Data Security Standard 9

IT Protection

The bigger picture and how the standard fits in

2023/24

Information and technology
for better health and care

Contents

Overview 5

Network components (9.1.1 – 9.1.2) 6

Definition and scope 6

Password strength, remote locations and managed estates (9.1.1 - 9.1.2) 7

Password Strength 7

Remote locations 7

Managed estates 7

Penetration testing (9.2.1 - 9.2.2) 8

Definition 8

Scoping the test 8

Commercially sourced or in house or partner 9

Selecting a commercial organisation 10

Active or passive 10

Know your boundaries (9.2.1 - 9.2.2) 11

Cyber security support model onsite assessments 11

Alerting interested parties 11

Risks 12

Remediation post testing (9.2.3) 13

Remediation post testing 13

OWASP Top 10 vulnerabilities (9.3.1, 9.3.3, 9.3.7) 14

National cyber security centre Web Check 15

Domain Name System (DNS) and IP Ranges (9.3.3 - 9.3.5) 16

Domain Name System (DNS) 16

IP Ranges 16

Connected Medical Devices (9.3.8 – 9.3.9) 17

Choices for implementing a connected devices register 17

Expanding your existing Medical Devices Register 17

Expanding existing IT register 18

Creating a new connected medical devices register 18

Connected medical devices policy 18

Perimeter defence (9.3.6, 9.4.1) 19

Transport Layer Security (TLS) 19
Everything has a shelf life 19
Assurance (9.4.4 – 9.4.5) 20
Examples of assurance in depth 20
Demonstrating your Assurance 21
Addressing deficiencies found during assurance activities 21
Assuring your assurance methods 22
DSPT Independent Assurance 22
An improving picture 23
SIRO involvement 25
Secure Configuration (9.5.1 - 9.5.10) 26
End user devices: Manage installation of software and approvals 26
Consistent secure builds 26
Encryption 26
Centrally setting settings 27
Auto-run 27
Network and systems: manage changes (change control) 27
Remote access authentication 28
Protecting networked non internet devices 28
Secure email standard 29
Firewalls (9.6.1 – 9.6.6) 30
Boundary firewall(s) 30
Firewall admin interface on the internet 30
Block unauthenticated inbound connections 31
Get approved 31
Bin the old rules 31
PC Personal firewalls 32
Frameworks that can help 33
Cyber Essentials / PLUS 33
Scope 33
Assurance framework 34
ISO 27001 35
What an ISMS is 35
Certification to ISO/IEC 27001 35
IT Infrastructure Library (ITIL) 36

About ITIL 36
Part 11 Mapping 36
Appendix 1 - Useful resources 38
Appendix 2 – The National Data Guardian Reports 39

Overview

The NDG’s review data standard 9 states that:

“A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.”

NHS England assists risk owners in understanding which national frameworks do what, and which components are intended to achieve which outcomes.

There is a clear understanding that organisations can tackle the NDG Standards in whichever order they choose, and that the emphasis is on progress from their own starting points.

Please refer to further note on professional judgement, auditing and UK GDPR.
https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/using-professional-judgement

Network components (9.1.1 – 9.1.2)

Definition and scope

Networking components are physical devices which are required for communication and interaction between devices on a computer network they include, but are not limited to:

- firewalls
- switches and hubs
- bridges
- routers
- wireless access devices.

Out of the box network devices may ship with the same username and password for that specific type of device or even be the same for all that provider’s devices. Consequently, the login details are available on the internet and this makes the devices very vulnerable to misuse.

> *“Data security incidents, such as the May 2017 global ransomware attack which affected NHS services, as well as other public services and private companies in many other countries, have highlighted the potential for cyberattacks to disrupt services by having a direct impact on the availability of care for patients and service users.”*
>
> **Your Data: Better Security, Better Choice, Better Care Government Response**

All network components need to have their default passwords changed.

