



Certified Digital Security Level 1 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 1.



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 admin 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 1.....	6
Part 3 CDS Audit Requirements.....	25
Logistics for a CDS Level 1 Audit.....	50





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 taking steps to improve your system security in a managed and easily achievable way. It enables you to put simple but effective measures in place which can then be independently audited to prove to others that you are actually doing what you claim you are doing,. This way you are able to show clients, service providers and shareholders that you take the security of data and your IT systems seriously.

To achieve a Level 1 certification requires an organization to do the following:

Publish a policy governing how the organization wishes to manage its information security and explain, in simple terms what it expects of its staff. The policy must cover what is and is not acceptable staff behavior when sending email and browsing the internet.

Individual User Accounts for all users (including Administrators), so the organization can quickly and easily determine who has carried out specific activities on the IT system.

Making Administrators use a normal user level account for all work not requiring the special capabilities of an Administrator account significantly reduces the chances of their account being taken over or abused by malware or hackers.

Install *Anti Virus software* on servers and desktop / laptop computers to reduce the risk of a virus or other malicious software stopping the IT system from working, or making it unreliable.

Publish a *policy explaining what the organization's important data assets are and how they are to be disposed of when they become unusable or are no longer required*. This will help to prevent the organization accidentally disposing of items that have stored sensitive data (including client or personal data), and attracting criticism.

Check with the Information Commissioner's Office that any handling or storage of personal data meets the registration requirements of the Data Protection Act.

By implementing Level 1, an organization can expect to see:

- The legal responsibility for Users' actions moved from the organization's Directors and Senior Staff to the individual users.
- Greater productivity as the system suffers fewer virus attacks.
- More productive users as a result of improved system performance with less user induced breakdowns and failures
- Legal compliance is simpler to achieve with template forms and links to agencies.





PART 2

REQUIREMENTS FOR LEVEL 1





ABOUT THIS PART

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

RECOMMENDED PROCESS

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

- Step 1. Use the CDS Rough Assessment Workbook to see where there might be gaps in your security.
- Step 2. Select the CDS level based upon the needs of the business and the desired security measures.
- Step 3. Read the guidance document(s) for your target CDS level (note: any level requires that the levels below it are also implemented).
- Step 4. Look at your organization's current security to assess how it measures against the standard.
- Step 5. Note the gaps between your current security measures and those of your chosen level to calculate the work needed to meet your target.
- Step 6. Put in place work packages to fill the gaps.
- Step 7. Include security and regular reviews into normal business practice.

IF SEEKING AN AUDIT

If the organization is seeking an independent audit for CDS certification the reader is strongly encouraged to use Part 3 as the guide to what the auditor will need to see as proof that the CDS level has been correctly achieved. Part 3 is only used for CDS audits and is designed to show exactly what is required to be presented for audit and how it can be produced.

CDS Audits are speedy as, where possible, all evidence is simply being checked to ensure it is correct, relevant and compliant. The audits are check-sheet based (where possible) to ensure that they are transparent and objective.





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 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 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, appropriate credit is given to the CDS standard and that documents are kept in the format in which they are provided.

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 even 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 series of requirements which are numbered so they can easily be cross and externally referenced.

The requirement numbering includes the CDS level followed by that requirement's position in the list for that level.

For example: The fourth requirement on level 6 is identified as REQ6.4.

In Part 3 of this document the CDS audit evidence elements are defined. These are similarly numbered, but have an additional character for each separate element:

For example: The evidence for level 6 requirement number four (ie REQ6.4 from above) is noted under Part 3 as SOE6.4. The first evidence element for this requirement is noted as SOE6.4.a, the next as SOE6.4.b and so on.

Thus, the reader can easily cross-refer to both the requirement and evidence statements as REQ6.4 is supported by SOE6.4.

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 explanation of what the requirement is designed to achieve or introduce.
4. The group or individual that is assumed most likely to deliver, benefit or implement the requirement.
5. A detailed explanation of the requirement and how it needs to be implemented.
6. A list of the potential benefits that the implementation may bring.
7. Whether the requirement is recurring and if so the recurrence period (eg annually, monthly).
8. Any notes relevant to the implementation of the recommendation.



Basic Security Policy

Requirement Number: REQ 1.1

Overview:

The organization must have a published Policy for how it manages Information Security and how it expects staff to behave when handling information and using the organization's IT.

Responsible Group or Users:

The Policy should be developed by a nominated individual within the organization who understands the needs of the business and its processes. It should be endorsed by the owner or senior manager of the organization and should be made available to all users of the IT system or all employees, who should sign as having read and agreed to comply with it.

Requirement Description:

The policy must include or address the following topics:

- ❖ What staff are allowed to use the provided office equipment (fax, printers etc).
- ❖ How staff are to be aware of and protect the organization's Intellectual Property Rights (IPR).
- ❖ For staff with internet access, what they are allowed, and not allowed to do when surfing the internet.
- ❖ For staff that have access to internal and/or Internet email, what they are and are not allowed to send, and who they are allowed to send to.
- ❖ Where the staff can get advice or assistance on security matters and what they should do if they discover something unusual (eg a virus on their system).
- ❖ Who is allowed to make changes to the organization's system.
- ❖ What Anti-virus software is installed and how it is expected to work.
- ❖ How permission to take data off site can be obtained and that all data must be returned or wiped when the employee leaves the organization.
- ❖ The use of individual computer accounts for each member of staff, and a statement prohibiting the sharing of their account with other people unless specifically authorized in writing by senior management.
- ❖ How staff should select and protect their passwords, including the criteria for acceptable passwords (upper and lowercase letters, use of numbers and special characters (&, @, £ etc)
- ❖ A statement that employees are accountable for what they do using the computer accounts allocated to them, for which they have the password.
- ❖ A statement that, unless employees have previously reported that their account has been broken into, they are accountable for all activity that occurs on the computer accounts allocated to them, for which they have the password.

- ❖ A statement that the organization may conduct monitoring of their equipment and networks and what level of privacy users may expect.

Whist Email and web browsing are covered by other Level 1 CDS Requirements, general computer and office equipment usage are not. These two items are explained further below:

Acceptable Computer Usage:

The following topics must also be included in the Security Policy so that the staff are fully aware of their responsibilities and liabilities:

- ❖ What the organization's computer equipment can be used for, and where it can be used.
- ❖ Whether staff are allowed to upload files or computer programs into or out of the organization
- ❖ Whether staff are allowed to bring their own data (eg music libraries or photographs) to be stored, accessed or processed on the organization's systems.
- ❖ What the organization will do in the event of unacceptable computer usage (eg the disciplinary process), including reference to the organization's grievance process, complaints process and any Trade Union requirements or agreements.

