



Certified Digital Security Level 3

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 (CDS) Level 3.



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 3.....	6
Part 3 CDS Audit Requirements	28
Logistics for a CDS Level 3 Audit.....	52





INTRODUCTION

The Certified Digital Security (CDS) Levels were designed to allow an organization's IT administrative and security staff 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: An organization that is aiming for level 3 will have already fully implemented all of the Level 1 and 2 requirements.

This level aims to continue building on the security procedures established in levels one and two whilst expanding the capabilities of support staff, establishing greater control of network assets and introducing physical and electronic security barriers.

Specifically, Level 3 requires the organization to have the following:

To have carried out a *Software Audit* that will assist legal compliance and identify unnecessary or unauthorised programs. Formal *Administrator Training* helps ensure that support activities are delivered correctly and from a position of knowledge rather than best intentions. The deployment of a *Stateful Firewall* provides security of enterprise links to the outside world.

Secure Disposal ensures that sensitive data does not leave the organization on redundant equipment, hence the importance of only allowing organization-owned assets on the LAN. A requirement to have a *Business Continuity and Disaster Recovery Plan* is introduced to provide organizational resilience to attack and disaster. *Physically Secure Servers* and *Data Stores* increase the protection of sensitive information. The *Removal of Private and External Assets* from the network, together with the requirement to *Prevent Unauthorized Remote Access or Email Portals* reduces the methods available to circumvent the physical security.

With Level 3 implemented, an organization can expect to see:

- ❖ Reduced risk of legal action as illegal software is purged.
- ❖ Reduced risk of a PR disaster through compromised client data on disposed assets.
- ❖ Your data is retained on your network.
- ❖ Increased uptime of systems as staff don't introduce viruses internally.
- ❖ Better skilled staff are more efficient.
- ❖ More dynamic firewall that reduces the exposure of the network.





PART 2

REQUIREMENTS FOR LEVEL 3





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 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 Board.

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

RECOGNITION OF SOURCE

The CDS Standard is 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 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 (eg all Part 1's 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 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 as SOE6.4.

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 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

Software Audit

Requirement Number: REQ 3.1

Overview:

A software audit should be conducted and the results analysed to ensure the organisation is not operating illegal software (either prohibited by law in the location they are operating or not licensed to the organization by the copyright owner). Furthermore, the organisation should ensure that the software provided to any user is only the software required for them to undertake their allocated functions.

Responsible Group or Users:

The management should mandate the conduct, and support the findings of, the software audit. The audit should be carried out by the system Administrators, or by an independent body assisted by the Administrators

Requirement Description:

To provide the organization with the confirmation that all software on their system is required and correctly licensed they should:

- ❖ Conduct an audit of all workstations and servers to identify the installed software.
- ❖ Remove any identified software not required for the business functions.
- ❖ Remove any software not owned or licensed to the organisation.
- ❖ Remove any 'dangerous' software such as:
 - Peer 2 Peer or Bit-torrent software.
 - Hacking tools.
 - Viruses, Trojans or general Malware.
 - Security tools (not provided by and for the administrator).
 - Out of date or obsolete software.
- ❖ Demonstrate that the audit has occurred by:
 - Presenting a log of the system on the organisation's LAN:
 - Log should indicate activity in last 6 months.
 - This should be undertaken by using software not manual checking.
 - Showing what prohibited software was identified and removed/purged/licensed/rectified.
 - Present evidence that management has understood the content and have endorsed the results of the audit and action plan.



Benefits of Implementation:

The organization gains visibility and control of the software installed and running on their system. Management and control of software reduces the chances of malware being introduced and prevents attack by the use of hacking tools. Liability for copyright or licence violations are also reduced.

Recurring? If so frequency:

After the initial audit, an update check should be undertaken quarterly.



Administrator Training

Requirement Number: REQ 3.2

Overview:

Administrator training ensures that those responsible for correct functioning of a system remain up to date with its correct operation. Similarly, Administrators should have an understanding of the security implications of their activities

Responsible Group or Users:

The management should mandate the undertaking of training to be carried out by the system Administrators. The Administrators should be encouraged to highlight training shortfalls.

Requirement Description:

To ensure that their system administrators are appropriately trained, the organization should ensure that among the administrators supporting the system between them have undertaken at least two of the following types of training course: *Network Configuration, Platform Configuration, Introductory Network Security, and Platform Specific Training*. Training should focus on the individuals remaining up to date with new technology and techniques, but the main emphasis must be on those technologies and systems in use within the organization.

A trained administrator can usually support up to 250 systems without significant stress and loading. Thus if an organisation has more than 250 systems, they should employ additional trained administrators to ensure the average number of systems per administrator is not more than 300. Each administrator should have complete training as indicated below:

Mandatory - two of the following (multiple courses from a group are permissible):

Network Configuration

This training is designed to ensure that the administrator has a fundamental understanding of how to install and manage (securely) network devices. The training should have covered the following:

- ❖ How to install devices on the LAN.
- ❖ How to optimise a device.
- ❖ How to control access across the LAN to a device.
- ❖ How to backup and store configuration files.
- ❖ How to audit the operational configuration of a device.
- ❖ How to securely manage the device remotely.
- ❖ The need and how to patch/update the devices.

Platform Configuration

This focuses upon the installation and configuration of Operating Systems (OS) and should provide the individual with the information on how to install, manage and support the OS. The training should have covered the following:

- ❖ How to install the operating system from a reliable source.
- ❖ How to optimise the operating system for performance.
- ❖ How to control access across the LAN to the platform.
- ❖ How to backup and store configuration files (securely).
- ❖ How to audit the running configuration of a device.
- ❖ How to securely manage a device remotely.
- ❖ How to add and manage users, including:
 - The type of users they should add (eg temporary, power or root level).
 - How to limit their access (permissions and profiles).
 - How to control the times of 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.

