data assets must use strong encryption.

### **Responsible Group or Users:**

System Administrators should configure wireless network services to use WPA.

### **Requirement Description:**

WEP encryption can be cracked in a few minutes with a laptop, a free suit of hacking tools and a laptop.

WPA2 is to be implemented between infrastructure and client connection, where older technology is still being used WPA is acceptable (until April 2012). No new hardware installations are permitted to use WPA or WEP (inc dynamic WEP), as these are insecure implementations of network encryption

Where possible, this should be implemented via an infrastructure implementation i.e. using AES and not TKIP encryption.

Very few exceptions are permitted and, where possible, these should be isolated from the main network (these may include):

- ❖ Presentation Screen control devices.
- ❖ Presentation support devices that display data but do not cache or process it (media centres).
- ❖ Window/blind control systems.
- ❖ Streaming music/video systems where the whole system is totally separate from the main network.

Wireless Access Points must be configured to refuse connections offering only Wired Equivalent Privacy (WEP) authentication.

All WPA passwords should be long and contain both upper and lower case characters, numbers and special characters.

Passwords should be at least 12 characters long, but ideally 20+ characters long.

### **Benefits of Implementation:**



The organization will be able to reduce the risk of their wireless networks being breached by unauthorized devices.

**Recurring? If so frequency:**

Wireless network configuration should be reviewed annually. The review should include consideration of newer or advanced protection technologies when they become available.





# PART 3

## CDS AUDIT REQUIREMENTS



## ABOUT THIS PART

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

## RECOMMENDED PROCESS

If the organization is 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 the 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.



## **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 can only be 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.

## **THE AUDIT PROCESS**

### ***ABOUT THE PROCESS***

CDS Audits are designed to check all the evidence<sup>1</sup> necessary to prove the requirements<sup>2</sup> have been met. They are designed to use check sheets wherever possible to remove ambiguity, hearsay, misinterpretation and other subjective types of inputs which may 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 actually 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 offer is not supported nor condoned by CDS or Digital Security. 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 to 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.

---

<sup>1</sup> Identified in the Part 3 of the guidance document for the Target CDS Level

<sup>2</sup> Identified in the Part 2 of the guidance document for the Target CDS Level



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 which have been presented for audit<sup>3</sup>. 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 hot debrief.

The Auditor will forward their report to the Certification Body (Digital Security).

The Certification Body will review the Auditor's report and, if satisfactory, will endorse the report's recommendation. The Certification Body will inform the organization of the result within four working days (usually one to two 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 Body will destroy their copy with ten working days (for security reasons).

The organization will be asked to confirm the level of publicity they would like, to which the CDS and Certification Body will adhere. Options include:

1. Listing on the CDS website with achieved level - either a level number or the level grouping e.g. 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 which pass a CDS level will be issued a unique reference which can be given to clients or external third parties. This can be quoted to CDS staff in order to receive a verification and validation of the organization's achievement.

---

<sup>3</sup> 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 COMPLETE**

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 which 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 which 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 SOEs for short. These are similarly indexed.

For example: The evidence for level 6 requirement number four (i.e. 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 comprises 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 the 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 of how the evidence can be generated.
7. The details of the pass/fail criteria, if known.
8. Any notes relevant to the SOE.



# ***Harden Public Facing Servers***

**Statement of Evidence (SOE) Number:** SOE 4.1

**Overview:**

The organization must provide evidence that all public facing servers are secured, their configuration defined and recorded, and the system backed up fully to read-only media (DVD/Blu-Ray).

**Statement of Evidence (SOE) Description:**

**SOE 4.1a**

The organization must present details of the current patch state of all public facing servers in accordance with SOE 2.3c.

**SOE 4.1b**

The organization must demonstrate that all server secure configurations are backed up. This can be demonstrated by the production of the media register showing the entries relating to server configuration backups.

**SOE 4.1c**

The organization must show that all unnecessary services are disabled by production of the network configuration records.

**SOE 4.1d**

The organization must assert in writing that:

- ❖ Public Facing servers do not have any internal network credentials entered, stored or cached.
- ❖ No externally facing server has ever been part of the internal domain.
- ❖ The administrator/root account and password used in the installation are not used on the internal domain/administrator account.
- ❖ Where any physical machine has been moved from the internal domain to the external domain, and all new servers to be installed after a CDS Audit to level 4, the HDD has been (or will be) wiped to ensure no internal LAN credentials are stored on it. This assertion must state that every sector of the HDD must be overwritten rather than formatted before being used.