Some network components (particularly those provided by internet service providers for home or small business use) can have a unique username and password 'out of the box'. So, it can be acceptable to not change those Internet Service Provider (ISP) provided devices, subject to confirmation and the device itself not having a label attached in a public setting with the login details.

Similarly, to scanning software in Data Security Standard 8, it's important to know the boundaries of your estate and not go beyond them and attempt to change a password on a device not managed by your organisation.

As well as networking components other devices should also have their default passwords changed (where applicable). Devices encompass servers, desktop computers, laptop computers, tablets and mobile phones.

Password strength, remote locations and managed estates (9.1.1 - 9.1.2)

Password Strength

The type of password used for changing a default network component, should consider the following:

- Not using a single word
- Think random
- Think multiple (3 random passwords technique)
- Not using or containing a common password

Remote locations

Where your organisation has remote locations, it will generally fall into one of these categories:

- scenario a: your organisation manages the whole remote site network infrastructure
- scenario b: another organisation (such as the main organisation at the remote site) manages the network infrastructure

For scenario a: you are responsible for changing the network components default password.

For scenario b: you will require cooperation with the remote site organisation, assurance from them that the password change has occurred, and the equipment is covered in their Data Security and Protection Toolkit assessment.

Managed estates

Where your organisation network infrastructure is managed by another party you will require a degree of cooperation with your supplier. Generally, it will be expected that your supplier changes the default passwords. The third party would then provide confirmation that this has taken place.

Penetration testing (9.2.1 - 9.2.2)

Definition

There are a few definitions of what constitutes a penetration test and the difference between penetration testing and vulnerability scanning. The differences are mostly around intent, with vulnerability scanning producing a list of items requiring updating or patching, and penetration testing having a defined goal, for example getting access to a network share or an elevated account.

Many of the tools available on the internet market are completely legitimate, however some can be utilised for less legitimate purposes for example cybercrime. Ensure you have sufficient technical capability before downloading and using any tools.

Consider a penetration test at least annually and vulnerability scanning which should occur more often. A penetration test usually includes a vulnerability scanning element.

Scoping the test

A penetration test should be undertaken (at least annually).

The penetration test must include the following elements:

- all webservers the organisation utilises
- vulnerability scans
- checking that the default password of network components have been changed.

There is an expectation that the penetration test would cover all the organisation’s critical network structure such as server farms.

Commercially sourced or in house or partner

The options for penetration testing are to either to outsource to commercial specialist or if you have the relevant capability and capacity or perform in house partner 'buddy up' with another care organisation and perform each other’s tests.

	Advantages	Disadvantages
Commercial	Independent	Cost
	With right supplier more, experience and expertise.	Lack of knowledge of your network and dependencies
	Reduced burden on existing staff	
In-house	Cheaper	Requires inhouse staff to have capabilities and capacity
	Knowledge of network and dependencies	Lack of segregation of duties
		Cost of tools and upkeep.
		Sole responsibility
Health and care partner	Independent	Network knowledge would be general and may not be site specific.
	Cheaper	Requires both parties to have a similar level of capability and capacity.
	Understanding dependencies on health and care systems	

Selecting a commercial organisation

Although we do not endorse any supplier there are several indicators that may help you decide:

- CREST UK Approved Member Company
- CREST or Tiger Scheme, qualified testers and / or CHECK Team Leaders
- ISO 27001 and / or 9001 certified
- a Digital Marketplace seller (see Appendix 2: useful resources)

Active or passive

Penetration testing can have a varying degree of aggression between active and passive (or combinations).

Know your boundaries (9.2.1 - 9.2.2)

Understand the boundaries of your digital estate and do not overstep them.

Boundaries can occur at many levels such as multiple networks and tenancy in a single building, between your local network and Health and Social Care Network (HSCN) and between wide area networks on the same estate.

Ultimately, you should know where your responsibilities end and another organisation's begin. Consequently, you should not scan or try to update assets that are beyond your boundary.

