NHS
England

Data Security Standard 7

Continuity Planning

The bigger picture
and how the standard fits in

2023/24

Information and technology
for better health and care

Contents

Commented [VA1]: table of contents is for standard 6...

Overview

The National Data Guardian review’s data standard 7 states that:

“A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.”

A business continuity exercise is run every year as a minimum, with guidance and templates available from the toolkit. Those in key roles will receive dedicated training, so as to make judicious use of the available materials, ensuring that planning is modelled around the needs of their own business. There should be a clear focus on enabling senior management to make good decisions, and this requires genuine understanding of the topic, as well as the good use of plain English.

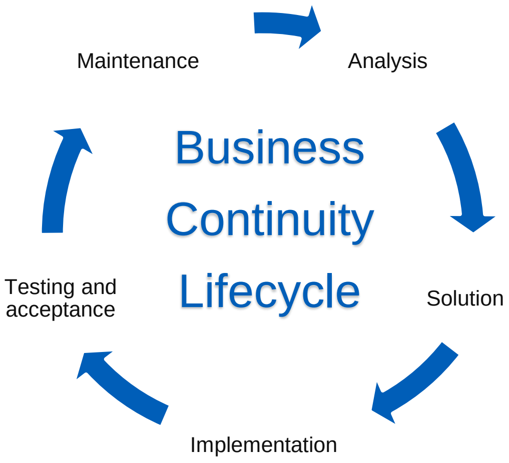


Image description

The business continuity lifecycle is a continuous cycle of:

- analysis
- solution
- implementation
- testing and acceptance
- maintenance

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

Know your services (7.1.1)

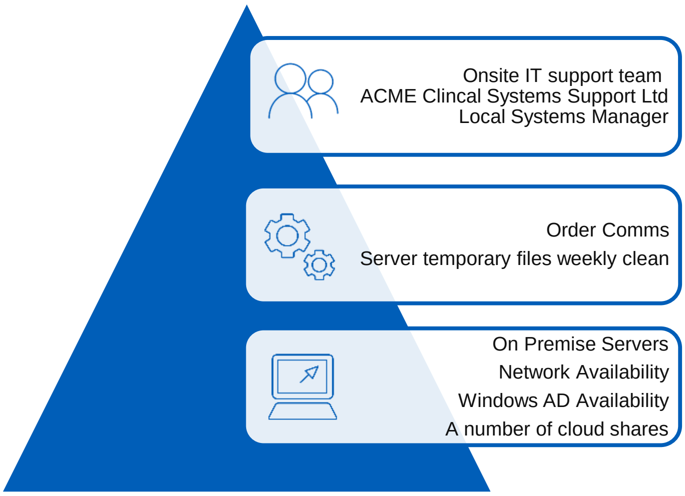
Understanding and cataloguing the health and care services your organisation provides is a vital precursor to continuity planning.

For each of those catalogued services you should know:

- what technology and services underpin that service in terms of availability and security
- other dependencies such as power, cooling, data, people and other systems
- the impact of the system being unavailable

For example, looking at a generic clinical service that is underpinned by or dependent on people, processes and technology.

Example clinical service:



Onsite IT support team
ACME Clincal Systems Support Ltd
Local Systems Manager

Order Comms
Server temporary files weekly clean

On Premise Servers
Network Availability
Windows AD Availability
A number of cloud shares

Image Description

Example hierarchy or people, processes and technology that underpin a clinical service.

From top to bottom:

1. On-site IT support team, ACME Clinical Systems Support Ltd, local support manager
2. Order comms, server temporary files weekly clean
3. On-premises services, network availability, Windows AD availability, a number of cloud shares

Business continuity and disaster recovery - part 1 (7.1.2)

Definition and background

The terms business continuity and disaster recovery are often interchanged and sometimes viewed as the same thing. A business continuity plan (BCP) is concerned with how you keep the organisation going and could involve relocation and reshaping services.

Disaster recovery is effectively a plan of attack of how you fix the problem and return the organisation back to normality.

In the care system, organisation business continuity tends to focus on:

- "Acts of God" – such as flooding or high winds
- staffing – such as medical virus outbreak or industrial action
- major incidents – such as a terrorist attack or major fire
- site unavailability – such as a power outage or road issues
- extreme demand – such as winter pressures or service closures elsewhere

The global WannaCry cyberattack in May 2017 has reaffirmed the potential for cyber incidents to impact directly on patient care and the need for our health and care system to act decisively to minimise the impact on essential frontline services.