Introductory Network Security

This course will allow the administrator to become more aware of the effort required to protect IT Systems. The course should explain the common weaknesses in aspects of modern computing. With this knowledge the individual can help shape future purchases of equipment and new policy or procedures. The 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 across the LAN to data/information.
- ❖ 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 to aid identification of common configuration and security issues.
- ❖ How to report these identified issues.
- ❖ How to record and describe the severity of the issue.
- ❖ Impact of corrective action.
- ❖ 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.
 - Awareness of other technologies that can be introduced for increased security.

This should be a high level introduction to:

- Intrusion Detection Systems (IDS).
- Intrusion Prevention Systems (IPS).
- Firewalls.
- Threat Management tools.
- Wireless Attack Detection Systems.
- Rogue Access Point Detection Systems.
- Network Access Control.
- Anti Virus (Enterprise Management).
- Host Based IDS.
- Secure Web & Mail Proxy Devices.
- Multifactor Authentication.
- Encryption.

❖ Courses known to have met the criteria:

- SANS 401 – Security Essentials Course.
- See the CDS Website for further training courses known to meet this requirement.

Platform Specific Training

This training written by a vendor or manufacturer of an item of equipment to allow the subject to install and maintain that specific device. The applicable training for each device should include:

❖ Router Configuration; covering the following:

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

❖ Firewall or Security Appliance Configuration; covering the following:

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

❖ The Wireless Device Configuration; covering the following:

- How to install the device.
- How to optimise the power of the device for the environment.
- How to control access across the LAN to the device.

- How to backup and store configuration files.
- How to implement the Security on the device.
- How to implement WPA and WPA2.
- The fact that Infrastructure or Enterprise (RADIUS) is preferred over Personal WPA, and how to implement it. NOTE: WEP is not approved under CDS.
- How to audit the running configuration of the device.
- How to securely manage the device remotely.

Optional Skills

The following skills are optional for compliance with this CDS Standard level, however, their addition to the organization will add considerably to their ability to examine their own security with a view to addressing the items identified. Assuming that all wireless has a minimum of WPA implemented, the *Vulnerability Analysis* is recommended first, then *Wireless Security* and finally *Penetration Testing*.

Vulnerability Analysis

- ❖ This course should have covered:
 - Legal Aspects of testing.
 - Planning and Scoping the Testing.
 - Engaging with the customer/client.
 - The stages of the Testing.
 - The equipment and 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 organisation and the tester).
 - How to report the findings.
 - What to do to validate the report/findings.
- ❖ The course should have the student undertake hands on elements for the following as a minimum:
 - Information Gathering.
 - Scanning systems.
 - Mapping networks.
 - Identifying targets and running software.
 - Auditing password length and complexity.
 - How to rate findings in terms of criticality.
 - How to report findings to the organization.
 - The importance of logging while testing the system.
- ❖ Courses known to have met the criteria:
 - SANS 504 - Hacker Techniques, Exploits & Incident Handling Course.
 - See the CDS Website for further training courses known to meet this requirement.

Wireless Security

- ❖ This course should have covered:
 - The Threat from using Wireless technologies.
 - Wave propagation and signal strength.
 - Sniffing Wireless networks.
 - Auditing WLANs for compliance and Rogue Access Points.
 - The Security of WEP, WPA, LEAP, WIMAX.
 - Bluetooth Vulnerabilities.
 - Wireless Segmentation on the main LAN.
- ❖ Qualifying Courses include:
 - SANS 617 - Wireless Ethical Hacking, Penetration Testing, and Defenses Course.
 - SANS 559 - Wireless Security Exposed Course.
 - See the CDS Website for further training courses known to meet this requirement.

Penetration Testing

- ❖ This course should have covered:
 - Legal Aspects associated with testing in the location and over borders.
 - Planning and Scoping the Testing.
 - Engaging with the customer/client.
 - The stages of the Testing.
 - The equipment and 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 organisation and the tester).
 - How to report the findings.
 - What to do to validate the report/findings.
 - The course should demonstrate the core tools that are available to testers – open and closed source.
- ❖ The course should have the student undertake hands on elements for the following as a minimum:
 - Information Gathering.
 - Sniffing Ethernet packets.
 - Scanning systems.
 - Mapping networks.
 - Identifying targets and running software.
 - Using exploits to gain access to a system.
 - Gaining access to stored passwords.
 - Cracking passwords.
 - How to gain access to a system.
 - How to retain access to a system.
 - How to report findings.
 - The importance of logging.

- ❖ Courses known to have met the criteria:
 - SANS 560 - Network Penetration Testing and Ethical Hacking Course.
 - See the CDS Website for further training courses known to meet this requirement.

Benefits of Implementation:

The organization gains an increased level of skill in those personnel responsible for the configuration, control and management of their IT systems. This increased level of skill will translate directly into the delivery of optimised security measures and an ability to defend a system against electronic attack.

Recurring? If so frequency:

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

Note:

SANS Training has been readily identified in this CDS level because it is known by the authors to be of a high standard and internationally available. The CDS Website will build upon this starting list and will include additional courses that have syllabus that provide the required training.

If the course your administrator's have undertaken is not listed, please send the details of the course, its syllabus and provider to audit@certifieddigitalsecurity.com and the CDS staff will review the information and if appropriate will add the course to the list of approved courses.

The list on the website will be reviewed at least annually and updates will include new courses to be added to the list and those that are deprecated. A deprecated course will have a change date that indicates when the syllabus was no longer deemed to meet the requirements. Staff that have attended and passed the course between the added and deprecated dates will be deemed to have been trained to the required level. Those trained after the course changed and was deprecated will not be deemed to have been trained to the correct level.