**SOE 4.1e**

The organization must produce an updated Security Policy covering the following additional measures:

- ❖ Public Servers must never be (or have been) members of the internal domain.
- ❖ Public Servers must never be used as general systems.
- ❖ Public Servers must never be used to browse the internet.
- ❖ Public Servers must never be used to read publicly received email.
- ❖ Any new server that is to be public facing should be built securely.
- ❖ The new server must be built from a known good data source.
- ❖ The new server must be patched to the same standard as the defined network configuration before being connected to the internet.
- ❖ The server must be hardened to the same standard as the defined network configuration before being exposed to the internet.
- ❖ New servers must not be installed in the DMZ and then built in place.
- ❖ The server administrator accounts must not be using the same names or passwords as for internal LAN servers.

**How this can be generated:**

The patch status can be produced as printed output from the system. A photocopy of the relevant section of the media register is acceptable. The acceptable network configuration can be either a separate document or form part of the overall security policy document. The assertions of **SOE 4.1d** can be presented as a list of statements signed by a Senior Manager. **SOE 4.1e** can be met by amendment of the organization's security policy and producing the newly endorsed version at audit.

**Details of the pass or fail criteria for SOE 4.1:**

**SOE 4.1** 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 fails to produce details of the current patch state of all public facing servers.

**Fail Criterion 2:**

The organization fails to provide evidence of a backup regime for the server configuration.

**Fail Criterion 3:**

The organization fails to produce a server configuration document.



**Fail Criterion 4:**

The server configuration document does not show that unnecessary services have been disabled.

**Fail Criterion 5:**

The organization does not produce an assertion letter in accordance with **SOE 4.1d**, or the letter produced is missing 1 or more of the assertions.

**Fail Criterion 6:**

The organization's security policy is not produced.

**Fail Criterion 7:**

Where produced, the security policy has 2 or more of the additional items from **SOE 4.1e** missing.



# Harden Internal Servers

**Statement of Evidence (SOE) Number:** SOE 4.2

**Overview:**

The organization must provide evidence that all internal servers are secured, their configuration defined and recorded, and the system backed up fully to read-only media (DVD/Blu-Ray).

**Statement of Evidence (SOE) Description:**

To meet the evidence requirements the organization must:

**SOE 4.2.a.**

Show that the servers are patched to the highest level possible (as per CDS:REQ 2.3).

**SOE 4.2b**

Assert that all unnecessary services and software items are disabled or removed.

**SOE 4.2c**

Show that the servers are backed up in the secure configuration.

**SOE 4.2d**

Update their security policy to include the following measures:

- ❖ The servers must not be used as general purpose systems.
- ❖ The servers must not be used to browse the internet.
- ❖ Internal servers must never have been part of the organization's DMZ (as they could be importing Trojans, root kits or other software to assist an attacker).

**How this can be generated:**

The patch status can be produced as printed output from the system. Photocopies of the relevant section of the media register showing the creation and retention of backup media. The acceptable network configuration can be either a separate document or form part of the overall security policy document. The assertion of **SOE 4.2b** can be presented as a statement signed by a Senior Manager. **SOE 4.2d** can be met by amendment of the organization's security policy and producing the newly endorsed version at audit.

### Details of the pass or fail criteria for SOE 4.2

**SOE 4.2** 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 details of the current patch state of all internal servers.

**Fail Criterion 2:**

The organization does not provide an assertion that all unnecessary services have been disabled or removed.

**Fail Criterion 3:**

The organization fails to provide evidence of a backup regime for the server configuration.

**Fail Criterion 4:**

The organization's security policy is not produced.

**Fail Criterion 5:**

Where produced, the security policy has any of the additional items from **SOE 4.2d** missing.

## ***Configuration Control Implemented & Enforced***

**Statement of Evidence (SOE) Number:** SOE 4.3

**Overview:**

This will check that Configuration control is in place ensuring that only approved and recorded changes happen to the system.

**Statement of Evidence (SOE) Description:**

**SOE 4.3.a.**

The organization must provide written proof that someone or some committee within the organization is empowered to approve changes to the system.

**SOE 4.3.b.**

The organization must provide written proof that users cannot install or uninstall software.