Acceptable Office Equipment Usage:

The following topics must also be included in the Security Policy so that the staff are fully aware of their responsibilities and liabilities:

- ❖ What office equipment is available for employees to perform their duties.
- ❖ What facilities are available to employees for personal use and what the organization thinks is an acceptable amount of usage in terms of volume and time.
- ❖ What the organization will do in the event of unacceptable equipment usage (eg the disciplinary process), reference to the organization's grievance process, complaints process and any Trade Union requirements or agreements.

For all policies, users should be asked to read them on an annual basis and sign to signify that they agree to follow and adhere to the Organizational Security Policy.

Benefits from Implementation:

Computer and equipment users will be aware of how they should use equipment and data provided to them by the organization. This provides the organization with some legal protection in the event of improper use by its staff.

Recurring? If so frequency:

This policy should be reviewed annually by the organization or their nominated



representative, with the date of the review recorded. The policy must be endorsed by the senior manager or owner whenever it is amended, and staff should be required to re-sign their acceptance of it.



Acceptable Email Usage Policies

Requirement Number: REQ 1.2

Overview:

The organization must have a published Policy for how it expects staff to behave when using the organization's email system.

Responsible Group or Users:

The Policy should be developed by a nominated individual within the organization who understands the needs of the business and its processes. It should be endorsed by the owner or senior manager of the organization and should be made available to all users of the IT system or all employees, who should sign as having read and agreed to comply with it.

Requirement Description:

The policy must include or address the following topics:

- ❖ A statement that each member of staff is responsible for all activities carried out on the computer accounts with which they have been provided.
- ❖ A statement that, unless a user has previously reported that their account has been broken into, all emails will be deemed to have been composed and sent by the account holder.
- ❖ What systems can or cannot be used for official email (eg that hotmail is not appropriate for communicating with clients).
- ❖ What type of email is considered to be unacceptable (offensive, racism, threatening etc).
- ❖ What actions should a member of staff should take in the event that they receive unacceptable email, either from an internal or external source.
- ❖ What style and content the organization considers to be suitable for email communication and whether the style and content should vary dependent upon the recipient's relationship with the organization.
- ❖ What types of attachments, if any, are allowed to to be sent – based on any built-in controls or the need to keep certain information confidential.
- ❖ What methods can be used for sending specific categories of information such as contracts, invoices and reports. This can be by nominating who can send such communications (eg: Only purchasing staff can send purchase orders, or only HR staff can send contracts).
- ❖ Whether any sort of encryption is to be used; if so, the specific circumstances in which it is to be used and how to obtain the encryption key or password.
- ❖ What the organization will do in the event of unacceptable behavior relating to the email system (eg the disciplinary process), reference to the organization's grievance process, complaints process and any Trade Union requirements or agreements.

The organization should also tell its employees of any legal obligations for both the organization and the employee, which can include:

- ❖ Any email or attachment containing information known to be, or suspected of being, illegal in either the country of origin or country of receipt.
- ❖ Any email or attachment considered to be, or suspected of being, defamatory or indecent to any religion, group, person or organization.
- ❖ Any email or attachment considered to be, or suspected of, using derogatory language, tone or content which could be interpreted as abusive.

These policy statements are best placed in the organization's overall security policy documents.

For all policies, users should be asked to read them on an annual basis and sign to signify that they agree to follow and adhere to the Organizational Security Policy.

Benefits from Implementation:

- ❖ An accidental loss or leak of data is made less likely
- ❖ The organization gains some legal protection in the event of improper use by its staff.
- ❖ Staff are made aware of their responsibilities and are less likely to embarrass the organization, attract unwanted media attention or cause either themselves or the Directors/Owners/Senior Staff to face court action.

Recurring? If so frequency:

The policy should be reviewed:

- ❖ At least annually by the organization or their nominated representative, with the date of the review recorded.
- ❖ When the organization commences operating in new countries or regions.
- ❖ When the organization's goals or objectives change.
- ❖ If the organization is the subject of bad press or media coverage following a leak or compromise of email based information.

The policy must be endorsed by the senior manager or owner whenever it is amended, and staff should be required to re-sign their acceptance of it.

Acceptable Internet Usage Policy

Requirement Number: REQ 1.3

Overview:

The organization must have a published Policy for how it expects staff to behave when using the internet via the organization's IT system.

Responsible Group or Users:

The Policy should be developed by a nominated individual within the organization who understands the needs of the business and its processes. It should be endorsed by the owner or senior manager of the organization and should be made available to all users of the IT system or all employees, who should sign as having read and agreed to comply with it.

Requirement Description:

The policy must include or address the following topics:

- A statement that staff are accountable for all activity carried out whilst using their computer account to access the internet unless they have previously reported that their account has been broken into.
- What purposes the internet access can be used for.
- Whether use is permitted for personal purposes (e.g. are they allowed to surf to web-based email accounts, instant messaging and social networking sites (Facebook, , LinkedIn etc)? And, if so, during what periods (e.g. lunchtime, refreshment breaks)) and whether they can expect any privacy in relation to their personal activities.
- A statement of what subjects are deemed as or unacceptable when users are using search tools (such as Google or Ask) whilst surfing the internet.
- A statement on what to do if a user inadvertently accesses a web site prohibited by the organization.
- Guidance on the types of web site a user is not permitted to browse (inadvertent access should be acknowledged as differing from investigating various pages on a prohibited site). The following are generally not required for business or normal computer usage, although depending on the sector in which the organization operates there may be a need to have some access. A statement must be made on whether each of the site types listed below is allowed or banned (this list is mandatory but is not exhaustive):
 - Pornography or sex sites
 - Sites depicting violence
 - Sites encouraging or supporting illegal activities
 - Shopping sites

- Gambling sites
- File sharing sites such as Warez, Peer-2-Peer (P2P) or bit torrent.
- Weapon or war sites
- Religious sites (it is easiest to ban all, then all are equal)
- Medical sites (this is to discourage individuals looking at medical images which might cause offence or upset).
- ❖ What the organization will do in the event of unacceptable internet activity (eg the disciplinary process), reference to the organization's grievance process, complaints process and any Trade Union requirements or agreements.
- ❖ The organization must inform its employees of any legal obligations for both the organization and the employee (in the local office and also the location of their clients or users where these are located outside the country).
- ❖ A clear statement that the organization will assist law enforcement to investigate any breach of national or international laws that are alleged to have been committed by the users operating the organization's equipment. This includes, but is not limited to, terrorism, human trafficking, drug trafficking and child pornography.