Implement a Stateful Firewall

Requirement Number: REQ 3.3

Overview:

A Stateful Firewall helps to prevent unwanted or unknown network traffic being able to gain access into the organization's CIS systems by recording outbound traffic and only allowing return traffic on the basis of the outbound request.

Responsible Group or Users:

System Administrators, or a qualified 3rd party on their behalf, should install and configure the firewall in accordance with its operating parameters and the requirements of this Standard. System Administrators are to ensure that the Firewall logs are regularly inspected.

Requirement Description:

To provide the organization with protection from network based attack, it needs to install a firewall capable of Stateful packet inspection. The firewall must operate at Open Systems Interconnection (OSI) Reference Model Layer 3 and should be able to:

- ❖ Track the internal outbound request.
- ❖ Allow the returning response to this request and allow it based upon information in its state table.
- ❖ Deny a connection to a timed out or dynamically closed connection.
- ❖ Block access from IP addresses to dynamically opened ports that are not available to that address (ie the state table entry does not match).
- ❖ Only allow connections for which there is a rule.

Benefits of Implementation:

Successful external network-based attacks are significantly reduced, with only the more sophisticated ones having a chance of success.

Recurring? If so frequency:

Firewall accounting logs should be examined for signs of unusual or suspicious activity at least monthly by the Administrators.

Secure Disposal

Requirement Number: REQ 3.4

Overview:

The organisation should implement a secure disposal policy to ensure that no digital media is discarded intact. In this context intact means that a human or computer could read the data using tools or forensic software.

Responsible Group or Users:

Building on the Level 1 Asset Disposal Policy, senior management should ensure that secure disposal is included in the Policy and that their chosen media destruction method is consistently used.

All users of media should adhere to the stated policy and ensure media is disposed of in accordance with it.

Requirement Description:

To ensure that all media is disposed of correctly and consistently, the organization must ensure the following:

- ❖ Ensure items are tracked when sent for disposal.
- ❖ Ensure that logs are retained that can be searched to find items that are later 'found'.
- ❖ Destroy Hard Disk Drive (HDD) data by either:
 - Conducting a full and complete wipe of the drive.
 - Destroying the HDD itself by shredding or melting.
 - Degaussing the HDD.
 - Damaging the HDD sufficiently to render the HDD inoperative.

See the CDS website for details of how to correctly wipe a HDD with software tools, and for the list of approved disposal standards and products.

Benefits of Implementation:

With an effective Secure Disposal process the likelihood of data compromise is reduced which in turn reduces the potential for damaging or embarrassing newspaper headlines or the loss of commercially or personally sensitive information. This in turn reduces the chances of costly or damaging legal action being taken against the organization.

Recurring? If so frequency:

This policy should be reviewed annually by the organization or their nominated representative. The process should be endorsed by the Senior Management and appropriate funding allocated to it.

Business Continuity & Disaster Recovery Plan

Requirement Number: REQ 3.5

Overview:

The organization must have a documented Business Continuity and Disaster Recovery Plan.

Responsible Group or Users:

The Business Continuity and Disaster Recovery Plan should be developed by a nominated individual within the organization. It should be endorsed by the owner or manager of the organization and should be made available to all users of the system or employees.

Requirement Description:

To provide the organization with the clarity and legal protection it needs, this policy must include or address the following items:

- ❖ The organisation must have a Business Continuity and Disaster Recovery Plan (BC & DRP). This plan should include technical aspects, personnel and facilities to ensure that the business can continue to operate in the face of outages and incidents and that it is capable of surviving a major incident.
- ❖ This plan should:
 - Include systems, facilities and people.
 - Identify the critical people and assets in the organisation.
 - Identify the critical aspects of the business (see REQ 3.6).
 - Include a high level overview and some detailed steps to take following an incident.
 - Cover physical, technical and human based incidents.
- ❖ The plan must be supported by management (ie written endorsement).
- ❖ See the website for details of templates and internet resources that can be of assistance.

Benefits of Implementation:

The organization will be able to respond quickly and effectively to incidents which jeopardise their business activity and facilitate an efficient return to normal operations.

Recurring? If so frequency:

This policy should be reviewed annually by the organization or their nominated representative. The policy should be endorsed by the Senior Management at each significant revision. A review should also take place following a significant change in the organization's structure, business output or following an incident resulting in the plan being put into action.

Physically Secure Servers & Data Stores

Requirement Number: REQ 3.6

Overview:

Servers and data stores must be protected from unauthorized physical access or attack.

Responsible Group or Users:

The System Administrators, with sanction and support from senior management within the organization, should physically isolate servers and data stores, and control access to them. Any outsourced facilities should meet the standards laid down in this requirement.

Requirement Description:

To provide the necessary degree of physical security the organization must address the following items:

- ❖ Physical access to servers must be controlled and limited to only the named staff with a need to access, visit or work in their location.
- ❖ Only named administrators are to have routine access to servers.
- ❖ Security staff may have access to conduct reviews, log analysis or incident response activities.
- ❖ Other staff are only to have access in emergency.
- ❖ All visitors to the server room/area/cabinet are to be logged together with their access times and purpose of visit.
- ❖ These logs are to be retained for at least one year.
- ❖ Notes:
 - If seeking CDS certification, then these will need to be presented to cover the time from application to the date of the initial inspection.
 - For subsequent inspections these must show (at least) access logs dating back to the date of the previous inspection.
 - The physical access to servers is to be controlled but this is to be proportionate to the size of the organisation.
 - Small organisations may only be able to provide a locked cabinet or cupboard.
 - Medium sized organisations may have separate server rooms; access to the room and server is to be controlled.
 - Large organisations' server rooms must be controlled access and, where sensitive data is stored, access to those racks housing the data store is to be controlled.