Under no circumstances should you scan over HSCN without consulting NHS England prior to doing so. Some vulnerability scanners (dependent on how aggressively or passively they are being used) can cause a false positive (where you think you have a specific vulnerability in your program but in fact you do not) and maybe indistinguishable from a cyber-attack, with the same tools being used by hackers.

Cyber security support model onsite assessments

If your organisation has received a data security onsite assessment within the fiscal year, this may count as the penetration test or contribute towards it.

The security assessment should include the following 2 mandatory items:

- webservers
- default password network components

If it does not include the mandatory elements, it is acceptable to have a commercial or in-house or partner penetration test to just cover these elements, provided the Senior Information Risk Owner (SIRO) signs off the scope of the data security onsite assessment.

Alerting interested parties

Before any test, there should be sufficient time to inform interested parties of the test. Interested parties include, but are not limited to:

- system managers or information asset owners
- service desk(s)
- server and network teams
- third parties who support systems or networks

Risks

There are a couple of general risks involved in undertaking a test.

1. The test may be mistaken for the reconnaissance or delivery stage of a cyber attack. As many of the tools and techniques used for penetration testing are the same ones as used by hackers. This can be mitigated by informing all the interested parties and knowing and keeping to your boundaries.

2. The test may have an adverse effect on the asset(s) being scanned. Depending on the aggressiveness of the test and the vintage of the asset this could result in an adverse effect, such as service unavailability requiring a reboot.

Remediation post testing (9.2.3)

Any test results will show a number of vulnerabilities. Critical or high-risk vulnerabilities should be remediated within 14 days.

Where they cannot be remediated within the 14 days the risk should be documented, understood, and agreed with your Senior Information Risk Owner (SIRO).

If the remediation has dependencies that will take longer to fix, such as a legacy system requiring replacement, this should form an action in your data security improvement plan.

Remediation post testing

Any test results will show a number of vulnerabilities. Critical or high-risk vulnerabilities should be remediated within 14 days.

Where they cannot be remediated within the 14 days the risk should be documented, understood, and agreed with your SIRO.

If the remediation has dependencies that will take longer to fix (such as a legacy system requiring replacement) this should form an action in your data security improvement plan.

More information

For more information see Appendix 2: useful resources at the end of this guide.

OWASP Top 10 vulnerabilities (9.3.1, 9.3.3, 9.3.7)

The primary aim of the Open Web Application Security Project (OWASP) Top 10 vulnerabilities is to educate developers, designers, architects, managers, and organisations about the consequences of the most common and most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high-risk problem areas and provides guidance on where to go from here.

The Top 10 list is revisited and renewed over time. OWASP publish a number of release candidates until they have a final release. For example, at the time of writing the OWASP Top 10 2017 is the current latest official release.

Only the official release of this Top 10 should be followed as part of the toolkit.

You should ensure your web applications are protected against the common security vulnerabilities and the OWASP top 10 represents a good starting point. However, it is not a replacement for specific NHS Cyber alerts, as described in the Data Security Standard 6, which you should still action.

The OWASP Top 10 is quite technical and will require liaising with your web site developers to assure compliance.

You will also need to ensure that all your web servers or sites are covered by a penetration test and remediations are followed through and overseen by your Senior Information Risk Owner (SIRO).

National cyber security centre Web Check

As well as manually checking against OWASP you should use a web check service. The National Cyber Security Centre's Web Check is highly recommended for public sector bodies.

For those in the private sector there are commercial and free services such as Sucuri, which offer a free website security check and malware scanner.

Domain Name System (DNS) and IP Ranges (9.3.3 - 9.3.5)

Domain Name System (DNS)

Your DNS query service should use National Cyber Security Centre’s Protective Domain Name Service (PDNS) for your name to Internet Protocol (IP) resolution.

Where you can add a manual DNS entry or override an existing one this action should be adequately secured. This is to ensure changes are only made via strongly authenticated and authorised administrators, so you know exactly who made the changes and that they were authorised to do so.

This safeguards your internet users from being directed to a bogus website.