These policy statements are best placed in the organization's overall security policy documents.

Benefits from Implementation:

- ❖ The organization gains some legal protection in the event of improper use by its staff.
- ❖ Staff are made aware of their responsibilities and are less likely to embarrass the organization, attract unwanted media attention or cause either themselves or the Directors/Owners/Senior Staff to face court action.
- ❖ Users will be less likely to waste time 'just browsing' and productivity should increase.
- ❖ The risks of web site-based attacks, or inadvertent loading of malicious code (viruses or spyware) are reduced.
- ❖ By laying the policy down in written form, legal process can be followed for habitual offenders (eg cease their employment contract).

Recurring? If so frequency:

The policy should be reviewed:

- ❖ At least annually by the organization or their nominated representative, with the date of the review recorded.
- ❖ When the organization commences operating in new countries or regions.
- ❖ When the organization's goals or objectives change.
- ❖ If the organization is the subject of bad press or media coverage following a leak or compromise of email based information.

The policy must be endorsed by the senior manager or owner whenever it is amended, and



staff should be required to re-sign their acceptance of it.

Notes:

Organizations may wish to consider having their policy reviewed by their legal advisors or legal representative on an annual basis to ensure continuing compliance with national legislation.



Individual User Accounts

Requirement Number: REQ 1.4

Overview:

Provide each person with an individual computer account that only they have access to and use of. Require administrators to have a normal user level account for email, web browsing and routine work and a separate Administrator account for admin functions and tasks.

Responsible Group or Users: This applies to ALL users of the system.

Requirement Description:

All users are to have individual accounts with a basic level of access. This level of access follows the principle of least privilege where users are only able to carry out the tasks needed to do their job.

Every system administrator should have an account with the basic level of access. They should only make use of their Administrator privileged account when carrying out work that requires the increased permissions of that type of account. No email account is to be associated with the higher privileged account, nor should it be used to access the internet. At all other times system administrators should make use of their basic level account.

Individual basic level accounts should have their privileges set to prevent the following:

- ❖ Installing and uninstalling software.
- ❖ Altering any security software (e.g. Anti Virus, Firewall, HIDS etc) or preventing it from working.
- ❖ Adding new equipment or hardware to the IT system.
- ❖ Adding operating software, such as device drivers, to the system.
- ❖ Adding, Deleting or changing user accounts.
- ❖ Changing how the network is set up (eg. IP address, connectivity etc).
- ❖ Altering computer settings that control who is able to access information not owned by the user.
- ❖ Running any higher privileged 'system/administrator/root' type command without having to change from a basic level to an Administrator level.

Benefits from Implementation:

Supports the policy aims of REQ1.1 that users are responsible for their actions on the organization's system.

Reduces the risk that a hacker can take over an administrator account, which is possibly the



most dangerous for any system.

Makes the audit of administrator accounts easier and the noticing of any potentially dangerous activity more likely.

Reduces the chances of administrators accidentally changing a critical setting on the system.

Recurring? If so frequency:

This is to be implemented and permanently enforced. Accounts must be checked every 6 months to ensure that any unnecessary accounts are removed or disabled.

Notes:

See Section 3 for ways to check the numbers of accounts that should be required.



Anti-Virus

Requirement Number: REQ 1.5

Overview:

Simple Anti-virus software and procedures must be put in place and regularly updated.

Responsible Group or Users: System Administrators should install and configure the software to run without user interaction.

Requirement Description:

The organization must determine what antivirus products it wishes to use and where these are best installed (whether on servers, PCs or both), this decision should be documented somewhere (the organization Security Policy is the best place).

Anti-Virus software should have the following features:

- ❖ Be able to scan on both PCs and Servers, and able to scan without the user being aware it is being done and without a large drop in the speed of the computer (on-access and background scanning).
- ❖ Be able to move any detected virus infected files or other suspicious software to a safe area for examination (quarantine).

Anti-Virus products should be installed according to the manufacturer's instructions and must be set to ensure that a user cannot stop it working without getting permission.

The product must be regularly updated to ensure it continues to provide protection against new virus threat. Updates can be set to occur automatically and should be done at least weekly, but daily is recommended.

In circumstances where Anti-Virus products cannot be installed, then other measures to prevent virus infection should be considered. These must be documented (in the Security Policy) and agreed as part of the acceptance process for the security policy.

All Anti-Virus products must be lawfully licensed and operated in compliance with the licence. It should be noted that some 'free' anti-virus products remain free only for personal use and their use in the corporate environment is not free.

Benefits from Implementation:

The organization will:

- ❖ Have a more stable and resilient IT system, with a lower risk of lost productivity resulting from a virus infection.
- ❖ Have a more reliable IT system.
- ❖ Be less likely to suffer the embarrassment and possible legal consequences of sending an infected document to a client.
- ❖ Be less likely to suffer a failure of the IT system or have data destroyed by malicious software.

Recurring? If so frequency:

Signature files must be updated at least weekly on client systems and at least daily on server systems where they are connected to the Internet. Where systems are isolated from the internet and other networks, a slightly slower update frequency maybe acceptable.

Notes:

Where systems are unable to run Anti-virus products, or business circumstances prevent their use, the reasons why must be documented, together with any additional procedures being used instead of Anti-virus software. This can be sent to the CDS Certification Body with a request for this requirement to be waived at audit. Circumstances and supplementary procedures will form the basis of the Certification Body's decision.

Asset Disposal Policy

Requirement Number: REQ 1.6

Overview:

The organization must define how it will dispose of equipment and other media which has been used to store information when it has reached its end of life, is broken or is to be returned or sent to another organization.

Responsible Group or Users: All members of the organization

Requirement Description:

To prevent data loss through asset disposal an organization must:

- ❖ Identify which assets require secure and controlled disposal.
- ❖ Determine how these assets can be disposed of (e.g. shredding of all paper documents and CDs) and implement the disposal methods across the organization.
- ❖ Consider how assets can be tracked and managed in the organization (e.g a hard drive removed from a computer and awaiting disposal recorded in a register).
- ❖ Identify who will be responsible for determining and ensuring proper asset disposal.
- ❖ Identify where assets marked for disposal will be securely kept to prevent unauthorized access or reuse prior to disposal.