- Where server facilities are shared then the servers are to be in lockable cabinets.
- Care is to be taken to ensure that panels are not left insecure and that inter-rack panelling is installed.
- ❖ Data stores must also be secured to a similar level as the servers. Data stores include:
 - Online Just a Bunch of Drives (JBOD) stores.
 - Online Network Attached Storage (NAS).
 - Online Storage Area Networks (SANs).
 - Offline backup devices and media (Hard Drives, DVD or CD stores etc).
 - Offline backup tapes.
- ❖ Online data must be physically secure (see servers).
- ❖ Data stores must be protected from theft as well as covert copying.
- ❖ Data stores (especially backups) must be protected from poor environmental conditions.
- ❖ Backups must be conveyed to, and stored in, appropriate containers and locations to prevent damage from:
 - Dust.
 - Dirt.
 - Smoke.
 - Strong Electromagnetic Fields.
 - Strong Magnetic Fields.
- ❖ The following requirements apply to all physical aspects of the system, servers, backup devices, backup media and any other aspect of the system that is held under lock & key or combination locks:
 - All lockable units must be routinely locked.
 - Locks must be used where they are provided.
 - Spare keys must be correctly secured with details of who can request use of the spare keys recorded in a register.
 - Spare keys should be swapped for the in-use keys every 6 months to prevent uneven wear in the keyset. The swap should be recorded within the key register
 - Combinations must be:
 - Changed regularly (at least annually) and when any member of staff that knew the combination no longer has a need to know it or leaves the organisation.
 - Stored in a safe location and/or stored in a fireproof safe to prevent loss through fire.
 - Written down and sealed in an envelope by the person that sets the combination at the time they set the combination.
 - Records must be maintained of sealed combination envelopes, including who is allowed to open the envelope and the date of the last change.
 - The organization's Disaster Recovery or Business Continuity Plan must take into account accessing stored combinations and keys.



Benefits of Implementation:

Physical security reduces the opportunities for technical and non-technical attack, theft or damage, and limits the chances of staff having unnecessary access to data.

Recurring? If so frequency:

The security measures should be reviewed annually by the organization or their nominated representative. The review should ensure that changes of keys and combinations are being undertaken in the required time frames. A review should also take place following an incident resulting from a breach of any of the measures contained in this requirement.



Control of LAN Assets

Requirement Number: REQ 3.7

Overview:

Personal or non-organizationally owned assets are not permitted to connect to the LAN or any part of the system.

Responsible Group or Users:

The System Administrators, with sanction and support from senior management within the organization, should configure LAN policies to prevent unauthorised connection of external equipment.

Requirement Description:

- ❖ The organization must prevent personal or non-organizationally owned assets from being able to connect to the corporate LAN. This could be achieved by:
 - Physically locking or sealing ports.
 - Disabling external ports (e.g. switching off USB).
 - Using Group Policy Objects.
- ❖ If it is deemed essential that visitors (contractors or clients) must have access to IT services, then a separate guest LAN should be implemented in the following manner:
 - The Guest LAN can only connect to shared guest assets (e.g. file server, printers).
 - The guest assets must be protected and monitored (e.g. behind a firewall controlled by passwords and have physical access protection).
 - The Guest LAN should be cabled separately to the visitor's desktop.
 - A separate connection to the internet can be provided for visitors working in the organisation (eg contractors).
 - The Guest LAN can be provided via wireless, but it should be low-powered and only in the areas necessary.
 - If the organisation's assets connect to the guest LAN they must use a Virtual Private Network (VPN) to connect back to the organisation.
- ❖ Internet Conference software eg WebEx may be permitted where a clear policy on its use is written and issued to staff with the business need to use the facility.

Benefits of Implementation:

Reduced risk of non-corporate assets being used to introduce viruses, other malicious code, or unlicensed software resulting in a more stable and reliable system and increased uptime. Reduced risk of unauthorised removal of data, improving data security and reducing risk of litigation under data protection legislation.



Recurring? If so frequency:

The security measures should be reviewed annually by the organization or their nominated representative. A review should also take place following an incident resulting from a breach of any of the measures contained in this requirement.



Remove Remote Portals

Requirement Number: REQ 3.8

Overview:

The organizations data can be easily migrated off the system if remote access and control it permitted to locations that are untrusted and outside the LAN. This does not prevent remote administration where this is defined and endorsed by management.

Responsible Group or Users:

The System Administrators, with sanction and support from senior management within the organization, should configure LAN policies to prevent unauthorised connection to or from external portals.

Requirement Description:

To prevent data migration from the organization's systems, the use of remote email and remote system access (except via an approved VPN link) must be disabled. The following technologies are prohibited from this level upwards:

- ❖ LogMeIn.
- ❖ Outlook Web Access (OWA).
- ❖ PCAnyWhere.
- ❖ Externally Accessible VNC.
- ❖ Non encrypted Remote Desktop (RDP).
- ❖ Windows Remote Assistance.

Internet Conference software eg WebEx may be permitted where a clear policy on its use is written and issued to staff with the business need to use the facility.

Where remote support is required (ie contracted remote engineers access the internal LAN via a encrypted link to correct or address issues) the following should be recorded in the Systems Security Policy:

- ❖ The organization that requires the remote access.
- ❖ The reason for the remote access.
- ❖ The IP, port and protocol to enter the LAN (for firewall configuration reasons).
- ❖ The authority the 'visitors' on the LAN have and when.
- ❖ The checks that have been conducted on the remote 'visitors' organization (eg are they certified under CDS (ideally they should be at least level 3 to gain remote access))



Benefits of Implementation:

By blocking remote portals and remote access into the network from uncontrolled endpoints, the organization prevents data from being moved onto hardware and systems that are not secure or are not under their control. This prevents data loss and also prevents the import of hacking tools, malware and other undesirable software or programs.

