



# Certified Digital Security Level 2

## 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 2.*



*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.....                      | <b>Error! Bookmark not defined.</b> |
| Part 1 Executive Summary .....         | 4                                   |
| Part 2 Requirements for Level 1.....   | 6                                   |
| Part 3 CDS Audit Requirements .....    | 30                                  |
| Logistics for a CDS Level 2 Audit..... | 54                                  |





## 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 2 certification requires an organization to do the following:

Carry out *Background Checks on their system Administrators*; these checks are intended to ensure that the staff with the greatest capabilities on the system can be relied upon and trusted. Provide *User Training*; users should receive a minimum of 30 minutes training per year on their responsibilities and how to assist with the secure operation of the IT, this will reduce helpdesk calls and reduce security induced downtime.

The organization must have applied software updates to *its Servers and Workstations* (and major applications where possible) to ensure they are as reliable, functional and secure as the vendor can make them.

*Asset Tracking* will allow the staff and management to clearly identify what actually belongs to the organization and therefore needs to be protected or controlled. By *Enabling Basic Logging* the organization will be able to investigate and assess the cause of an incident and plan corrective action. Linked to this, a *Basic Forensic Readiness* plan will help to prevent the actions carried out to resolve a problem or incident from destroying digital evidence and important data, and aid a speedy return to normal working. *Wireless Encryption* reduces the chances of a security problem caused by improper use of the organization's wireless network. Finally, an audit of the network looking for electronic devices which do not belong to the organization followed by actions to *Prohibit the Connection of External Electronic Devices* to the system; such devices are often used to introduce unwanted or malicious software or to remove information without proper approval.

With Level 2 implemented, an organization can expect to see:

- Increased productivity as users, through their increased understanding, cause fewer security issues and are more likely to report (in good time) security problems on the system.
- A better performing, more secure and reliable system.
- A more effective response to security incidents returning the system back to normal operation faster, and lost or damaged data restored quicker.
- A clear link between financial and network assets, and security investment.





## 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](http://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.



## ***Administrator Background Checks***

**Requirement Number:** REQ 2.1

**Overview:**

The organization must have carried out background checks on its system administration staff to confirm they are who they claim to be, that they are trustworthy and as professionally qualified as they claim to be. Administrators are able to control all aspects of the network, and the organization must be able to rely upon their honesty.

**Responsible Group or Users:**

The managers responsible for the administrators, the organization's HR department, Security Office or the Head of the Organization should request or arrange the checks and only they should review the results.

**Requirement Description:**

The administrators have overall control of the network, workstations and servers and access to all the information held on it. It is vital that the organization is confident that they are honest and their trust is well-placed. This is achieved by the organization arranging for Background Checks to be carried out on all Administrators. In a CDS Audit, the auditor will not ask to see the output from the background check, they require only three items of evidence:

- ❖ That the subject gave consent,
- ❖ That the background check was conducted as outlined below, and
- ❖ That the organization is satisfied with the results of the check.

The elements which make up the background checks are detailed below. It is recommended that a national identity system is used where possible (National Identity Cards, Passport or Driving Licence), as these are already subjected to anti counterfeit mechanisms and the use of false documents of this type is usually a criminal offence:

- ❖ As this is an invasion of privacy the individual must specifically consent the information they supply being used for this purpose.
- ❖ The individual's Identity must be validated with the following information:
  - Their date and place of birth.
  - Two forms of ID - one with photograph if possible, and at least one giving a current

postal address.

- ❖ Contact the individual's claimed previous employer and confirm:
  - The individual's former status within their organization.
  - The reason for their departure from the organization.
- ❖ Check claimed professional certifications:
  - Where public records are available, check the validity of the certifications and expiry dates.
- ❖ Check claimed qualifications:
  - Check all qualifications claimed, where possible and pragmatic.
  - Check qualifications achieved in the last 5 years.
  - Conduct a pragmatic check of 'Higher' qualifications (BSc/MSc) (for example ask for degree certificate).
- ❖ Credit check:
  - Check that the individual is not in extreme debt.
  - Check that the individual does not have outstanding payments or unpaid fines against them, or is the subject of a County Court Judgment (from the local legal system).
  - Check that the individual is not currently or has recently been declared bankrupt.
  - Check that the individual is not the director of another company.

Note: Organizations are advised to only check relevant, current and valuable qualifications. School grades are not really of use to a 40 year old experienced Administrator, but are in a 21 year old newly qualified Administrator. Similarly organizations should check specific qualifications they have mandated that successful candidates must have – e.g. MCSEs, CCSE, RHCEs.

The information used for background checks may be retained by the organization, but there should be a clearly stated policy regarding the retention and where it is retained.

It is for the organization to decide who carries out this task, but records of the date of the check and the name of the individual checking must be maintained. Ideally the individual should make a written affirmation that they have confirmed the details and are satisfied with the results.

Where the Administrator is a director of another company (such as a service provider), organizations should seek assurance that the individual's other business is not competing in the same market as theirs. Furthermore, organizations should ensure that they have sole claim on the work of the individual and that another organisation is not able to claim IPR or Copyright on that work.

The organization must decide how they deal with the results of the background check.

Instances of staff claiming additional qualifications are not unheard of and whilst these can be serious it would be of greater concern if instances of hidden/undeclared criminal records or an exceptionally bad credit record (to the point of the individual having been declared bankrupt) were not considered as part of the decision as to the reliability of the individual as these may leave them susceptible to either blackmail or bribery.

If the individual has withheld information when joining the organization their integrity and honesty must be called into question. However, if the organization is content to have an individual with extensive system privileges and known issues surrounding their reliability, that is a risk decision for the organization to make.

It is the responsibility of Senior Staff, HR staff (if present) and potentially legal advisors to identify how best to deal with background check bad results.

Where staff members are promoted internally to an IT system administration role, the background check should be carried out (if not routinely done for all staff) prior to them being given the role.

Very Small (e.g. 1-3 staff) and Small organisations should still conduct this check. Sole traders and single person companies do not need to undertake this activity but should consider a means of demonstrating personal trustworthiness.

Numerous companies offer a background checking service, and the use of such services is encouraged. Details of some of these companies can be found on the CDS website.