IP Ranges

You should manage and record all of your IP ranges used across your organisations. Irrespective of that address space generation (IPv4/IPv6) or class.

Having good management of your address space, such as using Dynamic Host Configuration Protocol (DHCP) and not using fixed IP’s at client level, all helps.

It is recognised that you will probably have a mixture of address spaces. Not knowing all your address spaces means you are not managing the devices on them and they would not feature as part of your vulnerability scan.

HSCN IP Addressing good practice guidelines

This document provides advice and guidelines for IP addressing and related key protocols for organisations connected to the HSCN

https://digital.nhs.uk/services/health-and-social-care-network/hscn-technical-guidance/hscn-ip-address-management/hscn-ip-addressing-good-practice-guidelines

Connected Medical Devices (9.3.8 – 9.3.9)

With medical devices becoming more connected and, in many respects, subject to the same level of vulnerabilities (if not more) than a desktop, tablet or laptop device. These vulnerabilities are particularly marked with the 1st generations of connected medical devices some of which may have a decades long life span.

So just as it is important to know your user base and their devices, it is important to have a register of connected medical devices.

This register should include vendor, maintenance arrangements, any network segmentation in place and whether network access is given to supplier/maintainer. It is expected it would contain (or is linked) the items found in an IT asset register network name, IP address (if static), Mac address and software and versions (where appropriate).

At the time of writing there is not a prescribed register or set methodology of implementation. Consequently, there are 3 broad implementation choices.

Choices for implementing a connected devices register

There are three routes to implementing:

- existing medical devices register
- existing IT asset register
- new connected medical devices register

You can expand the existing medical devices register or your IT asset or create new connected medical devices register.

Whichever route you choose they should ideally be linked or synchronised with themselves and other products such as asset discovery tools. It is important to avoid duplication and any subsequent version control issues.

Expanding your existing Medical Devices Register

With this option you would need to add the specific item's vendor, maintenance arrangements, any network segmentation in place and whether network access is given to supplier/maintainer and then linked to IT asset register/discovery tool showing network name, IP address (if static), Mac address and software and versions.

Expanding existing IT register

With this option you would need to add the specific item’s vendor, maintenance arrangements, any network segmentation in place and whether network access is given to supplier or maintainer. You wouldn’t need a link to a discovery tool (as this is hopefully inbuilt) but the device would still need to exist as an entry in any medical device register so ideally should be linked.

Creating a new connected medical devices register

In some ways, the most challenging option as well as the items mentioned in the other two options for registers. It would ideally require linkage to both the IT asset register and medical devices register.

Connected medical devices policy

This should be a policy or process documenting the full explanation of how the organisation assures data security during the full life cycle of the medical device.

At the time of writing there is not a set format for the policy or procedure however it should treat a medical device in the same way of any IT device that may contain patient information. So that covers inception with security awareness before purchase, ongoing support both manufacturer/supplier teams and patching/updating. It should also cover the retirement/disposal of devices with the presumption there will be sensitive/patient information stored on them.

The policy/procedure itself can be incorporated into an existing policy (medical devices or IT policy) or standalone. However, much like the register, it is important it does not duplicate or is contrary to policies covering the same ground.

Further Reading

Guidance on protecting connected medical devices

https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/guidance-on-protecting-connected-medical-devices

Perimeter defence (9.3.6, 9.4.1)

You should have a suitable perimeter defence such as next generation firewall described in the HSCN perimeter security guide.

The National Cyber Security Centre provide guidelines on the network perimeter defence.

If you are an NHS body we recommend you consider the NHS Secure boundary solution.

Transport Layer Security (TLS)

Transport Layer Security (TLS) is used in client server communication and a well-configured TLS ensures that no third party can eavesdrop or tamper with any message.

Well configured in the sense it follows the National Cyber Security Centre requirements on ciphers and certificates for Opportunistic TLS used in mail (as one example). The version utilised should be 1.2 or 1.3 (1.3 being the newest at the time of writing).