These do not need to be lengthy statements, and should be proportional to the size of the organization and number of systems that handle data.

For a small organization with 10 dedicated pc's working on client data, a simple record of the asset and planned disposal (eg wiping or physical destruction), would be sufficient.

Due consideration must also be given to any requirements for safe disposal. These may be covered under the organization's Health & Safety or Waste Electrical & Electronic Equipment legislation.

Benefits from Implementation:

An organization that controls its asset disposal will have reduced the risk that:

- ❖ Client data will leak into the public domain as a result of uncontrolled disposal or poor asset handling.
- ❖ Adverse criticism will be leveled against them due to sensitive data being found in bins,



on internet sales sites or some other public location such as rubbish tips or recycling plants.



Recurring? If so frequency:

The records should be checked every 6 months to ensure the disposal processes are being implemented and are working effectively..



Personal Data Protection

Requirement Number: REQ 1.7

Overview:

The organization must confirm whether it needs to be registered as a data custodian under the Data Protection Act 1998.

Responsible Group or Users: The senior person in the organization, or the person nominated as being responsible for data protection issues.

Requirement Description:

To ensure compliance with Data Protection legislation, the organization must:

- ❖ Identify the types of data held within the organization.
- ❖ Conduct the Information Commissioner's Office online self-assessment. The assessment can be found at <http://www.ico.gov.uk/notify/self/question1.html>.
- ❖ Notify the Information Commissioner's Office if the self-assessment indicates that it is necessary.
- ❖ Comply with Data Protection Act 1998 provisions, and the advice on data protection measures given by the ICO, if they are a notified organization.

If the Organization notifies the Information Commissioner's Office that personal data is being processed, the Security Policy (**REQ 1.1**) must contain details of measures to be taken for the safe custody, storage and transmission of personal data.

Benefits from Implementation:

An organization that holds or processes data will have an understanding of its legal obligations regarding personal data and benefit from:

- ❖ Reduced risk of legal action due to non-compliance with legal requirements.
- ❖ Understanding how personal data can be handled, transferred and managed.
- ❖ Being able to assign appropriate protection to data storage and transfers.

Recurring? If so frequency:

Annual checks of data holdings should be carried out and, if necessary or to remove doubt, the self-assessment should be conducted again.



PART 3

CDS AUDIT REQUIREMENTS





ABOUT THIS PART

Part 3 outlines what an organization must do to demonstrate that their implementation of their chosen target Certified Digital Security (CDS) level is compliant with the standard.

IF SEEKING AN AUDIT

If your organization is seeking an independent audit of their CDS implementation, you are strongly encouraged to use this Part 3 as the guide to the production of the necessary proof that you meet the requirements of your chosen target level. Compliance with Part 3 is only used for the purpose of auditing and is designed to inform the reader of the type, quality and timeliness of the required information and detail the structure of the proof that must be presented for audit.

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 (remembering that you must include all preceding levels).
- Step 2. Go to the CDS Web Site (www.certifieddigitalsecurity.com) and read the audit process outlined on the 'Audit Requirements' pages (or Part 3 of the guidance document associated with your chosen CDS target level).
- Step 3. Implement the measures contained in each of the requirements for your chosen level of the standard.
- Step 4. Using Part 3, Identify the proof you will need to present to meet the Statements of Evidence (SOE) for each requirement within your target level (and those that precede it).
- Step 5. Arrange for the proof to be produced in printed copy (as required), whilst completing the application for CDS audit (and scheme membership, if not already done).
- Step 6. Once you have produced the required proof for your target level of the standard (or are close to doing so), contact a CDS Auditor via the CDS Web Site and arrange an audit.





- Step 7. Prepare the organization for the day of the audit – ensure the room meets the standard set in Part 3 and that all necessary proof is correctly formatted, labeled and presented for the level targeted.
- Step 8. 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 that all the proof¹ necessary to prove the requirements² has been provided. 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 proof presented to the auditor at the time of the audit. They are not protracted events since the room, lighting and even 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 need actually presented to the auditor. This ensures that the audit is conducted within the planned and quoted timeframe.

NO HANDS ON!

CDS auditors do not require to connect any computers onto your network and the auditor should not be offered any connections or access to your systems for review purposes. Any such request or offering is not supported or condoned by CDS or Digital Security Ltd. The Audit process is specifically designed to prevent the auditor from being able to affect the system being reviewed. Similarly, the auditor does not require general access to your premises, only the area provided for the audit.

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 as well 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 of proof or which levels are not required to be audited, or
- ❖ The organization presents an audit pass certificate for the lower level(s) dated within 4 months of the date of the audit

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 proof are correct and contain the information needed to demonstrate compliance, 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 presentation.

The auditor will forward their report to the Certification Body (Digital Security) who will review the auditor's report and, if satisfactory, endorse the report's recommendation. The certification body will inform the organization of the result within 4 working days (usually 1-2 days) of receiving the report.

The organization will be required to retain a copy of the auditor's report together with all documents provided as proof of compliance (the auditor will provide tamper-evident bags for this purpose) as the Certification Body will destroy their copy once their certification decision is made (for security reasons). This is regardless of whether the organization is awarded a certificate or not.

The organization will be asked to complete a certification application to confirm the title they wish to have on their certificate, the level of publicity they would like and whether they wish other organizations to be told of their certification level. Publicity 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 that pass a CDS level will be issued a unique reference that can be given to clients or external 3rd parties to allow 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

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

In the event that the audit findings result in non-compliance with your target CDS level a report will be provided to you explaining the corrective work needed to achieve the required standard prior to a re-audit.

HOW REQUIREMENTS ARE MET

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

The requirement numbering includes the CDS level followed by that requirement's position in the list for that level. Requirements are prefixed with 'REQ' (for requirement)

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

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

For example: The proof for level 6 requirement number four (ie REQ 6.4 from above) is noted under Part 3 as SOE 6.4. The first evidence element for this requirement is noted as SOE 6.4.a, the next as SOE 6.4.b and so on.

Thus, the reader can easily cross-refer to both the requirement and individual evidence statements as REQ 6.4 is supported by SOE6.4.

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 proof required (the numbers, percentages or other details relating to the quality and type of proof needed). This may be further broken down and may link to the CDS website for current information. Note: currency will be used for best practice, changes should not affect audit compliance.
6. Details of how the proof can be generated.
7. The details of the compliance or non-compliance Criteria – if known.
8. Any notes relevant to the SOE.