**Benefits from Implementation:**

The organization gains some assurance that individuals with extensive network permissions are honest and trustworthy, or where there are problems these are known about and can be managed.

**Recurring? If so frequency:**

All new staff recruited to fill positions with significant responsibility, (e.g. Director, Financial Control or Network Administrator) should be checked before they are given highly privileged access to data. Individuals should be periodically checked/screened, ideally annually, by the organization or their nominated representatives.

## ***Basic Training for Users***

**Requirement Number:** REQ 2.2

**Overview:**

Users should receive training on some basic principles of Information Security so they can implement good practice in their daily activities through knowledge rather than following meaningless instructions.

**Responsible Group or Users:**

Managers should ensure that all users receive this training and that it is current and relevant to the organization. All users should attend this training.

**Requirement Description:**

All users must undergo a minimum of 30 minutes of IT and security training every calendar year. The training syllabus should cover:

- ❖ Password selection, including:
  - What constitutes a 'good' password (i.e. not using ones like Password1, qwerty, letmein, or other very weak passwords).
  - Why using family names or other easily guessed information is bad.
  - Tips for remembering passwords.
  - How to store your password securely if you cannot remember it.
- ❖ Phishing attacks. The training should demonstrate:
  - What a phishing attack is and what it is trying to achieve.
  - How to recognise a phishing attack.
  - How and when to reporting a phishing attack.
- ❖ While Anti-Virus software is installed on all workstations and servers (as per Level 1) users should be shown:
  - Why they shouldn't open unsolicited or unexpected emails.
  - Why they shouldn't open unsolicited attachments.
  - How to run an Anti-Virus scan of a file or email attachment.
  - How to confirm that their Anti -Virus software is up to date.
  - Where to get free home use Anti-Virus software (to sort out the problem at home).
- ❖ Locking their computer for breaks away from their desk, including:
  - Why they need to lock the computer.

- How to lock and unlock the computer.
- When to lock the computer (e.g. when unattended).
- When to shut the computer down (e.g. at the end of the day).
- ❖ For laptop users, users need to be made aware how attractive a laptop is to a thief. To prevent them being the victim of crime, they should be shown how to secure their laptop assets:
  - When travelling away, such as staying in a hotel.
  - When travelling or on foot away from the office.
  - When at their home/place of residence.

The training is to last at least 30 minutes per year, but can be any combination of:

- Written guides and exercises.
- Trainer-led training.
- Online or other computer-based training.

All staff should be required to undertake instructor-led training within 3 months of starting (where practicable) or within 1 month if an online or a Computer Based Training (CBT) is used. However, as with any training, the sooner the better.

Training records should be retained for all staff, and these should include:

- ❖ The person's name.
- ❖ The date they joined the organization
- ❖ The Training Type (CBT, Instructor-led etc).
- ❖ The Trainer or source of the training (the organization or instructor's name if conducted in-house).
- ❖ The date of the training.
- ❖ The result of any associated exam.
- ❖ Validity period of exam.

Records can be online or paperwork.

The training requirement can be linked to the annual acceptance of the Organization's Security Policy and Acceptable Use Policy (as per Level 1). Holders of nationally or internationally recognized schemes that meet the training requirements do not need to undertake the initial training. They are not excused refresher training.

#### **Benefits from Implementation:**

Users are more aware of their responsibilities and the means of complying with the

organization's policies. They are less likely to embarrass the organization, attract unwanted media attention or cause either themselves or the Directors/Owners/Senior Staff to face legal action.

**Recurring? If so frequency:**

The training content and the subjects covered should be reviewed:

- ❖ At least annually.
- ❖ 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 information as a result of user activity.

**How to implement this:**

The training need not be a full blown course. It can be a series of short presentations, or videos delivered internally or via internet based training organizations.

Organizations may wish to contract this out, write their own or even check out some of the excellent security videos on the Internet (CDS itself provides a series of short videos on YouTube <http://www.youtube.com/user/CertifiedDigitalSy> ) and by sending out a link to videos and requiring staff watch them (individually or in meeting rooms), organizations can undertake this important aspect of information and network security training in a cost effective manner.

Equally, many larger organizations require staff to undertake other annual mandatory training, and the topics necessary to comply with REQ 2.2 can be added to the overall package (again, either instructor-led, slide driven, Computer Based Training or video based).

## *Server Patching*

**Requirement Number:** REQ 2.3

**Overview:**

Applying updates issued by the Operating System vendors will make servers more stable, and will correct known flaws and security weaknesses in the software. This will reduce the risk of a network attack being successful.

**Responsible Group or Users:**

Server Administrators should implement the update activities. The administrator, in collaboration with the system owner or senior manager, should develop the Update Policy that will set out what updating activities should be undertaken and when.

**Requirement Description:**

The organization should have a documented server update strategy/policy.

The policy should state how (automatically or manually), when (evenings, weekends or a particular day of the week) and how often (weekly, monthly bi-monthly) the servers' software and firmware (built-in hardware that has software which can be changed) should be updated.

All Servers must be updated regularly. Importantly, no server should operate for more than 3 months without any available update patches being applied. No security barrier (such as a firewall, secure switch or proxy server) should operate for more than 1 month without any available update patches being applied.

Where possible servers should be set to update automatically whenever a software vendor issues an update to the operating system or critical software such as business-dependant programs.

Where servers are running software which cannot be updated automatically, administrators should regularly check with the software vendors to see if an update has been issued. This should then be manually applied to the relevant servers.

Where updates are not available or cannot be implemented, the manufacturer's or vendor's recommended alternative solution should be implemented (where possible and practical).

The patching strategy must identify the organization's assessments of the priority in which



servers are to be updated.

**Benefits from Implementation:**

- ❖ Greater productivity as servers are more likely to remain stable and will perform better.
- ❖ Resistance to internet-based and internal hacking attacks.
- ❖ Greater reliability from in use equipment communicating with the server.

**Recurring? If so frequency:**

- ❖ Organizations should install server updates on a regular basis as they become available.
- ❖ No available server updates should remain outstanding for more than 3 months after the software vendors have issued them.

**How to implement this:**

The records of manually implemented updates can be maintained in an electronic spread sheet. Periodic 'snapshots' should be taken of the lists of automatically installed updates.