Everything has a shelf life

Over time, security measures and controls can become less effective. Static security measures are not like a fine wine, they generally don’t get better with age.

That insightful and cutting-edge security induction can soon date, your polices may reflect obsolete advice such as the use of strong passwords and that market leader proxy server you purchased several years ago, may now only be receiving minimal updates.

To know how effective your security measures and controls are it is important to know what and where they are. Therefore, an inventory view of your security posture can be useful.

How you chose to validate your controls and measures is not mandated and would probably come from a variety of sources given it covers all your network and information systems.

Assurance (9.4.4 – 9.4.5)

You will have a variety of assurance mechanisms available to you, knowing what they are and which to apply and how, is critical.

Ranging from the DSPT assurance to onsite assessments, automated assurance (such as vulnerability scanners) and bespoke interventions.

It can also involve certification particularly CE+ and ISO 27001, peer reviews and surveying your staff.

Having assurance in depth is just as important as its defence counterpart, no one assurance method is king and having a mix of assurance methods is the best option.

Examples of assurance in depth

People

- survey
- forums
- spot tests

Process

- onsite assessment
- CE+
- DSPT audit
- ISO 27001

Technology

- scanners
- survey tools
- simulations

Demonstrating your Assurance

Regardless of the assurance method you select, you should be able to demonstrate your confidence in security at least annually.

For NHS organisations this will generally be the uptake of relevant services from NHS England Cyber Security Services, particularly the onsite assessment.

For local authorities, this can be PSN IA, for others ISO 27001 and CE+.

Addressing deficiencies found during assurance activities

You should respond to and treat NHS cyber alerts and treat the route security deficiencies post an incident. You should also triage and treat discovered deficiencies during assurance activities in the same way.

The important factor is what you do post an assurance activity not just undertaking the activity itself.

Discovered deficiencies should be triaged and remediated depending on their risk. Some may need to be remediated very quickly, such as discovering a server that has not been remediated following a high severity cyber alert, or some more long-term item featured in a data security improvement plan.

Some you may not be able to remediate at all, such as with a legacy system which must be retained, and these should be recorded and the Senior Information Risk Owner (SIRO) informed.

Assuring your assurance methods

As well as managing the outputs of your assurance activities you should intermittently look at how effective your assurance posture is.

This can take several forms:

- looking at your suppliers, testing the market
- horizon scanning not just today's environment but what assurance is required in future
- a review of your methods looking at effectiveness
- looking at your local healthcare economy partners to see their approach
- being prepared to drop or change ineffective assurance activities

DSPT Independent Assurance

The DSPT independent guidance enables better assurance of DSPT submissions by standardising assessments. It will also help to give a better understanding of data security and protection risk themes across the health and care system.

This is mandated for NHS organisations

- NHS Trusts (acute, foundation, ambulance and mental health)
- Integrated Care Boards
- Commissioning Support Units
- Arm's Length Bodies
- IT suppliers

It is important that organisations assure themselves that audit providers follow the mandated scope which for this year is:

1.1 The organisation has a framework in place to support Lawfulness, Fairness and Transparency

2.2 Staff contracts set out responsibilities for data security

3.1 Staff have appropriate understanding of information governance and cyber security, with an effective range of approaches taken to training and awareness

3.2 Your organisation engages proactively and widely to improve data security, and has an open and just culture for data security incidents

4.4 You closely manage privileged user access to networks and information systems supporting the essential service

5.1 Process reviews are held at least once per year where data security is put at risk and following DS incidents

6.2 All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway

7.1 Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services

8.4 You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service

9.2 A penetration test has been scoped and undertaken

9.5 You securely configure the network and information systems that support the delivery of essential services

9.6 The organisation is protected by a well-managed firewall

10.2 Basic due diligence has been undertaken against each supplier that handles personal information

It is also important that organisations assure themselves that their chosen audit provider is aware of the mandated framework which needs to be followed.