Basic Security Policy

Statement Of Evidence(SOE) Number: SOE 1.1

Overview:

Confirmation that the organization has a published policy for how it manages Information Security and how it expects its staff to behave when handling information and using the organization's IT, that has been endorsed by the owner or senior manager of the organization and is being read by the users.

Statement Of Evidence (SOE) Description:

SOE 1.1.a.

The organization must have a published Security Policy for all staff to follow. The policy must be endorsed (in writing) by the owner or senior manager within the organization. The written policy must be presented to the auditor in printed copy on A4/letter size paper.

The policy must include or address the following topics:

SOE 1.1.b.

A statement that employees are accountable for what they do using the computer accounts allocated to them, for which they have the password..

SOE 1.1.c.

The email usage policy (proven separately under **SOE 1.2.**) should form part of the overall Security Policy. An organization will be non-compliant with this element if the email policy is not included or referenced in the overall Security Policy.

SOE 1.1.d.

The internet usage (proven separately under **SOE 1.2.**) should form part of the overall Security Policy. An organization will be non-compliant with this element if the internet usage policy is not included or referenced in the overall Security Policy.

SOE 1.1.e.

A statement as to who is allowed to make changes to the organization's system.

SOE 1.1.f.

Details of how staff should select and protect their passwords, including the criteria for acceptable passwords (upper and lowercase letters, use of numbers and special characters (&, @, £ etc)

SOE 1.1.g.

The fact that employees are accountable for what they do using the computer accounts allocated to them, for which they have the password, including a statement that, unless employees have previously reported that their account has been broken into, they are accountable for all activity that occurs on the computer accounts allocated to them.

SOE 1.1.h.

The fact that users are not to share their computer accounts unless specifically authorized, documented and endorsed by senior management (written proof of any authorized sharing must be produced at the time of the audit).

SOE 1.1.i .

A statement as to whether users are authorized to upload files or programs into or out of the organization.

SOE 1.1.j.

How the users are to be aware of and protect the organization's Intellectual Property Rights (IPR).

SOE 1.1.k.

Where the staff can get advice or assistance on security matters and what they should do if they discover something unusual (eg a virus on their system).

SOE 1.1.l.

The organization must have defined what personal processing may be conducted on the system including a statement that the organization may conduct monitoring of their equipment and networks and what level of privacy users may expect.

SOE 1.1.m.

The policy must be in circulation or use. Proof of users having read the policy must be produced. This proof must be in the form of a hard copy showing that at least 90% of users have seen the policy and agree to be bound by it in their use of the system. This will require a nominal roll or register to show the total number of users in the organization and the percentage of user acceptance.

SOE 1.1.n.

There must be either a process in place for reviewing the security policy (if it is less than one year old) or evidence of previous (at least annual) reviews having been conducted. A record should be placed in each document showing the dates of the review and the person who conducted it.



How this can be generated:

The policy should specifically include all of the evidence requirement's outlined above, but ideally include all the items in REQ 1.1. The policy can be endorsed separately by management, but it is recommended that all readers are able to see the endorsement at the time they read it, thus it is preferred that a signed endorsement is included in the policy itself.

The users can physically sign a sheet of paper that refers to the organization security policy. This should include words to the effect:

“By signing this sheet I certify that I have read the organization’s Security Policy and I agree to operate the provided IT equipment in the manner outlined and required in the policy”

The user should add their given and family names and date the signature.

Alternatively, the organization can email out the policy and require that the user e-sign the policy and returns something that can be evidenced (in hard copy) as their acceptance of the policy (MS Exchange allows the use of voting buttons that will facilitate this function – with the tracking pane of original email being printed as the evidence).

Template policies are available on the CDS website⁴.

Details of the compliance Criteria for SOE 1.1:

SOE 1.1 Will be deemed to be non-compliant if any compliance Criterion is not met or is outstanding at the end of the audit period:

Criterion 1:

Presentation of a full hard copy of the in use Security Policy (**SOE 1.1.a.**) which includes the sub elements covered by **SOE 1.1.b - SOE 1.1.I.**

Criterion 2:

Production of the required evidence, with fewer than two items from the **SOE 1.1.b. - SOE 1.1.I.** missing (ie not having addressed or included two or more elements in the presented Security Policy will be non-compliant).

Criterion 3:

Presentation of proof that the Security Policy from **SOE 1.1.a.** has been read and accepted by 90% of staff (as indicated by the nominal roll and user acceptance list). An organization that cannot produce an up-to-date hard copy user list and nominal roll will also be non-compliant

⁴ www.certifieddigitalsecurity.com





for this element.

Criterion 4:

Presentation of proof of previous reviews of the policy, or the process for how the policy will be reviewed in the future for **SOE 1.1.n**.



Acceptable Email Usage Policies

Statement Of Evidence (SOE) Number: SOE 1.2

Overview:

Confirmation that the organization has described to its users what types of email are acceptable, what types are not and how emails should be sent and what to do if unacceptable email is received.

Statement Of Evidence (SOE) Description:

SOE 1.2.a.

The organization must have a written Policy explaining what it considers to be Acceptable Email Usage for all users of the provided email system. It must cover the following items within its text:

SOE 1.2.b.

User accountability statement, that users are responsible for their actions when working with email using an account protected by a password selected by (and known only to) them. The fact that, unless a user has previously reported that their account has been broken into, all emails will be deemed to have been composed and sent by the account holder.

SOE 1.2.c.

The email usage policy must clearly state what systems can or cannot be used for official communications.

SOE 1.2.d.

The email policy must state what type of email is considered to be unacceptable (offensive, racism, threatening etc) and outline what actions a member of staff should take in the event they receive unacceptable email from either an internal or external source.

SOE 1.2.e.

The policy must outline what style and content is considered suitable for emails and what attachments, if any, are allowed to be sent internally and externally, including any size limits (eg: No program files to be sent externally and no files larger than 5mb to be emailed)

SOE 1.2.f.

The policy must detail how specific categories of communications such as contracts and invoicing are allowed to be sent.

SOE 1.2.g.

The users must be made aware of the use of any sort of encryption; how and when this is to

be used (eg: Personal, medical and names client data must be sent by encrypted emails only) and how to obtain the encryption key or password.

SOE 1.2.h.

The organization must also inform its employees of any likely penalties in the event of unacceptable behavior relating to email use, and any legal obligations for both the organization and the employee (in both the local office and in the location of their clients or users), and a statement that they will assist the local law enforcement should they be requested or required to do so.