## ***Workstation Patching***

**Requirement Number:** REQ 2.4

**Overview:**

Applying updates issued by the Operating System vendors will make workstations more stable, and will correct known flaws and security weaknesses in the software. This will reduce the risk of a network attack being successful.

**Responsible Group or Users:**

Workstation Administrators should implement the update activities. The administrator, in collaboration with the system owner or senior manager, should develop the Update Policy that will set out what updating activities should be undertaken and when.

**Requirement Description:**

This requirement applies to all non-server computers; including tablet, laptop and desktop 'PCs' although the generic term used is workstation.

The organization should have a documented workstation update strategy/policy.

The policy should state how (automatically or manually), when (evenings, weekends or a particular day of the week) and how often (weekly, monthly bi-monthly) the workstations' software and firmware (built-in hardware that has software which can be changed) should be updated.

All workstations must be updated regularly. Importantly, no workstation should operate for more than 3 months without any available update patches being applied.

Where possible workstations should be set to update automatically whenever a software vendor issues an update to the operating system or critical software such as business-dependant programs. Tablets and laptops in particular should be set to update whenever they are re-connected to the network.

Where workstations are running software which cannot be updated automatically, administrators should regularly check with the software vendors to see if an update has been issued. This should then be manually applied to the relevant workstations.



Where updates are not available or cannot be implemented, the manufacturer's or vendor's recommended alternative solution should be implemented (where possible and practical).

The patching strategy must identify the organization's assessments of the priority in which tablets, laptops and PCs are to be updated.

**Benefits from Implementation:**

Staff will be more productive as correctly updated workstations operate better since many updates improve stability and performance. Security updates make workstations less susceptible to exploits from worms and browser phishing attacks.

**Recurring? If so frequency:**

Ideally, workstations should be checked to ensure that available updates have been applied on a monthly basis and should go no longer than 3 months from updates being released to being implemented on systems.



## Management of Assets

**Requirement Number:** REQ 2.5

**Overview:**

The Organization should know what assets and devices it has that hold and process data; these assets should be recorded and managed throughout their lifecycle (purchase, use and disposal).

**Responsible Group or Users:** A nominated person or group should be responsible for cataloguing assets and devices, and recording their approved location or user.

**Requirement Description:**

The organization should maintain a register of its assets and devices so it can account for their location or the person they are assigned to.

The asset register should be supported by:

- ❖ A policy that sets the value of assets in the organization (in financial and/or business impact terms).
- ❖ Clearly stated responsibilities for staff with respect to how registered assets and devices are identified and handled.
- ❖ A method of marking, or indicating ownership of, the asset or device, or its importance/value to the organization. **Note;** there is a fine line between indicating value and placing a 'steal me, I am valuable' label on it.
  - For example, laptops do not need to be physically labeled with the organization's name and address on the lid, or a description of the laptop's function (such as 'Finance Laptop'); there are more subtle ways such as labeling the base of the device with an abbreviated code which is understood within the Organization.
- ❖ Limiting the ability to access and update the register to as few staff as practicable; those staff should be trusted and should have been background checked.

The register should list the following information about each asset or device:

- ❖ The manufacturer's serial number of the asset.
- ❖ A brief description of the asset.
- ❖ The normal location of the asset (or, in the case of mobile IT equipment, the name of the person to whom it has been issued).

- ❖ The Organization's unique identifier for the device. Unique identifiers can be gathered using operating system auditing software, or can be manually generated using an in-house numbering or lettering scheme. Other methods could include:
  - MAC address of the LAN network card and the WLAN card.
  - The operating system host name (Windows or Unix/Linux).
- ❖ Date of disposal of the asset. this should link to either the person who disposed of it, or a separate record of disposal (sales receipt, destruction certificate).

**Benefits from Implementation:**

By better understanding what assets an Organization holds it can calculate their value for insurance and loss claims purposes.

The Organization can plan its security more effectively, targeting its efforts at known important business assets. It will also aid in the optimization of resources such as buying only the software necessary for the business, and maximize the reuse of assets by reallocating unused assets to new tasks.

Finally, an organization may be better placed to identify, respond to, and control an incident of theft, damage or loss.

**Recurring? If so frequency:**

The asset register should be internally audited on a 6 monthly basis, but should be regularly maintained, with updates to the register occurring within a month of any changes to asset holdings (loss, theft, purchase or disposal).

The asset register should be reviewed by Senior Management at least once per year.

## ***Enable System Logging***

**Requirement Number:** REQ 2.6

**Overview:**

System Logs provide useful information that can aid problem resolution, incident response and legal prosecutions of groups or individuals that attack or damage IT Systems, or steal information from them.

**Responsible Group or Users:**

System Administrators or Server Operators/Managers.

**Requirement Description:**

Logs are used to assist in resolving problems and aid post incident (forensic) analysis. A policy should be published detailing what logs are implemented, who checks them and how frequently they are checked. To ensure that the necessary logs are available, administrators are to enable system logging (where available) of the following actions on servers which provide access to data and resources:

- ❖ The creation of any user, service or system account.
- ❖ The removal or suspension of any account.
- ❖ Any change of any account's permissions or capabilities (e.g. a normal user being increased to Administrator).
- ❖ All failed logon attempts.

Where Virtual Private Networks are used for remote workers, the logging should include the username used to gain access to the network and, if possible, the remote IP address they connected from.

These logs are to be kept for at least 1 year and ideally removed onto CD/DVD/Blu-Ray media on a regular basis. "Regular" means a frequency which will prevent logs being lost as a result of being erased or overwritten due to their size exceeding the system's capacity to store them.

Administrators should check logs on at least a weekly (ideally a daily) basis. All reviews should be recorded in a log or notebook to prevent duplication of effort.



In addition, the following non - security logging should be enabled, reviewed and archived on a regular basis:

- ❖ Application logs.
- ❖ Backup logs.
- ❖ Replication or synchronization logs.
- ❖ Non-security patching and update logs.

A written policy should be produced detailing the standard of logging to be implemented, the frequency of log reviews, and the method and frequency of archiving them.

**Benefits from Implementation:**

Administrative staff is better able to resolve network and system problems using the additional information provided by logs.