The hallmark of the methodology is an output with a risk rating against of the 10 data security standards, an overall risk rating, based on the 10 individual ratings, and a confidence rating.

An improving picture

This process should be viewed as a continuous cycle of improvement.

It should follow a Plan, Do, Check, Act model as follows:

- scope the plan
- SIRO approves scope
- data planned and stakeholders informed
- SIRO reviews results
- remediation

SIRO involvement

The SIRO should have an active role in the scoping process, including approval of the scope of the plan, particularly any penetration testing including OWASP tests.

Secure Configuration (9.5.1 - 9.5.10)

End user devices: Manage installation of software and approvals

Installation of software is controlled so there is a conscious decision of who, how and what is installed.

For example, in Microsoft Windows you would not expect standard users to be members of the administrator group as they could install any software. Equally, you would expect a normal user to install approved software, where technically feasible or desirable. This could be accomplished through allow-listing, where an index of approved software applications is specified that are permitted, and an organisation app store.

Consistent secure builds

You have a secure build for each of your platforms (computers, laptops and tablets with main corporate operating system), that is secure by design and standardised where possible. The build image or gold build should be updated at regular intervals to prevent a newly imaged device requiring numerous updates or running out of date software.

It is recognised that imaging tablets/mobile phones with 'phone operating systems' such as android is unrealistic and these should be managed through mobile device management solutions.

Encryption

Device level encryption (such as AES 256) is applied on all mobile devices and removable media for data at rest.

Mobile devices include:

- laptops
- tablets
- mobile phones

Consider 'at risk' desktop PC’s, such as those in public areas

Removable media include:

- USB flash drives

- USB hard drives

You should also wipe or revoke access for those devices normally through a mobile device management system.

It is recognised that remote wiping of removable media is technically unachievable.

Centrally setting settings

The ability to set and change security settings centrally across your entire estate and device mix is incredibly powerful. It allows you to update your security posture during times of high risk and then relax it afterwards such as turning on USB Restricted Mode to make hacking more difficult in iPhone Operating System (IOS) devices.

In Windows this would normally be accomplished by group policy setting, windows setting and the group of security settings. In mobile devices this would normally be through a mobile device management system.

Auto-run

Having programs autorun creates an attack vector for malicious software to be executed. Consequently, it should be switched off on all your device type where applicable.

Network and systems: manage changes (change control)

Having the ability to easily change system and network settings is very powerful but also very dangerous. Without effective change control and system documentation even a well-intentioned change can permeate throughout your infrastructure and be difficult to reverse.

Having a baseline and snap shots, whether automated or manual, helps you return configurations to normal post an incident.

Ensuring changes are authorised, planned and have a credible reversal plan can help.

Formalising this process with a methodology such as Information Technology Infrastructure Library (ITIL) can also assist.

Blogpost: Want to make an IT service change? Here’s how to do it

Change, release and deployment in ITIL help to ensure that what a requester, such as a service owner wants, can be delivered from a technical and feasibility perspective.

https://www.axelos.com/resource-hub/blog/want-to-make-an-it-service-change-here-s-how-to-do-it

Remote access authentication

As remote access opens your resources (corporate networks and web applications) potentially to the entire internet, it is important that all remote access has strong authentication.

Ideally this should be multifactor, normally 2 form, which usually takes the form of the following:

- username
- password
- hardware or soft token

Guidance: Multi-factor authentication for online services

National Cyber Security Centre (NCSC) advice for organisations implementing multi or 2 factor authentication to protect against password guessing and theft on online services.

https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services

Protecting networked non internet devices

These are devices that are connected to your network (but not the internet) either because they are legacy systems, medical devices or untrusted systems that cannot be patched.

It is important you protect these systems and your wider network from each other. This can be accomplished through such techniques as:

- network separation (such as VLANs)
- maintaining a deny list
- virtualisation
- sandboxing
- separate firewall
- non-routable subnets

One method is to treat all of these systems as obsolete systems and, therefore, unmanaged or untrusted, as described in the Data Security Standard 8.