Recurring? If so frequency:

The security measures should be reviewed annually by the organization or their nominated representative. A review should also take place following an incident resulting from a breach of any of the measures contained in this requirement.





PART 3

CDS AUDIT REQUIREMENTS





ABOUT THIS PART

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

IF SEEKING AN AUDIT

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

RECOMMENDED PROCESS

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

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



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

THE AUDIT PROCESS

ABOUT THE PROCESS

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

TIME IS MONEY...

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

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

NO HANDS ON!

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

LOWER LEVELS ARE INCLUDED TOO

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

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

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



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

or

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

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

ON THE DAY OF AUDIT

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

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

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

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

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

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

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

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





IF THE EVIDENCE IS NOT CORRECT OR IS INCOMPLETE

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

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

HOW REQUIREMENTS ARE MET

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

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

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

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

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

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

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

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

1. The Statement of Evidence (SOE) title.
2. The related requirement title (or short name) - if different from SOE title.
3. Its unique requirement number.
4. A short overview of what the requirement is designed to achieve or introduce.
5. The details of the evidence required (the numbers, percentages or other details relating to the quality and type of evidence needed). This can be further broken down and may link to the CDS website for current information.
6. The list detailing how the evidence can be generated.
7. The details of the pass/fail Criterion – if known.
8. Any notes relevant to the SOE.



Software Audit

Statement of Evidence (SOE) Number: SOE 3.1

Overview:

This audit requirement is to ensure that a software audit has been conducted and the results analysed to ensure the organisation is not operating illegal software (either prohibited by law in the location they are operating or not licensed to the organization by the copyright owner). The organisation must show that the software provided to any user is only the software required for them to undertake their allocated functions.

Statement of Evidence (SOE) Description:

SOE 3.1.a

The organization must produce a software audit report.

The report must include the following:

SOE 3.1.b

Audit details of all software installed on all servers.

SOE 3.1.c

Audit details of all software installed on all workstations.

SOE 3.1.d

A log of the system on the organisation's LAN. The Log must indicate activity in last 6 months.

SOE 3.1.e

The audit report must be generated by a software audit tool.

SOE 3.1.f

The audit report must include or be accompanied by a list of all software licences held for the software on all servers and workstations.

SOE 3.1.g

The audit report must include or be accompanied by a list of all software that is unlicensed or included on the 'dangerous' software list (See REQ 3.1) and has been removed from the system or licensed, where appropriate.

SOE 3.1.h

The audit report must include or be accompanied by a statement of necessity endorsed by senior management within the organization to the effect that all software on users'

workstations is required for the conduct of their role.

SOE 3.1.i

The audit report must contain a comments section for senior management to note their endorsement of the audit. The endorsement must be signed by the endorsing manager.

SOE 3.1.j

The organization must provide a list of all Servers and Workstations within their enterprise.

How this can be generated:

Hard copy printed output from the audit tool. Separate sections can be provided for management comment and signature, lists of software licences, lists of removed software, and the statement of necessity, but they must clearly reference the specific output forming the body of the audit report.

The list of Servers and Workstations must be produced independently from the output of the audit tool.

Details of the pass or fail criteria for SOE 3.1

Fail Criterion 1:

The organization fails to produce an audit report.

Fail Criterion 2:

The audit report does not detail software installed on all servers.

Fail Criterion 3:

The audit report does not detail software installed on all Workstations.

Fail Criterion 4:

The organization fails to produce a log of the system on the organisation's LAN indicating activity in last 6 months.

Fail Criterion 5:

The audit report is not generated by a software audit tool.

Fail Criterion 6:

The organization does not provide a list of all software licences held for the software on all servers and workstations.

Fail Criterion 7:

The organization does not provide a list of all software that is unlicensed or included on the



'dangerous' software list (See REQ 3.1) and has been removed from the system or licensed, where appropriate.

Fail Criterion 8:

Examination of the presented evidence shows unlicensed software is still present on the system.

Fail Criterion 9:

The organization does not provide a statement of necessity endorsed by senior management within the organization.

Fail Criterion 10:

The audit report does not contain a comments section for senior management to note their endorsement of the audit.

Fail Criterion 11:

The audit endorsement is not signed by the endorsing manager.



Administrator Training

Statement of Evidence (SOE) Number: SOE 3.2

Overview:

This audit requirement is to ensure that system Administrators have received formal training to a standard acceptable to CDS.

Statement of Evidence (SOE) Description:

SOE 3.2.a

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

SOE 3.2.b

The organization's statement must show that the optional elements (Vulnerability Analysis, Wireless Security and Penetration Testing (See **REQ 3.2**)) of the CDS training requirements form part of their administrator development plans.

SOE 3.2.c

The organization must produce a list of names of all their system administrators.

SOE 3.2.d

The organization must produce details of the training undertaken by their system administrators, including administrators' names, training dates, venues and training providers.

SOE 3.2.e

Provided training must include the mandatory elements of two of the following courses: (Note: see REQ 3.2 for full details of the syllabus required, the heading are listed here for brevity).

- ❖ Network Configuration.
- ❖ Platform Configuration.
- ❖ Introductory Network Security.
- ❖ Platform Specific Training.
 - Router Configuration.
 - Firewall or Security Appliance Configuration.
 - Wireless Device Configuration.

SOE 3.2.f

The organization must produce the certificates and qualifications held by their administrators which support the requirements of **SOE 3.2.b** and **SOE 3.2.d**.

SOE 3.2.g

Certificates and qualifications presented under **SOE 3.2.f** must be in-date.

SOE 3.2.h

The organization must produce copies of the syllabi of all training courses undertaken to support the requirements of **SOE 3.2.b**, **SOE 3.2.d** and **SOE 3.2.f**.