Frequent reviews of the logs may provide indications of developing problems, the need for early corrective actions, or signs of an ongoing attack or security problem on the system.

Logging provides evidence of due diligence on the part of the organization in the event of legal action resulting from a data loss or breach.

**Recurring? If so frequency:**

Logs should be constantly updated. Logs should be archived regularly; it is recommended that this is done weekly, but should never be any longer than monthly. Logs should be reviewed daily, but weekly may be more appropriate on small networks. In large organizations with dedicated Systems Administrators, logs should be reviewed and archived on a daily basis.



## *Forensic Readiness Plan*

**Requirement Number:** REQ 2.7

**Overview:**

Security incidents and IT disasters can occur for many different reasons; business continuity is often dependent upon being able to restore data to affected systems. Investigation of the causes of an incident can also require evidence to be gathered to a standard acceptable in a court of law. By being able to call upon experts to recover data an organization can reduce the impact of a loss, speed up the recovery of the data and, if necessary assist in the prosecution of offenders.

**Responsible Group or Users:** System Administrators

**Requirement Description:**

Digital forensics is a specialist subject and one that requires the practitioner to be skilled, experienced and equipped to undertake the task correctly. Organizations should be aware of how they should deal with an incident so as to minimize the loss of data or digital evidence which will reduce delays in recovering to normal operations.

Therefore the organization should have a plan covering:

- ❖ Where they can obtain digital forensic support from (contact telephone numbers, fax etc).
- ❖ The actions to take to prevent suspect items such as computers, laptops, accounts or servers from being further interfered with.

The plan does not need to be long or detailed, but should provide at least enough information to allow an administrator to undertake the first steps to protecting evidence without jeopardizing the chances of recovery. The brief should be in hardcopy so the plan can be initiated following a suspected attack without the attacker being alerted to the organization's suspicions; this will also prevent the plan being unavailable in the event of loss of the network

The communication methods listed in the plan should enable the reader to contact the digital forensics response without using a network technology i.e. a VOIP phone, emails or other open communications.

**Benefits from Implementation:**

The organization is better able to recover data from assets following accidents (user error in



deleting critical files for example), viruses or catastrophic damage to equipment (e.g. fire or flood damage). The organization will also be able to react correctly to hacking attacks ensuring evidence is preserved so the option of legal restitution is available.

**Recurring? If so frequency:**

The forensic readiness plan should be updated annually, or whenever there is a change of service provider; contact details should be checked every 6 months.



## *Reducing the Risk from Wireless LANs*

**Requirement Number:** REQ 2.8

**Overview:**

Wireless networks (including 802.11a/b/g/n networks and Bluetooth PicoNets) allow access to internal network resources. Unless operating a public Hotspot, there should be no unsecured Wireless Access Points, and the means of securing should be a recognized strong method.

**Responsible Group or Users:**

Administrators are to check that all wireless devices have been set correctly and are able to use strong encryption.

**Requirement Description:**

Wireless connections if incorrectly located or configured will allow unauthorized access to an organization's resources, business information and data. Open or unsecured access points allow easy unauthorized access.

- ❖ There must be no unencrypted Wireless network that connects to the organization's normal working network LAN.
- ❖ WPA2 encryption is to be implemented wherever the technology allows.
- ❖ Where WPA2 is not possible WPA is to be implemented.
- ❖ Where WPA is not possible, the device cannot be permitted to connect to the normal working network.
- ❖ WEP is not to be used under any circumstances.
- ❖ Other authentication methods should be considered where possible (e.g. RADIUS).
- ❖ If using Pre Shared Keys (PSK), also known as WPA(Personal), strong passwords are to be used; at least 20 characters in length, and include upper and lower case letters together with punctuation and special characters (!\$%&@).
- ❖ High powered free Internet connections that are shared out by Wireless Access Points are strongly discouraged.
- ❖ Where a guest network is provided for visitors or members of the public, it must not share any of the security barriers provided for the organization's normal working network (to prevent it being used for reconnaissance of the network's security barriers). Guest networks must be low powered, limited to locations where the authorized guests are located (i.e not available throughout the premises) and must use a closed channel



(VPN) to access services outside the organization's Firewall/Perimeter.

**Benefits from Implementation:**

Removing free wireless internet connections removes potential distractions from the workplace, prevents others using the internet in the organization's name, and so reduces the risk of a PR disaster following the abuse of the provided connection.

Limiting wireless and removing poorly secured devices (those supporting only WEP) will increase the security of a network. The move to WPA2 with strong authentication will significantly reduce the risk of attack.

**Recurring? If so frequency:**

The Access Point, RADIUS server and Authenticator's configuration should be checked every 6 months.

Network Pre-Shared Keys should be changed annually.



## *Check for Unauthorized System Hardware*

**Requirement Number:** REQ 2.9

**Overview:**

The organization should only have its own equipment on the network. Allowing users to use external devices or their own equipment (also known as Rogue Devices) provides an uncontrolled network entry point that can bypass other security controls. A check should be carried out for any rogue devices connected to the network.

**Responsible Group or Users:**

Senior Staff must endorse this update to the security policy and allow only equipment owned by the organization to be used to process the organization's information or connect to the organization's network.

System Administrators will implement the policy and conduct checks for devices being attached (or official equipment being removed).

**Requirement Description:**

Scans or checks of the network for the connection of rogue devices must be carried out. The scan or check should be checked against those devices recorded in the asset register (**REQ 2.5**), and any anomalies investigated.

If an unauthorized device is discovered it must be disconnected from the network. Before being removed from the organization the device should be checked for the presence of any of the organization's data; any data discovered on a rogue device should be copied off and then wiped from the device (see CDS website for details of wiping standards).

If the organization uses 802.1x asset authentication and Network Access Control, logs from these should be checked for Rogue devices.

If the organization is under 100 systems but has no 802.1x authentication, then 6 monthly audits of the network should be carried out to check that only authorized devices are connected.

Software can be used to automate this and the CDS website carries a list of software that may be of assistance (CDS make no claims as to the suitability of software).

Devices that should not be connected to the organization's network are:

- ❖ Personal Laptops.