Your Data: Better Security, Better Choice, Better Care, government response.

Whereas the IT tends to focus on disaster recovery, with a focus on:

- identifying IT objectives and timescales
- priority of recovery
- the recovery team
- actions for recovery

For smaller organisations, there tends to be one type of plan which would mitigate against their most common risks.

Business continuity and disaster recovery - part 2 (7.1.2 - 7.1.4)

A continuity plan for data security incidents (7.1.2)

There are 3 routes to implementation:

1. Expanding and testing your existing business continuity plan.
2. Expanding and testing your existing IT disaster recovery plan.
3. Creating and testing a data security incident plan.

You can expand an all-encompassing business continuity plan to include data security content, alternatively expand your IT disaster recovery plan. However, where possible we would recommend you have a separate data security incident plan.

Whichever route you choose, data security should be included in any plan, even those not related to cyber incidents. For example, where a restored system that may have the full of access control not being in situ.

Expanding your existing business continuity plan

Generally, this is for smaller organisations that already have an all-encompassing business continuity plan. You should include sections on data security including what to do, what to avoid and scenarios. A smaller organisation business continuity plan (a generalised version of the pharmacy business continuity plan is contained in full in Appendix 2 : Useful resources.

Expanding existing IT disaster recovery plan

Generally, this is for organisations that have an existing IT disaster recovery plan. The team responsible is a small set of people who would respond to data security incidents as well as the more traditional IT ones. This approach can be useful in dealing with an incident where the initial cause may not be known, such as network problem that could be caused by faulty equipment or a denial of service attack.

It is important data security is featured as prominently as the more traditional causes of incidents and includes as a minimum what to do, what to avoid and scenarios.

Good practice guidelines for business and IT security plans are referenced in Appendix 2: Useful resources.

A set of suggested scenarios for data security testing are contained in Appendix 2: Useful resources.

Creating a data security incident plan

For organisations with granularity of roles and sufficient size, we would recommend a separate data security incident plan.

This will allow you to really focus on data security incidents, the actors, attack surface, basic and sophisticated attacks, the phases of the attack and the response.

There are 2 examples in Appendix 2: Useful resources:

- the Cyber Security Incident Response Guide by Crest (The Council for Registered Ethical Security Testers)
- the Computer Security Incident Handling Guide by National Institute of Standards and Technology (NIST) U.S. Department of Commerce

Whilst both examples are very useful, it is important to note the CREST document is written from a point of view of those wishing to augment their data security response with external help. The NIST guidance in parts can be quite US centric.

Know what you need

The length of time it takes to resolve an incident can be prolonged by a lack of knowledge of the resources needed and their availability. This can be compounded by treating each incident in isolation and in a bespoke way rather than using lessons learned and shared resources.

The resources can be people and one widely used method is to formally set up an incident response team. This will generally be a multidisciplinary IT team which can tackle a range of incidents ranging from hardware/network failure to a large-scale malware outbreak.

It can be obvious when you need data security and protection resources to tackle a malware outbreak as it is seen as cyber issue. However, some issues not readily seen as data security and protection due to their nature e.g. server hardware failure, could bring about data security and protection challenges in their resolution.

For example, when commissioning a new server to replace the failed one, the understandable emphasis is to return the service back online with expediency and perhaps take a few short cuts (such as minimum patching, hardening and open file rights). Or it may be tempting to temporarily store file shares in the cloud during remediation, however no assessment may have been made of any legal data protection and contractual obligations before doing so.

The right tools for the job (7.1.3)

Just like any repair, having the right physical and digital tools at your disposal in a timely fashion can make all the difference. Having a 'grab bag' containing items such as switch, networks, diagnostic laptop (with server/network analysis software), USB drives with boot diagnostic software can be useful.

Careful consideration on how many grab bags are required and where they should be located, for example by storing them all on your main site which may have restricted access during an emergency would not be wise.

Public cloud can be a very useful resource (given its high availability and location independence) for machine images, restoration data and diagnostic software.

Whatever method you use to store your restoration resources, remember it is important that you are licensed for the software, that any data stored is secured and processed in a safe manner and that it is as up to date as it needs to be.

An Intelligence lead security posture (7.1.4)

You should be horizon scanning via the NHS Cyber alerts portal, the Cyber Associates Network (CAN) and other sources in order to make temporary changes to your security posture.