SOE 1.2.i.

These policy statements should be placed in, or referred to in, the organization's overall Security Policy; this will ensure they are reviewed by management at regular intervals and read by users at least annually.

How this can be generated:

Whilst the original document may be held only in soft copy format, the policy must be presented in hard copy format printed on A4/letter size paper for audit.

Endorsements should be in the form of either a signature on the front of the Policy, or a foreword by the senior manager that states the need for the policy and the endorsement of the requirements contained with the document.

All elements of the Acceptable Email Usage Policy are contained in the Acceptable Email Policy template which can be downloaded from the CDS website.

Details of the compliance Criteria for SOE 1.2:

SOE 1.2 Will be deemed to be non-compliant if any compliance Criterion is not met or is outstanding at the end of the audit period:

Criterion 1:

Production of a full hard copy of the in use Acceptable Email Usage Policy (**SOE 1.2.a.**) which includes all the sub elements covered by **SOE 1.2.b. - SOE 1.2.i.**

Criterion 2:

Production of the required evidence, with fewer than two items from the **SOE 1.2.b. - SOE 1.2.h.** missing (ie not having addressed or included two or more elements in the presented Security Policy will be non-compliant).



Criterion 3:

Presentation of evidence of previous reviews of the policy, or a plan for how the policy will be reviewed in the future for **SOE 1.2.i**.

Notes:

This item must be included or referenced in the main Security Policy. If the organization does not include it or reference it then they are not compliant with **this SOE** rather than **SOE 1.1.c**.



Acceptable Internet Usage Policy

Statement Of Evidence (SOE) Number: SOE 1.3

Overview:

Confirmation that the organization has described to its users what uses of any internet connection are acceptable, what types are not and what to do if unacceptable internet content is viewed.

Statement Of Evidence (SOE) Description:

SOE 1.3.a.

The organization must have a written Policy explaining what it considers to be Acceptable Internet Usage for all users of any Internet connection provided for their use. It must cover or address the following items within its text:

SOE 1.3.b.

The organization must define what acceptable behavior for users of the internet connectivity is.

SOE 1.3.c.

The organization must state what it will do in the event of a user carrying out unacceptable internet activities.

SOE 1.3.d

The organizations must define what (if any) personal use is permitted and, if so, the times when this is allowed. A statement should also be included on whether the users can expect any element of privacy regarding any personal information processed on the system. Clear guidance must be given for the following types of usage:

- ❖ Browsing to personal or other web-based email accounts outside of the organization.
- ❖ The use of personal accounts on instant messaging software outside of the organization.
- ❖ The use of social networking sites (including Facebook, Bebo, LinkedIn).

SOE 1.3.e.

The organization must state that staff are accountable for all activity carried out whilst using their computer account to access the internet unless they have previously reported that their account has been broken into.

SOE 1.3.f.

The organization must state what subjects are considered unacceptable as topics for internet

searches and the types of sites it is acceptable for users to visit. This must, as a minimum, include clear statements regarding the following types of sites:

- ❖ Pornography or sex sites.
- ❖ Sites depicting violence.
- ❖ Sites encouraging or supporting illegal activities.
- ❖ Shopping sites.
- ❖ Gambling sites.
- ❖ File sharing sites such as Warez, Peer-2-Peer (P2P) or bit torrent.
- ❖ Weapon or war sites.
- ❖ Sites with strong or stated religious orientations.
- ❖ Medical sites.

SOE 1.3.g

The organization should outline the ramifications should an employee break these rules or guidelines. This should be linked to the HR manual and Trade Union handbook where required by the organization.

SOE 1.3.h.

The organization must inform its employees of any legal obligations for both the organization and the employee (in the local office and also the location of their clients or users where these are located outside the country).

SOE 1.3.i.

The organization must clearly state in its policy that it will assist law enforcement investigate any breach of national or international laws that are alleged to have been committed by the users operating the organization's equipment. This includes but is not limited to, terrorism, human trafficking, drug trafficking and child pornography.

SOE 1.3.j.

These policy statements should be placed in, or referred to in, the organization's overall Security Policy; this will ensure they are reviewed by management at regular intervals and read by users at least annually.

How this can be generated:

The written policy must be presented in hard copy format printed on A4/letter size paper.

Endorsements should be in the form of either a signature on the front of the Policy, or a foreword by the senior manager that states the need for the policy and the endorsement of the requirements contained with the document.

All elements of the Acceptable Internet Usage Policy are contained in the Acceptable Internet Policy template which can be downloaded from the CDS website.



Details of the compliance Criteria for SOE 1.3:

SOE 1.3 Will be deemed to be non-compliant if any compliance Criterion is not met or is outstanding at the end of the audit period:

Criterion 1:

Presentation of a full hard copy of the in use Acceptable Internet Usage Policy (**SOE 1.3.a.**) which includes all the sub elements covered by **SOE 1.3.b. - SOE 1.3.i.**

Criterion 2:

Production of the required evidence, with fewer than two items from the **SOE 1.3.b. - SOE 1.3.i.** missing (ie not having addressed or included two or more elements in the presented Security Policy will be non-compliant).

Criterion 3:

Presentation of evidence of previous reviews of the policy, or a plan for how the policy will be reviewed in the future for **SOE 1.3.j.**

Notes:

This item must be included or referenced in the main Security Policy. If the organization does not include it or reference it then they are not compliant with **this SOE** rather than **SOE 1.1.c.**



Individual User Accounts

Statement Of Evidence (SOE) Number: SOE 1.4

Overview:

Confirmation that each user has been provided with a computer account that only they have access to and use of. Also confirmation that administrators have normal user level account for routine work and separate, more powerful accounts for system administration.

Statement Of Evidence (SOE) Description:

SOE 1.4.a.

The organization must present a nominal roll of all users on the system.

SOE 1.4.b.

The organization must present a consolidated list of user accounts on the complete system.

SOE 1.4.c.

The organization must show which accounts have higher privileges than normal accounts i.e. system, root or administrator level.

SOE 1.4.d.

The organization must show that all users have a basic level account, preventing them from:

- ❖ Installing and uninstalling software.
- ❖ Altering any security software (e.g. Anti Virus, Firewall, HIDS etc) or preventing it from working.
- ❖ Adding new equipment or hardware to the IT system.
- ❖ Adding operating software, such as device drivers, to the system.
- ❖ Adding, Deleting or changing user accounts.
- ❖ Changing how the network is set up (eg. IP address, connectivity etc).
- ❖ Altering computer settings that control who is able to access information not owned by the user.
- ❖ Running any higher privileged 'system/administrator/root' type command without having to change from a basic level to an Administrator level.