- ❖ Business laptops from external companies or other organizations (other than to a purpose-built 'guest' network).
- ❖ Personal PDAs and PalmTops or similar mobile devices, including MP3/MP4 players and cameras.
- ❖ Any personal or private network switch or hub devices.
- ❖ (unauthorized or rogue) Wireless Access Points.
- ❖ Personal or external printers.
- ❖ Dictation Devices (that connect via USB).
- ❖ Personal Mobile phones that connect via USB – if users need to charge mobile phones they should bring a charger that connects to the mains. (This should also be approved by management).
- ❖ External Hard Drives or media writers (CD/DVD/Blu-Ray).

**Benefits from Implementation:**

By removing private equipment from the network, the organization will establish greater control over the means by which data can enter and exit their networks.

Allowing only the organization's equipment onto the network will reduce the risks that a departing member of staff might remove critical and/or valuable IPR data on their personal system or device when they leave.

**Recurring? If so frequency:**

The network should be scanned or checked every 6 months.

The network should also be re-checked if there is an information security breach.

Ideally the network check should also be conducted following any updates to the network infrastructure (new servers, additional cabling, implementation of wireless etc.) and before any new client's data is added to the network.



# 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](http://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 proof<sup>1</sup> necessary to prove the requirements<sup>2</sup> 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;

---

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

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



- ❖ 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 audit<sup>3</sup>. 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 3<sup>rd</sup> parties to allow verification and validation of the organization's achievement.

---

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



### **IF THE EVIDENCE IS NOT CORRECT OR 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.



## ***Background Checks on Administrators***

**Statement Of Evidence(SOE) Number:** SOE 2.1

**Overview:**

This audit requirement is to confirm that the organization has conducted background checks on the administrators and that they are satisfied with the results of these checks.

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

**SOE 2.1.a.**

The organization must produce a list of the administrators on the network. Note: The number of administrator users must be similar to that contained in the **SOE 1.4.c.**

**SOE 2.1.b.**

The organization must produce letters signed by each administrator agreeing to have the background check undertaken. The letter must contain permissions for the specific checks required by **SOE 2.1.c.**

**SOE 2.1.c.**

The organization must produce a document signed by either the HR manager, Director or a member of the senior staff that confirms:

- ❖ The names of the individuals that were checked.
- ❖ The nature of the checks conducted, these must include:
  - Personal Identity.
  - Former Employer's Reference
  - Qualifications.
  - Financial status.
- ❖ That the organization is content with the results of these checks and that they are satisfied with the trustworthiness of the network administration staff detailed in the document.

**SOE 2.1.d.**

The organization must state if it has retained the information that was submitted and subsequently returned and if so where it is kept.

**How this can be generated:**

Lists of administrators can be generated by listing those in the Administrator or root workgroup. There are several ways that checks can be undertaken: The organization can subcontract the whole activity, seek the use of providers or make use of various information providers that will undertake separate checks that can be coordinated by an individual within the organization.

The letter for the individual agreeing to the check should be part of the form used to gather the additional information necessary for the detailed checks.

The document of confirmation that the check has been undertaken and that the organization is satisfied with the results need only be a single page in length. This letter must be signed by a senior member of staff and must detail the names of the individuals checked prior to the date of the signature on the letter.

**Details of the compliance Criteria for SOE 2.1:**

**SOE 2.1** 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 list of administrators required by **SOE 2.1.a**.

**Criterion 2:**

Support any change in staff numbers between **SOE 1.4.c**, **SOE 2.1.a** and **SOE 2.1.b** (i.e. if 6 administrators are listed in **SOE 1.4.c** the permission for checks must include all 6 administrators).

**Criterion 3:**

Presentation of an agreement for each administrator listed at **SOE 2.1.a**. that they agree to the check being carried out.

**Criterion 4:**

The organization must have conducted all of the checks listed at **SOE 2.1.c**. on all administrators listed at **SOE 2.1.a**.

**Criterion 5:**

Presentation of a document that lists the names of the individuals checked, the nature of the checks carried out and a clear statement to the effect that the organization is satisfied with the results. This document must be signed by a senior person in the organization.

## ***Basic Training for Users***

**Statement Of Evidence (SOE) Number:** SOE 2.2

**Overview:**

This is to confirm that the users have undergone the required duration of training and that the training covered the required material and specified subjects.

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

**SOE 2.2.a.**

The organization must produce a list of IT system users and have a training record for each member of the user community.

**SOE 2.2.b.**

The training record must detail:

- ❖ The User's name.
- ❖ When they started in the organization.
- ❖ The type of training e.g., Instructor led, On Line or Demand, Assessed Work Study Books.
- ❖ The training course's provider/vendor/author or source.
- ❖ The dates they have conducted various training activities.
- ❖ The duration of the training (days, hours or minutes)
- ❖ The result of any exam.
- ❖ The validity period of the exam.

**SOE 2.2.c.**

The syllabus for an outsourced course must be provided, and must show that it covers the required subjects to be claimed against this CDS Level 2.

**SOE 2.2.d.**

Each user must have completed the following in their training:

- ❖ Password selection, including sub topics of:
  - Good password selection (i.e. not using ones like Password1, qwerty, letmein, or other very weak passwords).
  - Why using family names etc is bad.
  - Tips to remember passwords.
  - How to store your password securely if you cannot remember it.
- ❖ Phishing attacks:
  - What a phishing attack is and what it is trying to achieve.
  - How to Spot a phishing attack.
  - How and when to reporting a phishing attack.
- ❖ Anti Virus:

- Why they shouldn't open unsolicited emails.
- Why they shouldn't opening unsolicited attachments.
- How to save a file to the desktop and run an AV scan of it.
- How to check the Anti Virus software is up to date.
- Where to get free home use Anti Virus software (to sort out the problem at home).
- ❖ Locking their system:
  - How to lock the computer.
  - How to unlock the computer.
  - When to lock the computer (e.g. when unattended).
  - When to shut the computer down (e.g. at the end of the day).
- ❖ Physical protection of their laptops or mobile assets:
  - When travelling away, such as staying in a hotel.
  - When travelling in the car or away from the office.
  - When at their home/place of residence.

#### **SOE 2.2.e**

Training records must show that all staff undertook the training within 3 months of starting where it is instructor led (unless there are no available courses in this period in which case next available dates must be shown) and within 1 month if an online or a Computer Based Training (CBT) course is used.