**SOE 4.3.c.**

The organization must demonstrate that users are not able to disable any security product, such as anti-virus or local firewall software.

**SOE 4.3.d.**

The organisation must produce a system-by-system inventory of the software installed.

**How this can be generated:**

Proof of configuration control can be provided as printed output from the system's Group Policies showing that users are denied the ability to install, uninstall or disable software. A system-by-system inventory can be either a database printout, or a spreadsheet showing software against IT asset.

Proof of approvals for configuration changes can be either Terms of Reference for the individual or group empowered to make changes, or minutes of meetings where configuration control is discussed and formally endorsed.

### Details of the pass or fail criteria for SOE 4.3

**SOE 4.3** 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:**

Failure to produce Terms of Reference or Minutes of meetings showing that configuration control is discussed and formally endorsed.

**Fail Criterion 2:**

Failure to present a hard copy of the Group Policies controlling user permissions.

**Fail Criterion 3:**

Where hard copy Group Policies are produced, failing to prevent users from installing, uninstalling or disabling software as required by **SOE 4.3.b & 4.3.c**

**Fail Criterion 4:**

Failure to present a hard copy of the system-by-system inventory as required by **SOE 4.3.d**.

# Create a Board level Risk Register

**Statement of Evidence (SOE) Number:** SOE 4.4

**Overview:**

This will confirm that the organization has compiled and maintains a Register of Risks relating to or potentially impacting upon the organization or its IT.

**Statement of Evidence (SOE) Description:**

**SOE 4.4.a.**

The organization must present a Register of Risks relating to impacts on the organization or its IT systems.

**SOE 4.4.b.**

The Register of Risks must record:

- ❖ A serial number (so all items are referenced and unique).
- ❖ The source of the risk.
- ❖ A short description of the risk.
- ❖ A full description of the risk.
- ❖ The assessed potential impact.
- ❖ A simplified Red/Amber/Green status of the risk.
- ❖ The event deemed to trigger the risk becoming an issue.
- ❖ The likelihood of the event occurring.
- ❖ The potential cost of rectification.
- ❖ The person that owns the risk.
- ❖ The chosen rectification method.
- ❖ The date the rectification decision was made.
- ❖ The resulting risk after the rectification action has been implemented.
- ❖ The date of review.

**SOE 4.4.c.**

There must be a record of the regular reviews of the Risk Register by the organization's senior staff (eg board of directors).

**How this evidence may be generated:**

A print out of the Risk Register will suffice, providing this demonstrates compliance with **SOE 4.4.b and SOE 4.4.c**. Where the Risk Register does not record senior management reviews, separate documentary evidence of review will be required.



**Details of the pass or fail criteria for SOE 4.4**

**SOE 4.4.** Will be deemed to have been failed if any of the following criteria are met:

**Fail Criterion 1:**

The organization fails to present a hard copy of their Risk Register.

**Fail Criterion 2:**

The Risk Register does not contain the information required by **SOE 4.4.b.**



# *Increased Level of Logging*

**Statement Of Evidence (SOE) Number:** SOE 4.5

**Overview:**

This will demonstrate that the organization has expanded its system event logging.

**Statement of Evidence (SOE) Description:**

**SOE 4.5.a**

The organization must produce a network diagram showing the presence of a synchronized timeserver, or where the LAN is small (less than 40 user machines), other evidence of where the network time is synchronised from.

**SOE 4.5.b**

Log settings are to be provided for review.

**SOE 4.5.c**

Log settings must show that logging occurs in the following places:

- ❖ All firewalls and boundary devices.
- ❖ All servers.
- ❖ All authentication points.
- ❖ All applications that require any authentication.
- ❖ All physical access to the servers or server rooms (not necessarily a digital log file).
- ❖ Where digital access control is implemented in a building that protects the servers or data stores.

**SOE 4.5.d**

Log settings must show that for Operating System authentication and applications that use or require authentication, the logging includes:

- ❖ The time of the event.
- ❖ The server or node the event was recorded on.
- ❖ The event.
- ❖ The importance of the event.