SOE 3.2.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 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 photocopies in accordance with **REQ 2.1**.

To be valid, course syllabi presented under **SOE 3.2.h** must be those produced by the training provider of the course in question.

Details of the pass or fail criteria for SOE 3.2

Fail Criterion 1:

The organization fails to produce a training policy statement for system administrators.

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 administrators' names.



Fail Criterion 4:

The organization does not produce records of training undertaken by administrators.

Fail Criterion 5:

The training provided to administrators does not include the mandatory courses detailed in **SOE 3.2.e**.

Fail Criterion 6:

The organization fails to produce the certificates and qualifications held by their administrators which support the requirements of **SOE 3.2.b** and **SOE 3.2.d**

Fail Criterion 7:

Certificates and qualifications presented under **SOE 3.2.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 3.2.b**, **SOE 3.2.d** and **SOE 3.2.f**.

Fail Criterion 9:

The syllabus evidence in **SOE 3.2.h** fails to cover 2 or more elements of any one of the mandatory training courses detailed in **SOE 3.2.e**.



Implement a Stateful Firewall

Statement of Evidence (SOE) Number: SOE 3.3

Overview:

This audit requirement is to ensure that Network assets are protected from external attack by a good firewall.

Statement of Evidence (SOE) Description:

SOE 3.3.a

The organization must assert in writing, endorsed by the management representative responsible for network services, that their external connections are only provided via a stateful firewall.

SOE 3.3.b

The senior network administrator must certify, in writing, that the following statements are correct:

- ❖ The firewall operates at at least Open Systems Interconnection (OSI) Reference Model Layer 3.
- ❖ The firewall tracks an internal outbound request.
- ❖ Inbound responses are allowed based on an initial outbound request recorded in the firewall's state table.
- ❖ The firewall will deny a connection to a timed out or dynamically closed connection.
- ❖ The firewall will block access from IP addresses to dynamically opened ports that are not available to that address (ie the state table entry does not match).
- ❖ The firewall will only allow connections for which there is a rule.
- ❖ Firewall accounting logs are enabled and audited for unusual or malicious activity.

SOE 3.3.c

The organization must provide a written policy, endorsed by senior management, that firewall accounting logs are audited at least monthly.

How this can be generated:

Written statements and policies signed by the appropriate representative will be acceptable for all evidential requirements.



Details of the pass or fail criteria for SOE 3.3

Fail Criterion 1:

The organization fails to assert that it utilizes a Stateful Firewall.

Fail Criterion 2:

The Senior Network Administrator fails to provide written confirmation of the statements in **SOE 3.3.b**.

Fail Criterion 3:

Any of the statements in **SOE 3.3.b** are missing from the confirmation statement.

Fail Criterion 4:

The organization fails to produce a policy statement that firewall logs are to be audited at least monthly.



Secure Disposal

Statement of Evidence (SOE) Number: SOE 3.4

Overview:

This audit requirement is to ensure that the organization has a written and management endorsed policy on the secure disposal of all media which is known to all members of staff responsible for management and disposal of network assets.

Statement of Evidence (SOE) Description:

SOE 3.4.a

The organization must provide a written policy for asset disposal, which includes their means of securely disposing of all media. Disposal methods must conform to the CDS acceptable methods.

SOE 3.4.b

The organization must provide their media or asset register to show that media is correctly accounted for prior to disposal.

SOE 3.4.c

The organization must provide their records of media that has been securely disposed of. The secure disposal of media may be recorded in the asset register in organizations where their size prevents them managing separate registers; however, the requirements of **SOE 3.4.d** must be met.

SOE 3.4.d

The organization's records must provide the following information:

- ❖ Unique identifier of the asset.
- ❖ Date of disposal.
- ❖ Method of disposal.
- ❖ Name and signature of the person responsible for disposal of the asset.

How this can be generated:

Written policies signed by the appropriate management representative. Registers of disposal can be either certificate based (i.e. a sheet containing the information required by **SOE 3.4.d** and signed by the person responsible for the disposal) or be a contiguous register such as a book. Where an online register is maintained, printed output covering the previous 12 months is required (or the lifetime of the register if this is shorter) must be presented with a signed declaration that the output is an accurate reflection of the online register.

Details of the pass or fail criteria for SOE 3.4

Fail Criterion 1:

The organization fails to provide a management endorsed written policy on the secure disposal of all removable media.

Fail Criterion 2:

The organization fails to provide a management endorsed written policy on the secure disposal of all server and workstation Hard Disk Drives.

Fail Criterion 3:

The organization fails to provide their media and / or asset register.

Fail Criterion 4:

The organization fails to produce their records of secure disposal of all media.

Fail Criterion 5:

Assets identified as being securely disposed of in the asset or media register do not have a corresponding disposal certificate, or entry in the secure disposal register.

Fail Criterion 6:

The disposal certificate or register does not contain the details required by **SOE 3.4.d**.

Business Continuity & Disaster Recovery Plan

Statement of Evidence (SOE) Number: SOE 3.5

Overview:

This audit requirement is to ensure that the organization has a written and management endorsed policy on the secure disposal of all media which is known to all members of staff responsible for management and disposal of network assets.

Statement of Evidence (SOE) Description:

SOE 3.5.a

The organisation must have a Business Continuity and Disaster Recovery Plan (BC & DRP) signed by senior management.

SOE 3.5.b

The BC & DR Plan must:

- ❖ Include systems, facilities and people.
- ❖ Identify the critical people in the organisation.
- ❖ Identify the critical assets in the organisation.
- ❖ Identify the critical aspects of the business (see **SOE 3.6**).
- ❖ Include a high level overview.
- ❖ Include some detailed steps to take following an incident.;
- ❖ Cover physical, technical and human based incidents.