SOE 1.4.e.

The organization must show that all system administrators operate a basic level account. Therefore, all administrators should have 2 accounts (one for email etc and one for system administration tasks). The total number of accounts must be at least the total number of all users (including administrators) plus the administrators.

How this evidence may be generated:

The organization must provide evidence that all users have individual accounts. In a small organization that is not using a system able to carry out central accounts management (Microsoft Windows can carry out central account management), the evidence will need to show each computer's user information.

The evidence must include both a nominal roll of approved users and the list of user accounts held on the system (including the administrators). The organization must identify who is an administrator on the system and the auditor must be able to see evidence of these staff holding two accounts (a normal account and an administrator account).

This evidence must be in hard copy form; auditors are not permitted to have any interaction with the system under audit.

A printout of the users and their accounts can be carried out within most operating systems. If the organization is not able to do this then simple screen shots will suffice.

Details of the compliance Criteria for SOE 1.4:

SOE 1.4 Will be deemed to be non-compliant if any compliance Criterion is not met or is outstanding at the end of the audit period:

Criterion 1:

Presentation of a nominal roll of staff that use the network that is to be CDS Certified and the list of user accounts and privileged accounts.

Criterion 2:

The organization has issued all administrators/superusers with a basic user level account as well as their administrator/superuser account.

Anti-Virus

Statement Of Evidence (SOE) Number: SOE 1.5

Overview:

Confirmation that the organization has up-to-date anti-virus software on computers and servers. Where anti-virus products are not used, or cannot be used, alternative methods to prevent virus infection have been considered, documented and accepted by the organizations' senior staff.

Statement Of Evidence (SOE) Description:

Unless the organization has decided that it will not implement Anti -virus software on every workstation and server that data is stored upon (eg file servers, web servers, mail servers), then each of these systems should have an up-to-date Anti-virus product on it.

Generally, all systems require Anti-virus software and the installed products should be licensed legally and must be set to update at least weekly. The specific evidence should be presented to the Auditor:

SOE 1.5.a.

The organization must present a list of all computers (including all desktops, laptops, netbooks and tablets, PCs and MACs) within the network to be CDS certified.

SOE 1.5.b.

The organization must show that the Anti-virus products installed on its systems are up-to-date and correctly set up. The settings of Anti-virus software must include on-access scanning and deletion or quarantining of suspicious or infected files. A system generated date of printing or creation of this information must be included.

SOE 1.5.c.

The latest update for the Anti-virus product must show that the update took place within one week of the evidence being printed. Where the evidence is manually generated (such as screen shots from each computer) it must be less than 3 weeks old at the time of audit. Where it is generated by a central management suite, the evidence must be less than 2 weeks old at the time of audit (this is to allow the organization some time to gather all necessary CDS evidence).

SOE 1.5.d.

The organization must show that more than 90% of computers meet the update requirement of **SOE 1.5.c** ie at least 90% must have been updated within a week of evidence production.

SOE 1.5.e.

The organization must produce a consolidated list of all servers on the network to be CDS certified, including the function of these servers. The following are considered to have some interaction with users and their information and therefore must have an Anti-virus product installed:

- ❖ File Servers.
- ❖ Mail Servers.
- ❖ Forum or blog servers.
- ❖ Web application servers.
- ❖ Database servers (where the database stores any files or user input).

If in any doubt please contact auditsupport@certifieddigitalsecurity.com

SOE 1.5.f.

The organization must show that the Anti-virus products installed on these servers is up-to-date and correctly set-up. The settings of the Anti-virus software of these servers must include on-access scanning and deletion or quarantining of suspicious or infected files. A system generated date of printing or creation of this information must be included.

SOE 1.5.g.

The latest update for the Server Anti-virus product must be within one week of the date of creation of the evidence. This evidence must be less than 2 weeks old at the time of audit.

SOE 1.5.h.

The organization must show that more than 90% of servers meet the update requirement of SOE 1.5.g ie at least 90% of them must have been updated within a week of the evidence being generated.

Note: A server that requires Anti-virus, but which is out of date (ie operating with signatures, dat files or updates more than a week old) will count towards the 10% allowed in **SOE 1.5.h.** If no Anti-virus is installed on a system which requires it, the organization will be non-compliant with this SOE.

If an organization is not using Anti Virus products on servers requiring it under this standard, they should contact auditsupport@certifieddigitalsecurity.com to register their exception. The Certification Board will issue an exception if the organization has a management endorsed mitigation plan. This mitigation will be assessed by the Certification Board and any implementation facts will be validated during the audit.

How this evidence may be generated:

For small organizations with fewer than 20 computers, screen shots of the software installed will suffice, providing it shows the software settings. For larger organizations a report from the Anti-virus product's central management software detailing the various settings and updates or versions should be provided.

If an organization is not using Anti-virus products on servers requiring it under this standard, they should contact auditsupport@certifieddigitalsecurity.com to register their non-compliance. The Certification Body will issue a waiver for REQ 1.5 if the organization has a management endorsed mitigation plan. This mitigation will be assessed by the Certification Body and existence of the claimed mitigation will be validated during the audit.

Details of the compliance Criteria for SOE 1.5:

SOE 1.5 Will be deemed to be non-compliant if any compliance Criterion is not met or is outstanding at the end of the audit period:

Criterion 1:

Presentation of a full hard copy of the list of computers and servers.

Criterion 2:

Production of the required evidence that computers were updated within a week prior to the evidence being generated.

Criterion 3:

Production of a system generated date included on the evidence to show when it was generated.

Criterion 4:

Production of the required evidence that servers were updated within a week prior to the evidence being generated.

Criterion 5:

Anti-virus software installed on all server systems requiring it (see **SOE 1.5.e**) or a valid waiver certificate issued by the Certification Body.

Asset Disposal Policy

Statement Of Evidence (SOE) Number: SOE 1.6

Overview:

Confirmation that the organization has a policy defining the equipment and media it considers important and the approved means of disposing of them.

Statement Of Evidence (SOE) Description:

SOE 1.6.a.

The organization must present a written policy relating to asset disposal.

SOE 1.6.b.