#### **SOE 4.5.e**

The log settings must show that the following events are logged:

- ❖ User account creation, modification and deletion (both successful and unsuccessful attempts).
- ❖ Any changes of permissions (both successful and unsuccessful).
- ❖ Any logon attempt, local or remote (both successful and unsuccessful).
- ❖ The remote connection of any user to the LAN or RAS type node (both successful and unsuccessful attempts).
- ❖ Any attempt to change any security policy (both successful and failed attempts).
- ❖ Any reboot of any server.
- ❖ Any restart of any service on any server.
- ❖ The insertion or removal of any USB Storage device.

#### **SOE 4.5.f**

The organization must provide evidence that all logs are reviewed at least weekly.

#### **How this evidence may be generated:**

All evidence for **SOE 4.5** can be generated and printed by the system. In a Microsoft Windows Domain environment, this will be a printout of the GPOs that enable the logging on all Domain Controllers and Member Servers. On Unix systems, the auditing/logging settings will usually need to be printed from each server. These server numbers and types will be cross checked with **SOE 2.2.a**. Evidence of reviews can be either by screenshots of the logs under review, signed by the reviewer, or other printed output showing that a review was carried out.

#### **Details of the pass or fail criteria for SOE 4.5**

**SOE 4.5** 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 logging settings.

##### **Fail Criterion 2:**

The log settings failing to show that logging covers all the elements as required by **SOE 4.5.c, d & e**.

##### **Fail Criterion 3:**

Failing to provide evidence that the logs are reviewed at least weekly.

# ***Auditing of USB devices***

**Statement of Evidence (SOE) Number:** SOE 4.6

**Overview:**

This is to check that All USB Devices connected to the system are audited.

**Statement of Evidence (SOE) Description:**

**SOE 4.6.a.**

The organization must provide a written policy governing the use of USB devices.

**SOE 4.6.b**

The policy must be incorporated as an update to the Security Policy as required by **REQ 1.1**.

**SOE 4.6.c**

The policy must explain the implementation of auditing and must include:

- ❖ Recording of the insertion of a device
- ❖ Recording of the filenames of data that are moved on and off the device.
- ❖ A process to examine all USB devices:
  - When they are brought onto site.
  - When they are taken off site.
- ❖ A policy to deny a user/staff/visitor the right to bring a personal USB device onto site.

**How this can be generated:**

The policy must be produced as a hard copy document.

**Details of pass or fail criteria:**

**SOE 4.6** The organization will be deemed to have 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 USB Audit Policy (**SOE 4.6.a.**).

**Fail Criterion 2:**

Failure to incorporate the USB Audit Policy into the Security Policy required by **SOE 4.6.b.**

**Fail Criterion 3:**

Failure of the USB Audit Policy to include the items required at **SOE 4.6.c.**

# Control Remote Access

**Statement of Evidence (SOE) Number:** SOE 4.7

**Overview:**

This is to check that only the organization's assets are permitted to connect to the network and that access away from the organization's premises does not break this rule.

**Statement of Evidence (SOE) Description:**

**SOE 4.7.a.**

The organization must provide a Remote Access Control Policy.

**SOE 4.7.b**

The provision and use of remote access must be included in the organization's Security Policy as per REQ 1.1.

**SOE 4.7.c**

The security policy must mandate that remote access must be implemented by one or more of the following means:

- ❖ Having machine passwords and not user VPN passwords.
- ❖ Installing non-exportable certificates on the mobile assets.
- ❖ Use of 3rd party software.

**SOE 4.7.d**

The policy must prevent users from connecting their own laptops and systems to the organization's network. How this is achieved must be explained in the policy.

**How this can be generated:**

The policy must be produced as a hard copy document.

**Details of pass or fail criteria:**

**SOE 4.7** The organization will be deemed to have 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 Remote Access Control Policy.

**Fail Criterion 2:**

Failure to incorporate the Remote Access Control Policy into the Security Policy required by **SOE 4.7.b**.

**Fail Criterion 3:**

Failure of the Remote Access Control Policy to mandate the remote access methods required at **SOE 4.7.c**.

**Fail Criterion 4:**

Failure of the Remote Access Control Policy to forbid remote network connections from users' personal laptops and PCs.

**Fail Criterion 5:**

Failure of the Remote Access Control Policy to explain how users are prevented from gaining remote access to the organization's network from their personal laptops and PCs.

## ***WiFi connecting to the LAN must use WPA***

**Statement of Evidence (SOE) Number:** SOE 4.8

**Overview:**

This is to check that the use of WPA is enforced on all wireless connections to the data LAN.