Secure email standard

Emails sent to and from health and social care organisations must meet the secure email standard (DCB1596) so that everyone can be sure that sensitive and confidential information is kept secure.

Firewalls (9.6.1 – 9.6.6)

Boundary firewall(s)

You should have a firewall at each boundary of your internal network to another network not in your control, for example to HSCN, the internet or a Community of Interest Network.

This should be in line with the HSCN requirement.

Firewall admin interface on the internet

Firewall admin interfaces are generally web based and would present a known attack vector to any potential threat actor, therefore, disable access to web interface of a firewall from the internet.

Consideration should be given if and how you manage access to the firewall web interface remotely, for example through a remote access session or Virtual Private Network (VPN).

NCSC blog post: Protect your management interfaces
Why it’s important to protect the interfaces used to manage your infrastructure, and some recommendations on how you might do this.
https://www.ncsc.gov.uk/blog-post/protect-your-management-interfaces

Block unauthenticated inbound connections

Unauthenticated inbound connections are bad, block them by default.

Examples include:

- SMB
- NetBIOS
- Telnet
- TFTP
- RPC
- RDP
- Rlogish
- Rsh
- rexec

Get approved

A single misinformed inbound firewall could present a tempting target to any threat actor. It is important that inbound firewall rules are business justified, documented and appropriately approved.

New or updated inbound firewall rules should be treated as standard pre-approved changes unless they are beyond tight pre-understood acceptable known configurations.

Where there is a conflict between business need and security, where appropriate, a risk should be raised for the Senior Information Risk Owner (SIRO) to consider.

Bin the old rules

Where a firewall rule is no longer required, for example where a system or process has been updated or retired, these rules should be removed or disabled as soon as possible.

It is understood for continuity reasons, that it is useful to disable a rule (for a period of time), so the option to re-enable is available as rollback before deletion.

As a part of your assurance process it is useful to review firewall rules to see if any rules do not have a least privileged approach or can be retired.

PC Personal firewalls

On top of a boundary firewall, having desktop PCs with personal firewalls represents another layer of defence. These should be configured to block unapproved connections by default.

Frameworks that can help

There are several frameworks that help in both achieving and demonstrating a managed data security plan, most notably Cyber Essentials, Cyber Essentials + and ISO 27001.

Cyber Essentials / PLUS

Scope

The Cyber Essentials Scheme covers the basics of cyber security in an organisation’s enterprise or corporate IT system. Implementation of these controls can significantly reduce the risk of prevalent but unskilled cyber-attack.

For many organisations, especially those with significant information assets or who are exposed to a wider range of threats, Cyber Essentials will become a practical component of a wider ranging cyber security posture. For example, as described in the 10 Steps to Cyber Security and Cyber Security: what small businesses need to know.

The scheme requirements document focuses on internet-originated attacks against an organisation’s IT system. Many organisations will have particular additional services, for example web applications, that will require additional and specific controls beyond those provided by cyber essentials.

Cyber essentials concentrates on 5 key controls.

These are:

1. Boundary firewalls and internet gateways

These are devices designed to prevent unauthorised access to or from private networks, but good setup of these devices either in hardware or software form is important for them to be fully effective.

2. Secure configuration

Ensuring that systems are configured in the most secure way for the needs of the organisation.

3. Access control

Ensuring only those who should have access to systems to have access and at the appropriate level.

4. Malware protection

Ensuring that virus and malware protection is installed and is it up to date.

5. Patch management

Ensuring the latest supported version of applications is used and all the necessary patches supplied by the vendor been applied.

Assurance framework

As stories of organisations exposing customers' information to cyber threats continue to create headlines in the media, it is becoming increasingly important for organisations to not only maintain a robust cyber security stance but also demonstrate this to clients.

The assurance framework is designed to provide a simple means for third parties to distinguish between organisations that are implementing basic cyber security controls from those that are not.