#### **SOE 2.2.f.**

Numbers of users that have undertaken this training must be at least **90%** of the total user numbers.

#### **SOE 2.2.g.**

No user is to miss training for more than 18 months, i.e. they are not to feature in the list of users not receiving training that year for more than 1 CDS audit (on the second audit they will cause the organization to be non-compliant).

#### **How this can be generated:**

If the organization does not have a training department or is looking to start holding such records then the following maybe of use.

A spreadsheet program can be used to record all the required information with users listed in the first column and the training events listed in the top row. A date placed against a user under the column indicating the course or training event they have attended is sufficient.

External training providers will provide syllabi upon request. If the course was instructor led or generated internally, include the slides or materials used to allow the auditor to confirm that they meet all the requirements of **SOE 2.2.d.**

**Details of the compliance Criteria for SOE 2.2:**

**SOE 2.2** 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:**

Presentation of a full hard copy of IT system users in the organization (this is also required for **SOE 1.4.c.** so should have already been generated for audit).

**Criterion 2:**

Production of a document or training record for each user - required at **SOE 2.2.a.**

**Criterion 3:**

Evidence must show that the training undertaken by the individuals included the subjects detailed at **SOE 2.2.d.**

**Criterion 4:**

At least 90% of the user base has undertaken the training.

**Criterion 5:**

No user of the system has gone without training for more than 12 months.

**Notes:**

For low cost training there are numerous internet podcasts and webcasts. These can be used by an organization, allowing users to undertake several short web/pod casts to achieve the overall training requirement.

A series of short training films covering many of the subjects to meet this requirement can be found on the CDS Channel at [www.youtube.com](http://www.youtube.com).

## Server Patching

**Statement Of Evidence (SOE) Number:** SOE 2.3

**Overview:**

This will check that the organization is carrying out updates to their servers.

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

**SOE 2.3.a.**

The organization must present its documented server updating strategy/policy. The strategy must cover the following areas:

- ❖ How the updates will be carried out (manually or automatically)
- ❖ When the updates will be carried out.
- ❖ How often updates are to be done.
- ❖ Identify which software cannot be automatically updated, and why.
- ❖ Whether any priority is to be applied to server updates, and what the priority is.

**SOE 2.3.b.**

The organization must provide a list of Servers in the network. Security Barriers (e.g. firewalls and proxy servers) are considered servers.

**SOE 2.3.c.**

All Servers must be updated regularly. Updates must be applied within 3 months of issue from the vendor. Security barriers must be updated within 1 month of issue from the vendor. This evidence must have been prepared within 3 weeks of the date of the audit.

**SOE 2.3.d.**

Where the organization is not able to implement an update (for example because other software on the system is not compatible), the organization is to record the fact, and provide written details of any alternative measures implemented to reduce the risks of a missing update.

**How this can be generated:**

An electronic spreadsheet can be used for manual update records or automated update management logs can be used to show automatic updates e.g. on Microsoft networks the Windows Software Update Service (WSUS) may be used to monitor and evidence system updates for servers (and clients).



Endorsements should be in the form of either a signature block on the front of the Update Policy that is then signed by some senior manager, or a forward by a notable individual in the organization that states the need for the policy and their endorsement of the requirements contained within it.

**Details of the compliance Criteria for SOE 2.3:**

**SOE 2.3** 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 organization's Patching Strategy as described in **SOE 2.3.a**, that has been endorsed by Senior Management.

**Criterion 2:**

Production of a list of Servers and Security Barriers in the organization as described in **SOE 2.3.b**.

**Criterion 3:**

Production of a record showing the update status of all servers (that are detailed in **SOE 2.3.b**). Evidence must be no older than 3 weeks prior to the date of the audit.

**Criterion 4:**

Production of explanatory notes as to why any updates have not been applied and details of any alternative measures implemented to reduce the risks of the missing updates.



## Workstation Patching

**Statement Of Evidence (SOE) Number:** SOE 2.4

**Overview:**

This will check that the organization is carrying out updates to their workstations.

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

**SOE 2.4.a.**

The organization must present its documented workstation patching strategy/policy. The strategy must cover the following areas:

- ❖ How the updates will be carried out (manually or automatically)
- ❖ When the updates will be carried out.
- ❖ How often updates are to be done.
- ❖ Identify which software cannot be automatically updated, and why.
- ❖ Whether any priority is to be applied to server updates, and what the priority is.

**SOE 2.4.b.**

The organization must provide a list of workstations in the network. Workstation's include laptops, desktops, notebooks, and netbooks.

**SOE 2.4.c.**

All workstations must be updated regularly. Updates must be applied within 3 months of issue from the vendor.

Note the word 'update' is taken to include patches, Service Packs, Rollup Patches.

**SOE 2.4.d.**

Where the organization is not able to implement an update (for example because other software on the system is not compatible), the organization is to record the fact, and provide written details of any alternative measures implemented to reduce the risks of the missing update.

**How this evidence may be generated:**

An electronic spreadsheet can be used for manual update records or automated update management logs can be used to show automatic updates e.g. on Microsoft networks the Windows Software Update Service (WSUS) may be used to monitor and evidence system updates for servers (and clients).



Endorsements should be in the form of either a signature block on the front of the Policy that is then signed by a senior manager, or a foreword by a notable individual in the organization that states the need for the policy and their the requirements contained within it.

**Details of the compliance Criteria for SOE 2.4:**

**SOE 2.4** 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 full hard copy of the organization's Patching Strategy as described in **SOE 2.4.a**, that has been endorsed by Senior Management.

**Criterion 2:**

Production of a list of workstations in the organization as described in **SOE 2.4.b**.

**Criterion 3:**

Production of a record showing the update status of all workstations (that are detailed in **SOE 2.4.b**). Evidence must be no older than 3 weeks prior to the date of the audit.

**Criterion 4:**

Production of explanatory notes as to why any updates have not been applied and details of any alternative measures implemented to reduce the risks of the missing updates.



## *Management of Assets*

### Statement Of Evidence (SOE) Number: SOE 2.5

#### Overview:

This is to confirm that the organization has taken steps to identify what assets are connected to its network and therefore may contain valuable digital information.