**Statement of Evidence (SOE) Description:**

**SOE 4.8.a.**

The organization must produce a wireless network configuration document.

**SOE 4.8.b.**

The wireless network configuration document must show that WPA or WPA2 is implemented between infrastructure and client connection.

**SOE 4.8.c.**

Where possible, this should be implemented via an infrastructure implementation i.e. using AES(CCMP) and not TKIP encryption. Exceptions to this will be the subject of a waiver from the certification body.

**SOE 4.8.d**

Where they are operated wirelessly, the following devices must be shown to be disconnected from the data LAN:

- ❖ Presentation Screen control devices.
- ❖ Presentation support devices that display data but do not cache or process it (media centres).
- ❖ Window/blind control systems.
- ❖ Streaming music/video systems where the whole system is totally separate from the main network.

**SOE 4.8.e**

The wireless network configuration document must show that Wireless Access Points are configured to refuse connections offering only Wired Equivalent Privacy (WEP) authentication.

**SOE 4.8.f**

Where passwords are used these must be longer than 12 characters. The wireless

administrator must produce a written statement that this is the case (including the minimum length of passwords in his area of responsibility) and that it will be maintained as such.

**How this can be generated:**

The wireless network configuration document must be produced as hard copy, network diagrams are useful, but not mandated providing the contents of the document clearly articulate all evidence requirements.

**Details of pass or fail criteria:**

**SOE 4.8** The organization will be deemed to have 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 wireless network configuration document.

**Fail Criterion 2:**

Failure of the wireless network configuration document to mandate the use of WPA or WPA2.

**Fail Criterion 3:**

Failure of the wireless network configuration document to mandate the use of AES instead of TKIP, or to produce an exemption certificate from the Certification Body.

**Fail Criterion 4:**

Failure of the wireless network configuration document to show that wireless control devices such as those in **SOE 4.8.d** are disconnected from the data network.

**Fail Criterion 5:**

Failure of the wireless network configuration document to show that devices offering only WEP authentication are forbidden to connect to the network.

**Fail Criterion 6:**

Failure to present the signed wireless administrators statement that the WLAN uses encryption with passwords that meet the requirement at SOE 4.8.



## LOGISTICS FOR A CDS LEVEL 4 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 4 audits.

### DURATION

A CDS Level 4 audit should take no longer than the following, depending upon the size of the organization:

Tiny – Small	-	2 day
Medium	-	2 days
Large	-	3 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; 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 checklist for those preparing for the audit. The following diagram shows the location of the various sections for the CDS Level 4 Audit.

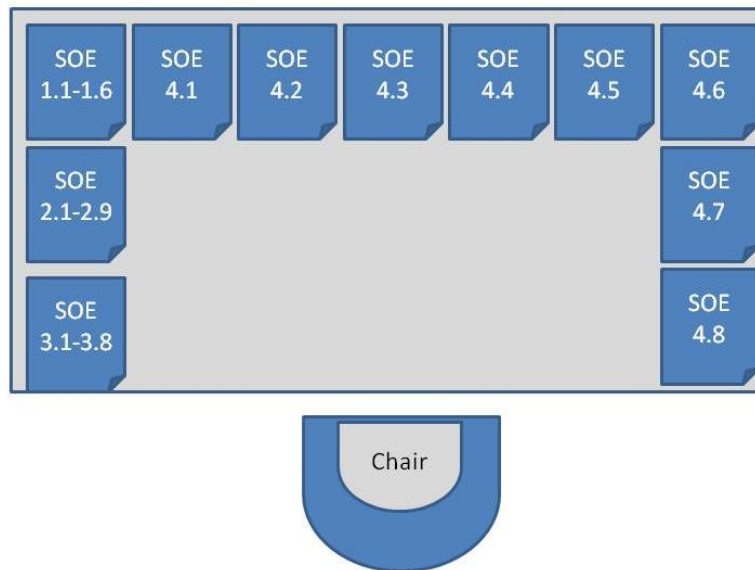


Figure 1 - CDS Level 4 SOE arrangement

Each collection of evidence generated to meet a particular SOE requires a cover sheet to allow the Auditor to see quickly 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 website<sup>4</sup> 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, which 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.

<sup>4</sup> [www.certifieddigitalsecurity.com](http://www.certifieddigitalsecurity.com)