For example, a developing situation with a widespread convincing phishing campaign that delivers a highly disruptive piece of malware could temporarily trigger

- a targeted awareness campaign
- a temporary freeze on optional updating
- blocking certain categories of websites
- elevated rights being restricted to a small cohort
- certain network segments with at risk systems (medical devices etc) being completely separated from the corporate network

Once the event has passed these, more draconian measures would be repelled.

Business continuity and disaster recovery - part 3 (7.2.1 - 7.2.2)

Testing the plan (7.2.1)

Testing the plan can generally be done in two ways - through live testing (simulation / active testing) or through desktop-based scenarios.

Live testing

This can take the form of more active penetration test with a threat actor with a defined target, for example bring down a system.

The testing can take place in a live environment or sand pit. It is important that if undertaking the testing in a live environment that you are confident the live environment will not be negatively affected. Conversely, if using a simulated / sand pit environment, it is important that it is a true reflection of a live environment to be representative.

The person undertaking the role of the threat actor should not be the person who would normally be on the incident response team and would normally not have 'insider knowledge'. Unless the scenario is of a disgruntled former employee.

Any live test does have many limitations as it must occur at a known time when the response team is already gathered, and the effect would have to be detected by the team. In a real scenario the time of the event will be unknown, and effects may not be flagged.

Desktop testing

This should form a realistic scenario and a frank and honest appraisal of your response. The goal of desktop testing if to identify gaps in your response in terms of people, processes and technology. These gaps should inform improvement actions that help your future response to any data security incidents.

These test(s) need to occur at least annually and have board level representation.

It is highly recommended that you utilise National Cyber Security Centre (NCSC)' Exercise in a Box' for desktop testing.

Exercise in a Box is an online tool from the NCSC that helps organisations test and practise their response to a cyber attack:

- it's completely free and you don't have to be an expert to use it

- the service provides exercises, based around the main cyber threats, which an organisation undertake in its own time, in a safe environment, as many times as it needs to
- it includes everything you need for setting up, planning, delivery, and post exercise activity, all in one place
- to use Exercise in a Box you need to register for an account, which enables the provision of a tailored report, helping organisations identify their next steps and pointing toward guidance that is most relevant for the organisation

Membership of the testing group (7.2.2)

It is recognised that the exact makeup will vary and be dependent on the size and nature of the organisation. The table below makes some recommendations of the type of roles, with an understanding that some roles may be merged.

Role	Description
Board level member	Mandatory, allows board to be informed
External chair / adjudicator	Someone independent from your organisation who is not involved in the incident response. They would have some experience in this area (such as your counterparts from a neighbouring organisation). They would deliver the scenario, respond to queries and develop the scenario based on the answers
Information / data security / IG	Specialist in data security and protection
Head / director IT	The person responsible for IT in your organisation
CCIO (Chief Clinical Information Officer)	To understand the clinical impact of incidents
Network manager	Specialist responsible for network infrastructure
Server manager	Specialist responsible for server infrastructure
Service desk manager	Responsible for the help desk service
Desktop manager	Responsible for team of desktop technicians

An example of an attendance sheet is shown in Appendix 2: Useful resources.

Exercise scenarios should be based on incidents experienced by your and other organisations, or are composed using threat intelligence.

This should be since 1 July 2021 with active board and business representation.

The type and volume of scenarios

The type of scenarios should be related to the most likely data security incidents. Some suggestions for the type of incidents are included in Appendix 1: Useful resources. Three of the most likely scenarios should be undertaken.

During the testing

During the test, the scenario should be explained to the incident team with replies and queries logged. The chair should probe the answer, not taking the response at face value, and develop the scenario. The intention, like any testing, is to identify areas for improvement. An example of a log of test is shown in Appendix 1: Useful resources.

Where you find gaps, you should log them (together with a name to look at them), however the exercise should not be overtaken by solutions analysis. The primary purpose is to identify a gap and then move on.

Post testing

Post testing a full action plan should be drawn up with allocated names and dates. This should be followed up. An example action plan is contained in Appendix 1: Useful resources.

Business continuity and disaster recovery - part 4 (7.3.1 - 7.3.6)

You are not alone (7.3.1)

Data security incidents when discovered can be daunting and it can be tempting to implement blanket controls. Your immediate response can either help remediate or worsen the situation.

It is important that you engage with NHS England (for an NHS body) or a Cyber Incident Response company where appropriate. They will have experience and a pool of resources to assist you.

Roles and responsibilities (7.3.2)

In the event of invoking the plan, it's essential that team members can be contacted and assemble the response team.