SOE 3.5.c

Where they are used, emergency access to combinations, passwords and off-site data stores must be included in the BC & DRP.

SOE 3.5.d

The BC & DRP must have been produced or reviewed and re-endorsed by senior management within the previous 12 months.

How this can be generated:

Hard copy output of written policies signed by senior management.

Details of the pass or fail criteria for SOE 3.5

Fail Criterion 1:

The organization fails to provide a management endorsed written BC & DRP.

Fail Criterion 2:



The organization's BC & DRP does not contain the elements of **SOE 3.5.b**.

Fail Criterion 3:

The organization's BC & DRP has not been reviewed for more than 12 months.

Fail Criterion 4:

The organization's BC & DRP has been reviewed in the last 12 months but has not been endorsed by senior management.



Physically Secure Servers & Data Stores

Statement of Evidence (SOE) Number: SOE 3.6

Overview:

This audit requirement is to ensure that the organization has taken steps to provide a practical level of physical security to protect its servers and data stores.

Statement of Evidence (SOE) Description:

SOE 3.6.a

The organization must provide written policy, endorsed by senior management, relating to physical security of and access control to servers and data stores.

The policy must include the elements of **SOE 3.6.b – SOE 3.6.p**:

SOE 3.6.b

Only named administrators are to have routine access to servers.

SOE 3.6.c

Security staff may have access to conduct reviews, log analysis or incident response activities.

SOE 3.6.d

Other staffs are only to have access in an emergency.

SOE 3.6.e

All visitors to the server room/area/cabinet are to be logged together with their access times and purpose of visit. Logs are to be retained for at least one year.

SOE 3.6.f

Data stores must also be secured to a similar level as the servers. Data stores include:

- ❖ Online Just a Bunch of Drives (JBOD) stores.
- ❖ Online Network Attached Storage (NAS).
- ❖ Online Storage Area Networks (SANs).
- ❖ Offline backup devices and media (Hard Drives, DVD or CD stores etc).
- ❖ Offline backup tapes.

SOE 3.6.g

Backups must be conveyed to, and stored in, appropriate containers and locations to prevent damage from:

- ❖ Dust.
- ❖ Dirt.

- ❖ Smoke.
- ❖ Strong Magnetic and Electromagnetic Fields.

SOE 3.6.h

Data stores (especially backups) must be protected from poor environmental conditions.

SOE 3.6.i

Online data must be physically secured to the same standard as the servers

SOE 3.6.j

Data stores must be protected from theft as well as covert copying.

SOE 3.6.k

Physical access to servers must be controlled as a minimum in accordance with table 1 below:

Size of Organization	Control Measure
Small	Locked cabinet or cupboard
Medium	Separate room with access control to room and servers. Criteria for small organization may still apply.
Large	Server rooms with controlled access. Where sensitive data is stored, access to those racks housing the data store is to be controlled. Servers in shared facilities must be in locked cabinets within the server room.

SOE 3.6.l

All lockable rooms and cabinets housing servers or data storage must be routinely locked.

SOE 3.6.m

Spare keys must be correctly secured with details of who can request use of the spare keys recorded in a register.

SOE 3.6.n

Spare keys should be swapped for the in-use keys every 6 months to prevent uneven wear in the keyset. The swap should be recorded within the key register

SOE 3.6.o

Where used, combinations must be:

- ❖ Changed regularly (at least annually) and when any member of staff that knew the combination no longer has a need to know it or leaves the organisation.
- ❖ Stored in a safe location and/or stored in a fireproof safe to prevent loss through fire.
- ❖ Written down and sealed in an envelope by the person that sets the combination at the time they set the combination.

SOE 3.6.p

Records must be maintained of sealed combination envelopes, including who is allowed to open the envelope and the date of the last change.

SOE 3.6.q

Server room visitor logs must be presented. They must cover the period from the date the organization applied for CDS certification, or date of last audit, to the time of the current audit

How this can be generated:

Hard copy output of written policies signed by senior management.

A photocopy of the server room and / or data store visitors log. The log is to be signed by the network manager as being a true copy of the original.

Details of the pass or fail criteria for SOE 3.6

Fail Criterion 1:

The organization fails to provide a management endorsed written policy covering physical security of servers and data stores.

Fail Criterion 2:

The organization's physical security policy does not contain the elements of **SOE 3.6.b – SOE 3.6.p**.

Fail Criterion 3:

The organization's physical security policy is missing 2 or more elements of **SOE 3.6.b – SOE 3.6.p**.

Fail Criterion 4:

The organization fails to provide a copy of the secure room and / or data store visitors log.

Control of LAN Assets

Statement of Evidence (SOE) Number: SOE 3.7

Overview:

This audit requirement is to ensure that the organization has a written and management endorsed policy on controlling personal equipment and non-owned assets connecting to their network.

Statement of Evidence (SOE) Description:

SOE 3.7.a

The organization must have a management-endorsed policy covering the prohibition of personal or non-organizationally owned assets being allowed to connect to the corporate LAN.

SOE 3.7.b

The policy must state what method is used to prevent unauthorised connections, such as:

- ❖ Physically locking or sealing ports.
- ❖ Disabling external ports (e.g. switching off USB).
- ❖ Using Group Policy Objects.

SOE 3.7.c

The policy must state that the use of remote email and remote system access (except via an approved VPN link) has been disabled.

SOE 3.7.d

The policy must include a statement on visitor access to IT services.

SOE 3.7.e

Where permitted in the policy, visitor access to IT services must be clearly stated as being via a separate guest LAN.