This policy must include specific statements on the following:

- ❖ Who is responsible for determining the need for, and ensuring to conduct of, proper asset disposal.
- ❖ Which assets would require secure and controlled disposal.
- ❖ How these assets are tracked and managed in the organization.
- ❖ Where assets marked for disposal are securely kept preventing unauthorized access or reusing prior to disposal.
- ❖ How each asset type is to be destroyed⁵.

SOE 1.6.c.

The organization must present records of any media containing 'digital assets' disposed of by the organization or its contractors. These must include at least:

- ❖ The unique asset identifier (eg laptop or hard drive item serial number).
- ❖ The system it came from (by asset number or location/user of the system).
- ❖ The data it contained (eg clients or the department that used it).
- ❖ The disposal method (eg wiping/destruction/shredding).
- ❖ The cross reference to any certificate of destruction⁶.

⁵ These include wiping, shredding, melting, grinding or degaussing.

⁶ This is any statement given by a person or individual that the item listed was identified and verified before being destroyed or treated as described in the statement. Eg that the hard drive serial number XXX was shredded in an industrial metal shredder by Mr Smith on 15/04/2010, all parts were observed to be broken and the device rendered useless.



How this can be generated:

The written policy must be presented in hard copy format printed on A4/letter size paper.

Details of the compliance Criteria for SOE 1.6:

SOE 1.6 Will be deemed to be non-compliant if any compliance Criterion is not met or is outstanding at the end of the audit period:

Criterion 1:

Presentation of a full hard copy of the Asset Disposal Policy (**SOE 1.6.a**).

Criterion 2:

Asset Disposal Policy (**SOE 1.6.a**) to include the 5 statements items required at **SOE 1.6.b**.

Criterion 3:

The Asset Disposal Policy not including the details of the 5 statements required under **SOE 1.6.b**.



Personal Data Protection

Requirement Number: SOE 1.7

Overview:

The organization must demonstrate that it has considered its position under the Data Protection Act 1998.

Statement Of Evidence (SOE) Description:

SOE 1.7.a

The organization must provide a copy of the notification to the ICO, or a written statement explaining the basis of its exemption from notification.

SOE 1.7.b

The exemption statement must be endorsed by the senior person in the organization or the person nominated as responsible for data protection matters.

SOE 1.7.c

If the organization has notified the ICO that it is processing personal data, the Security Policy must give details of measures to be taken for protecting the data, including:

- ❖ safe custody
- ❖ storage
- ❖ transmission.

How this can be generated:

All documents must be presented in hard copy format printed on A4/letter size paper.

Details of the compliance Criteria for SOE 1.7:

SOE 1.7 Will be deemed to be non-compliant if any compliance Criterion is not met or is outstanding at the end of the audit period:

Criterion 1:

Presentation of a printed copy of the ICO Notification or statement of exemption (**SOE 1.7.a.**).



Criterion 2:

Statement of exemption to be signed by the senior person in the organization or by the person with nominated responsibility for data protection issues (**SOE 1.7.b**)

Criterion 3:

The Security Policy not including the details of the 3 protection topics required under **SOE 1.7.c**.



LOGISTICS FOR A CDS LEVEL 1 AUDIT

The audit process for CDS has been designed to be extremely efficient in terms of time for both auditor and the organization. To gain the maximum advantage from this efficiency, organizations preparing for audit should note and, where possible, comply with the following provisions.

DURATION

A CDS level 1 audit, depending upon the size of the organization, should take no longer than the following amounts of time:

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 health and safety requirements in terms of height, stability and surface finish. The room must be a correctly heated, quiet and well lit space appropriate for normal human occupation and administrative working (ie 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; so do not locate them in a place where, generally, talking is frowned upon (eg a call center operations floor).

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

A local safe power outlet should be provided should the auditor require it for their IT. Use of a telephone is not mandatory but may benefit the organization if the auditor is not being accompanied throughout their visit and they need to clarify or expand 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 diagram below shows the location of the various sections for the CDS level 1 audit.

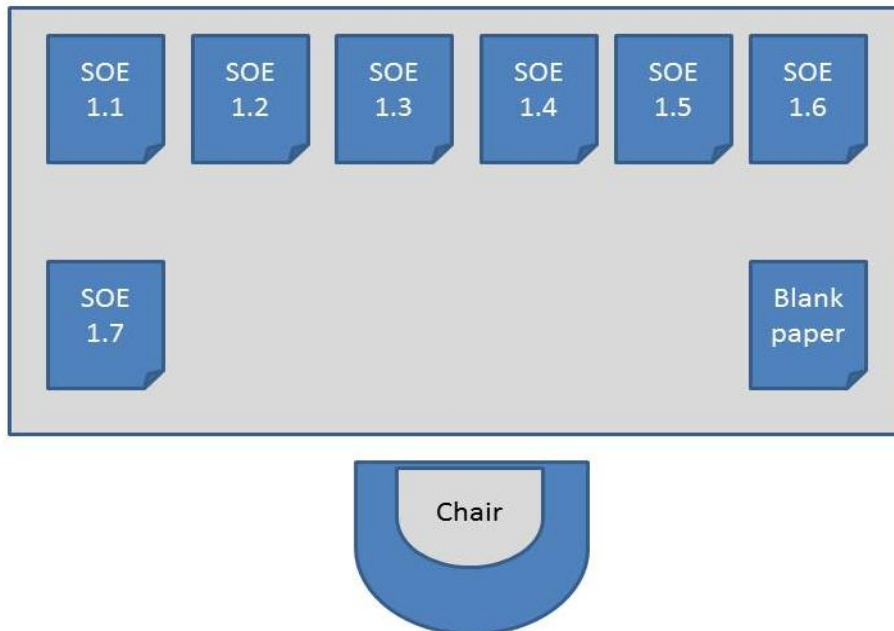


Figure 1 - CDS Level 1 SOE arrangement

Each collection of evidence generated to meet a particular SOE requires a cover sheet to allow the auditor to quickly see what SOE it relates 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 website⁷ and these will include a series of checkboxes to ensure that the organization has not missed any evidence.

Thus, if the auditor arrives and observes a missing or thin pile they can raise a query with the organization, which then have time to remedy the situation. If any SOE is completely missing, or has insufficient supporting evidence, the organization will be deemed non-compliant.

The blank paper is for the auditor to make notes upon; notes should be retained with the other evidence on completion of the audit. For further details of the CDS scheme and audit conduct, refer to the CDS Scheme Guidance document on the website, www.certifieddigitalsecurity.com

⁷ www.certifieddigitalsecurity.com