Therefore, there is a mandate that a hard copy of the contacts for the response team is kept securely and kept up to date. It is important that it is also known when it was last updated and printed.

Consideration should be given to where the copy of the contact list is located, especially in a scenario that affects access to the site (meaning the same list used for IT disaster recovery).

The contact list should be reviewed and updated at intervals. When updated the contact list should be reprinted.

Digital contact list

It is recognised that not every incident will require accessing a 'last resort' hardcopy contact list. Storing on a source outside your network (such as NHSmail or Cloud) which is accessed from any device can seem attractive. You will need to ensure the location and security of the service is compatible with trust and national guidance. However, digital storage should be additional and not a replacement for hard copy storage.

Press material (7.3.3)

A draft press statement should be drawn up in conjunction with your communications team to speed up the press response and ensure consistency.

There is a commercial sector link on how to handle the media following a cyber-attack in Appendix 1: Useful resources. This provides some key points to consider when crafting skeleton statements.

These should be reviewed and updated on a regular basis.

Back up the cloud? (7.3.4)

With traditional on-premises servers, there is a classical model of backup to an offline device/media (generally tape) using a backup technique with full/ incremental backup cycles such and grandfather-father-son rotation.

This ensured you go back to multiple points in time to restore your data and thus providing redundancy if your latest backup was corrupt.

Move forward to the cloud online world and with near 100% uptime with replication between multiple locations availability and therefore backups are seen as entirely the cloud provider’s responsibility.

However, it is entirely possible for the cloud provider to have 100% uptime with your critical data being up to date and replicated but you are not able to access it.

This can happen where ransomware can encrypt not only the physically connected drives but also network drives that can be cloud hosted.

This can lead to a situation where your critical data is encrypted and this is replicated in real time to all the instances of that data. Not having any other copies of the data and being entirely reliant on the cloud provider.

If I could turn back time (7.3.5)

Backing up to a different source has been a standard method of recovery for decades. However, when needed during an incident some organisations have found that restoring a backup has proven difficult and this has prolonged the time to return to business as usual.

This can be for a variety of reasons including:

- overused or old media
- corrupt catalogue

- bad image files
- multiple complex restores required - full and then a large number of incremental
- backup didn't occur or backed up the wrong system
- nowhere to store the restore
- networked disk-based storage being unavailable due to the nature of the incident

For all these reasons and more, it is important that you can have confidence in the recovery of essential service through testing, documenting and routinely reviewing.

The testing should be representative of the service or system in focus and not based on routine smaller scale requests or an old live incident. For example, a routine restore of single mailbox for a returning member of staff would not be considered as enough confidence to restore a whole email system.

Whether to use live or test systems should be determined on risk and whether the test system is sufficiently representative of the live system to make the testing valid.

Just as important as the tests themselves is documenting how to restore the system as well as any issues found during the test and the plan to rectify them.

The testing frequency should be routinely periodic especially after any major change in the system or service.

The 3-2-1 rule (7.3.6)

Nothing to do with an 80s gameshow but a technique to keep your data safe meaning have at least 3 copies, on 2 devices, and 1 offsite.

See the NCSC blog post Offline backups in an online world.

Appendix 1 - Useful resources

Emergency Preparedness, Resilience and Response (EPRR) business continuity toolkit: NHS England - Highlighting the need for business continuity management in NHS organisations so that they can maintain continuity of key services in the face of disruption from identified local risks.
https://www.england.nhs.uk/ourwork/eprr/bc/

Emergency Planning/Business Continuity: Pharmaceutical Services Negotiating Committee (PSNC) - PSNC has produced a business continuity template to meet the requirements of community pharmacy service providers.
https://psnc.org.uk/quality-and-regulations/clinical-governance/emergency-planning/

Response and recovery planning (CAF): NCSC - Putting suitable incident management and mitigation processes in place. There are well defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.
https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/d-1-response-and-recovery-planning

Data and cyber security: NHS England - View the latest cyber and data security policy and good practice guidance from NHS England’s 's data security centre. Sign up for security threat bulletins and emergency notifications.
https://digital.nhs.uk/cyber

How to handle the media following a cyber-attack: Mediafirst - Example from the commercial sector highlighting things to consider when handling the press following a cyber incident.
https://www.mediafirst.co.uk/blog/how-to-handle-the-media-following-a-cyber-attack/
https://digital.nhs.uk/cyber-security

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