This can be used in a number of ways:

- an organisation may undergo certification to mark them out from their competitors
- they may require certification from partners where contractual relationships expose them to wider cyber risk, for example where information is shared
- insurers, investors and auditors may take certification into account when assessing an organisation's risk profile

ISO 27001

The ISO/IEC 27001 is part of a family of standards which helps organisations keep information assets secure.

Using this family of standards will help your organisation manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).

What an ISMS is

An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

It can help small, medium and large businesses in any sector to keep information assets secure.

Certification to ISO/IEC 27001

Like other ISO management system standards, certification to ISO/IEC 27001 is possible but not obligatory.

Some organisations choose to implement the standard in order to benefit from the best practice it contains while others decide they also want to get certified to reassure customers and clients that its recommendations have been followed. ISO does not perform certification.

IT Infrastructure Library (ITIL)

IT Infrastructure Library (ITIL) is used by millions of professionals globally. Businesses are built on ITIL.

ITIL supports organisations and individuals to gain optimal value from IT and digital services. It helps define the direction of the service provider with a clear capability model and aligns them to the business strategy and customer needs.

ITIL, a professionally recognised certification scheme, provides comprehensive, practical and proven guidance for establishing a service management system, providing a common glossary of terms for businesses using IT enabled services.

About ITIL

ITIL is a widely accepted approach to IT service management (ITSM), which has been adopted by individuals and organisations across the world. It provides a cohesive set of best practice, drawn from the public and private sectors internationally.

Every year, organisations invest heavily in adopting and adapting ITIL into their business practices and upskilling their workforce with ITIL qualifications.

Extensive research by AXELOS, involving a diverse group of stakeholders (in excess of 2,000), has consistently shown that ITIL is fundamental to businesses, enables transformation and helps organisations realise value.

ITIL advocates that IT services are aligned to the needs of the business and support its core processes.

The ITIL approach provides guidance to organisations and individuals on how to use IT as a tool to facilitate business change, transformation and growth. ITIL is mapped in ISO 20000

Part 11 Mapping

This recognises the way that ITIL can be used to meet the requirements set out for ISO 20000 certification and the interdependent nature with ITIL. This is the first such mapping that ISO (the International Organisation for Standardisation) has allowed to be part of their standards. The ITIL ITSM best practice is supported by a certification scheme that enables practitioners to demonstrate their abilities in adopting and adapting the framework to address their specific needs.

Unlike CE+ and ISO 27001, ITIL is not security centric but does help with assets management, change control and managing incidents. Another difference is that organisations are not ITIL certified but individuals are.

Appendix 1 - Useful resources

Penetration Testing: NCSC - Advice on how to get the most from penetration testing.
https://www.ncsc.gov.uk/guidance/penetration-testing

Vulnerability management: NCSC - Guidance to help organisations assess and prioritise vulnerabilities.
https://www.ncsc.gov.uk/guidance/vulnerability-management

Buying cyber security services: NHS England - This guidance explains how to procure cyber security services for your NHS organisation. It covers the services provided by NHS England, along with services available from the NHS Shared Business Services and National Cyber Security Centre (NCSC) framework agreements.
https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/buying-cyber-security-services

Appendix 2 – The National Data Guardian Reports

The NDG Report

Recommendations to improve security of health and care information and ensure people can make informed choices about how their data is used.

National Data Guardian for Health and Care
Review of Data Security, Consent and Opt-Outs

Review of Data Security, Consent and Opt-Outs

The government response

‘Your Data: Better Security, Better Choice, Better Care’ is the government’s response to:

- the National Data Guardian for Health and Care’s ‘Review of Data Security, Consent and Opt-Outs’
- the public consultation on that review
- the Care Quality Commission’s Review ‘Safe Data, Safe Care’.

It sets out that the government accepts the recommendations in both the National Data Guardian review and the Care Quality Commission review.

It also reflects on what we heard through consultation to set out immediate and longer-term action for implementation.

Your Data: Better Security, Better Choice, Better Care