SOE 3.7.f

The organization must provide written confirmation, signed by the network manager that the guest LAN meets the following conditions:

- ❖ The Guest LAN can only connect to shared guest assets (e.g. file server, printers).
- ❖ The guest assets are protected and monitored (e.g. behind a firewall controlled by passwords and have physical access protection).
- ❖ The Guest LAN is either cabled separately to the visitor's desktop, or via wireless, which is low-powered and only available in the areas necessary for visitor working.
- ❖ A separate connection to the internet is provided for visitors working in the organisation

(eg contractors).

- ❖ If the organization's assets connect to the guest LAN they are using a Virtual Private Network (VPN) to connect back to the organization.

SOE 3.7.g

The organization must provide a high level network architecture diagram showing that corporate and guest LAN services are clearly separated.

SOE 3.7.h

Internet Conference software (eg WebEx), where used must have a clear statement on its use in the policy, and must be signed as having been read by all staff with the business need to use the facility.

How this can be generated:

Hard copy output of written policies signed by a senior management representative.

Details of the pass or fail criteria for SOE 3.7

Fail Criterion 1:

The organization fails to provide a management endorsed written policy on the control of LAN assets.

Fail Criterion 2:

The policy does not include the elements of **SOE 3.7.b – SOE 3.7.e** and **SOE 3.7.h**.

Fail Criterion 3:

The organization fails to provide written confirmation, signed by the network manager that the guest LAN meets the conditions of **SOE 3.7.f**.

Fail Criterion 4:

The organization fails to produce a high level diagram of the architecture.

Fail Criterion 5:

The organization's high level architecture diagram does not show a separation between corporate and guest LAN Assets.

Remove Remote Portals

Statement of Evidence (SOE) Number: SOE 3.8

Overview:

This audit requirement is to ensure that the organization has a removed or has a policy to allow a remote portal (or support VPN).

Statement of Evidence (SOE) Description:

SOE 3.8.a

The organization must have a management-endorsed policy covering the prohibition of portals and portal software on the LAN.

SOE 3.8.b

The policy must state that the use of remote email and remote system access (except via an approved VPN link) has been disabled.

SOE 3.8.c

The policy must explicitly prohibit the following technologies:

- ❖ LogMeIn.
- ❖ Outlook Web Access (OWA).
- ❖ PCAnyWhere.
- ❖ Externally Accessible VNC.
- ❖ Non encrypted Remote Desktop (RDP).
- ❖ Windows Remote Assistance.

SOE 3.8.d

Internet Conference software (eg WebEx), where used must have a clear statement on its use in the policy, and must be signed as having been read by all staff with the business need to use the facility.

SOE 3.8.e

The organization must present their inbound firewall rules to demonstrate that any portal or remote access software operated internally is not accessible from outside the LAN.

How this can be generated:

Hard copy output of written policies signed by a senior management representative.

The software report is required for **SOE 3.1.b** and **SOE 3.1.c** so can be represented for **SOE 3.8.c**.



The exclusions and remote support will be part of the management policy.

The firewall rules can be exported or screen shots provided of the interface (if a web management console).

Details of the pass or fail criteria for SOE 3.8

Fail Criterion 1:

The organization fails to provide a management endorsed written policy on the control of Remote Portals assets.

Fail Criterion 2:

The policy does not include the elements of **SOE 3.8.b – SOE 3.8.c** and **SOE 3.8.d** if internet or externally based joint working/collaborative meeting software is installed..

Fail Criterion 4:

Upon checking the software list at **SOE 3.1.b** and **SOE 3.1.c** the organization is found to have Remote Access or Portal installed and accessible from outside the LAN as indicated by the firewall rules provided for **SOE 3.8.e**.





LOGISTICS FOR A CDS LEVEL 3 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 3 audits.

DURATION

A CDS level 3 audit should take no longer than the following, depending upon the size of the organization:

Tiny – Small	-	1 day
Medium	-	1 day
Large	-	2 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 check list for those preparing for the audit. The following diagram shows the location of the various sections for the CDS Level 3 Audit.

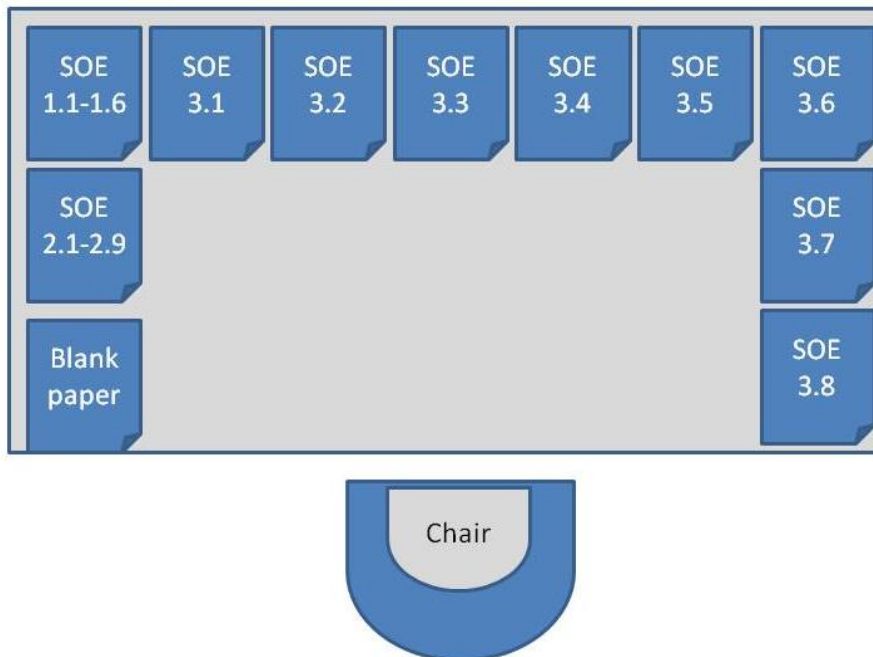


Figure 1 - CDS Level 3 SOE arrangement

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