#### Statement Of Evidence (SOE) Description:

The organization must maintain a register of its assets so it can account for their location and understand the security required to defend them.

#### SOE 2.5.a.

The organization must present an Asset Management Policy document that details the following (note this should be part of the organization's Security Policy document as required by REQ 1.1):

- ❖ How valuable information is classified (in either financial value and /or in terms of impact to the business).
- ❖ Clearly stated responsibilities for staff with respect to how registered assets and devices are identified and handled.
- ❖ A method of marking or indicating ownership of the asset or its internal value to the organization.
- ❖ Identifies the staff (by post, if not name) able to update the register.

#### SOE 2.5.b.

The organization must present an asset register that includes the following information:

- ❖ The manufacturer's serial number of the asset.
- ❖ The description of the asset.
- ❖ The location of the asset (or the name of the person to whom it has been issued in the case of mobile IT equipment).
- ❖ A unique identifier for the device.

#### SOE 2.5.c.

The asset register must be reviewed by Senior Management and signed at intervals not exceeding 12 months. In the case of a newly instituted register, there must be a clear indication that reviews are due every 6 months with an annual sign-off by Senior Management.

**How this evidence may be generated:**

For small organizations with fewer than 15-20 workstations, screen shots of installed software assets will suffice (screen shots can be used for larger networks however above 10 workstations it can be cumbersome to manage). For larger organizations a report from the central management suite detailing the various, settings and updates or versions etc will be acceptable.

Hardware assets should be recorded in a log, to be produced in hard copy for the audit.

**Details of the compliance Criteria for SOE 2.5:**

**SOE 2.5** 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:**

Production of the 'Asset Management Policy' as detailed at **SOE 2.5.a**.

**Criterion 2:**

Production of the 'Asset Register'.

**Criterion 3:**

Demonstrate how the assets are utilised (i.e. having 100 users but only 50 laptops in the asset register). This requires a comparison of user accounts from **SOE 2.2.a** against the asset register. If assets are shared by multiple users, this fact must be mentioned in the Asset Management Policy.

**Criterion 4:**

Produce evidence of review on a 6 monthly basis, and Senior Management review annually as described at **SOE 2.5.c**.

## ***Enable System Logging***

**Statement Of Evidence (SOE) Number:** SOE 2.6

**Overview:**

This is to check that the organization has basic system logging enabled, that they can track security relevant activities within their system and that they carry out periodic examination of the logs.

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

**SOE 2.6.a.**

The log settings for each server must be printed for review by the auditor. In a Microsoft Windows Domain environment, this will be a printout of the GPOs that enable the logging on all Domain Controllers and Member Servers. On Unix systems, the auditing/logging settings will usually need to be printed from each server. These server numbers and types will be cross checked against **SOE 2.2.a.**

**SOE 2.6.b.**

The printed logs must include the following:

- ❖ Any user, service or system account creation.
- ❖ The deletion or suspension of any account.
- ❖ Change of any account's permissions or capabilities.
- ❖ Failed logon attempts.
- ❖ The username used to authenticate remote users via VPNs (where applicable) and if possible the remote IP address they connected from.

As well as system logs the following logs are to be provided for all servers:

- ❖ Application logs.
- ❖ Backup logs.
- ❖ Replication or synchronization logs.

**SOE 2.6.c.**

The documented process for how logs are managed and archived is to be presented to the Auditor. A record of the archived logs is to be presented to the auditor (the auditor does not need the logs, only the records of them being archived).

**SOE 2.6.d.**

The Administrator's record of checking logs must be presented. This must show that audit logs are checked on a weekly basis (as a minimum). By weekly it is meant that no

more than 9 working days has passed between a check of the logs.

**How this can be generated:**

The log settings should be system generated.

The record of log checking can be a simple ruled notebook or an excel spreadsheet

**Details of the compliance Criteria for SOE 2.6:**

**SOE 2.6** 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 Logging settings for each server.

**Criterion 2:**

Logging settings show that the organization is logging all the items described at **SOE 2.6.b.**

**Criterion 3:**

Presentation of a process document describing how and where and by whom logs are archived (as required at **SOE 2.6.c.**).

**Criterion 4:**

Presentation of a record of the checks carried out on the logs.

**Criterion 5:**

The organization must show that the logs have been reviewed on a regular basis not exceeding 9 days between reviews.

## ***Basic Forensic Readiness Plan***

**Statement Of Evidence (SOE) Number:** SOE 2.7

**Overview:**

This is to check that the organization has a Basic Forensic Readiness Plan.

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

**SOE 2.7.a.**

Organizations must present their Basic Forensic Readiness Plan. This must cover:

- ❖ Where they can obtain digital forensic support from (contact telephone numbers).
- ❖ What actions to take to quarantine suspect items, computers, laptops, accounts or servers from further interference.

**SOE 2.7.b.**

The plan should be routinely held in hardcopy to ensure the organization can call it up without using IT.

**SOE 2.7.c**

The communication methods listed in the plan must enable the reader to contact the digital forensics response without using a network technology i.e. a VOIP phone, emails or other open communications.

**How this can be generated:**

The plan can be a written brief, notice or complete document. An example of a Forensic Readiness Plan can also be found on the CDS Website.

**Details of the compliance Criteria for SOE 2.7:**

**SOE 2.7** 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 Basic Forensic Readiness Plan as described at **SOE 2.7.a.**

**Criterion 2:**

The plan is maintained in hardcopy. This is detailed at **SOE 2.7.b.**

**Criterion 3:**

There must be a means within the plan for non-network based communication to contact the forensic specialist as required by **SOE 2.7.c**

## *Reducing the Risk from Wireless LANs*

**Statement Of Evidence (SOE) Number:** SOE 2.8

**Overview:**

This is to check that the organization has implemented wireless security measures in all areas where this technology is utilized.

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

**SOE 2.8.a.**

A list of wireless access points is to be maintained and presented for audit with a diagram of the LAN connectivity that shows all the wireless access points. This is to detail the following:

- ❖ The name of the access point.
- ❖ The SSID of the WLAN.
- ❖ The encryption used (either: none, WEP, WPA, WPA2).
- ❖ The Authentication used if any (e.g. 802.1x).
- ❖ RADIUS implementation type if used.

It must show that:

- ❖ There are no unencrypted Wireless LAN connections to the organization's production LAN.
- ❖ WPA2 encryption is implemented wherever the technology allows.
- ❖ WPA is to implemented where WPA2 is not possible.

NOTE: No device utilizing WEP is to be connected to the organization's production system. WEP security can be broken and data released in approximately 10 minutes.

**SOE 2.8.b.**

The use of strong passwords for Pre-shared Keys is to be demonstrated to the auditor (although he is not to see the actual password only the action of entering the password to a client trying to connect) The demonstration must show that passwords are at least 20 characters in length, and include at least one of each of the following:

- ❖ An upper case letter.
- ❖ A lower case letter.
- ❖ An item of punctuation or a special character.

**SOE 2.8.c.**

A diagram of any connectivity made available for visitors or the public must be provided at the audit. The diagram must show that this type of connection is low power and using a

closed channel (VPN) to access services outside the organization's Firewall/Perimeter.

**SOE 2.8.d.**

Where 802.1x is used to implement the encryption for wireless networks the key exchange encryption policy from the Authentication Server or RADIUS server that generates the keys is to be presented to the auditor.

**How this can be generated:**

The administrator should provide a list of all Access Points that they manage and configure. This can be a document or a spreadsheet. If a management tool is used to control passwords, authentication or some other features, then printouts or screenshots of these can be included. Password information should be obscured if it is readable in screenshots or printouts.

The diagrams can be drawn using anything from pen and paper to MS Visio, the method is not important only the quality of the information conveyed.

**Details of the compliance Criteria for SOE 2.8:**

**SOE 2.8** 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 numbers of access points and a diagram of LAN connectivity as required at **SOE 2.8.a.**

**Criterion 2:**

There must be no unencrypted or WEP encrypted Wireless Links.

**Criterion 3:**

The password required at **SOE 2.8.b.** must meet the required criteria (This is regardless of the implementation – PSK or 801.1x/RADIUS).

**Criterion 4:**

Guest or public connections must not share the production network without tunneling it out of the LAN to the internet. This is described in **SOE 2.8.c.**

## Check for Unauthorized Hardware

Statement Of Evidence (SOE) Number: SOE 2.9

**Overview:**

This is to check that the organization has a policy for regular checks for unauthorized hardware.

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

**SOE 2.9.a.**

The Organization must present a policy requiring that Administrators regularly (at least annually but ideally weekly or monthly) scan and monitor their network for the connection of rogue devices. The policy must also show:

- ❖ The types of device it considers to be unauthorized.
- ❖ That unauthorized devices are removed from the network on discovery.
- ❖ That any data is removed and the device is wiped before disposal.

**SOE 2.9.b.**

The Organization must present the output from the last two scans (if in the first year of CDS, one scan is sufficient). Output must not be dated more than 6 months apart.

**SOE 2.9.c.**

Scans must indicate that the whole subnet was scanned, including wireless and VPN subnets (cross check with **SOE 2.8.a.**).

**How this can be generated:**

The scan can be conducted over a period of time as long as something unique is used to index the results (e.g. MAC Address). The scan can be conducted using LAN management and discovery software, security software or can be conducted manually (on small LANs) by checking end points on network switches. The key is being able to see what should be on the network and how this is distinguished from what is not.

**Details of the compliance Criteria for SOE 2.9:**

**SOE 2.9** 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 hard copy policy as required at SOE 2.9.a.

**Criterion 2:**

The policy must include what response it will take to unauthorized items of equipment discovered during scans.



**Criterion 3:**

Presentation of a previous scan of the LAN that shows all the devices connected to the LAN at that time.

**Criterion 4:**

Presented scan results are no older than 6 months or are dated more than 6 months between scans (where 2 are required under **SOE 2.9.b**)





## LOGISTICS FOR A CDS LEVEL 2 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 requirement for CDS Level 2 audits.

### **DURATION**

A CDS level 2 audit should take no longer 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; so do not place them in a place 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 2 audit.

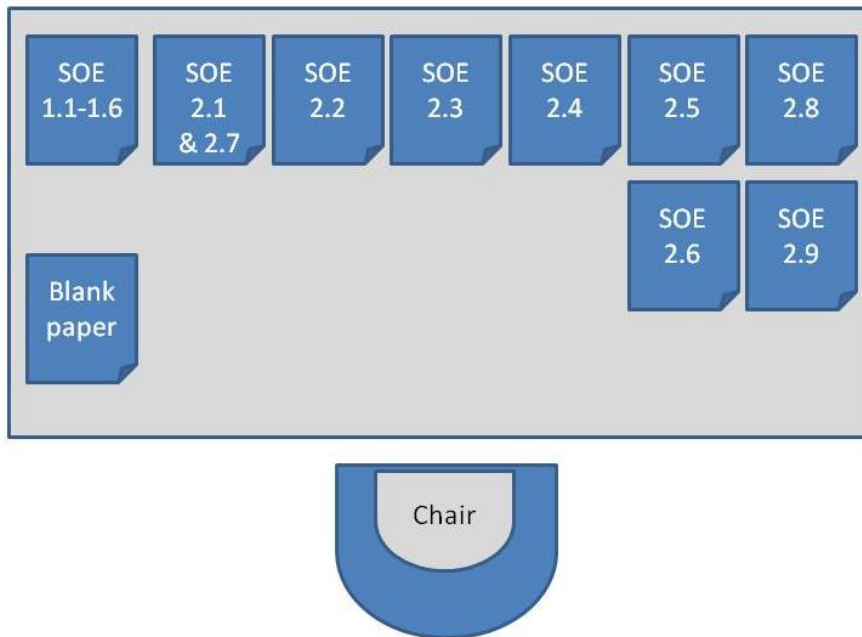


Figure 1 - CDS Level 2 SOE arrangement

Each collection of evidence generated to meet a particular SOE requires a cover sheet to allow the auditor to quickly see what SOE it pertains to. Sheets can locally produced and need only have the SOE number printed/written on the front. Advanced cover sheets will be available from the CDS website<sup>4</sup> and these will include a series of checkboxes to ensure that the organization has omitted 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, the organization will fail the audit.

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

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