KPMG

2023 Data Security and Protection Toolkit Benchmarking

October 2023

Contents

01

Executive Summary

> The nature of data security and protection attacks and breaches are rapidly changing and increasing in frequency, severity and impact.

NHS England

Strengthening Assurance Framework 2022/23

A Forward Look

Forging Resilience: The shifting landscape

In an era marked by rapid technological development and an increasingly sophisticated cyber threat landscape, the pressing need to fortify data security controls and safeguard patient, research, and sensitive commercial information continues to take centre stage.

This report demonstrates the progress and challenges faced by organisations year-on-year, highlighting the evolution of resilience across Health and Care.

In 2021/22, 80% of participating organisations struggled to substantiate the controls in place to protect systems from exploitation and vulnerabilities, but the 2022/23 assessment period saw a noticeable transformation, with 43% of participating organisations meeting the assertion. This signifies a concerted effort to improve controls around mission critical systems handling sensitive data.

Continuity planning continues as a forerunning challenge for Trusts. Our audits evaluated the design of continuity plans and tests, required in the event of cyber or data related security incidents. Encouragingly, the 2022/23 assessment period signals a shift with a drop to 36% non-compliance compared to 63% in 2021/22.

Raj Cheema - Partner, Digital Healthcare

Evolving defenses and a new horizon

The DSPT provides a comprehensive self-assessment framework, but increased digitalisation, risks in the supply chain, and rapidly evolving attack vectors have all driven the critical call to consider cyber security with heightened attention. Staying ahead of the curve and encompassing technical controls beyond data security is no longer a strategic decision, but an organisational imperative. Key factors that have contributed to this shift in focus:

— **Increasing digitisation*:*** the proliferation of Cloud services, Operational Technology, and network connected biomedical devices across hospitals has blurred the line between computer systems and physical infrastructure, creating a wider attack surface and introducing new vulnerabilities. Cyber security must be at the forefront of the risk management agenda to safeguard against potential breaches.

— **Supply chain networks:** organisations place heavy reliance on third party suppliers as the Health and care ecosystem becomes increasingly connected; a complicated network of suppliers supporting operational needs opens up new avenues for exploitation, with multiple points of entry/infiltration. Organisations must engage in effective monitoring to ensure suppliers across the digital ecosystem safeguard sensitive data, and adhere to data security standards.

— **Integrated care:** the transition towards Integrated Care Systems (ICSs) for many organisations are transforming the delivery of patient care and design of the digital ecosystem, which requires seamless connectivity and data sharing between multiple health and care entities and providers (further expanding the attack surface). A proactive approach to enhancing cyber and data security measures and defence strategies exists at the core of this agenda.

CAF is coming to the Health sector

Public sector bodies will be required to transition to the adoption of the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF) as an assurance framework. This provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are managed by an organisation.

For the Health and care sector this will be done through or be aligned with the DSPT. Considering the shift in evidence requirements and changes in approach required under the CAF framework there will be a need to create a comprehensive and strategic approach to the transition. Steps for consideration may include:

Current state and Gap Analysis – A thorough assessment of current data security and protection posture and current Cyber Maturity, to determine the gap analysis as a foundation for the transition strategy.

Gap remediation – Addressing any gaps between the current control environment, versus alignment with the NCSC CAF.

CAF Readiness assessment – An assessment of the organisation and the revised controls in place based on a understanding of the with the incoming criteria, and mapping existing controls to the specific criteria outlined in CAF, to enable the organisation to be able to both meet the requirements and evidence those requirements on an ongoing basis.

This transition isn't just a shift in assurance framework, but an opportunity for organisations to bolster their data security and protection resilience and effectiveness. Every Health and Care organisation should be taking steps to ensure a secure and seamless adoption of the CAF, looking at the DSPT and wider data security controls to assess the investment and support required to meet the standards. Swift adoption will ensure they demonstrate compliance and continue to meet contractual requirements, whilst safeguarding patient data, managing cyber risk and maintaining essential services.

Executive Summary

The ICO's latest Incident Trend analysis (Q4 2022) shows that 20% of all incidents reported in the UK were in the Health and Care sector, the highest of any sector and 5% more than any other sector. Against this backdrop, and in the current climate and context of managing sensitive data, all entities with access to NHS patient data must provide verifiable guarantees that a robust foundation of controls has been established for data protection and security as set out by NHS England in the Data Security and Protection Toolkit (DSPT).

All 'Category 1' organisations are mandated to undergo independent evaluations of their self-assessments annually. This comprehensive benchmarking report highlights the key themes identified over the past five years, and sheds light on insights from our independent review of 28 organisations in 2023, with a combined income from patient care activities of **£16.8 billion.**

Since the inception of the DSP Toolkit in 2018/19, our annual benchmarking reports have consistently highlighted three critical areas of concern within health and social care organisations. These areas, characterised by persistently lower maturity levels, pose substantial risks to the integrity of patient data and the overall effectiveness of organisations in their ability to manage cyber risk and sustain services. The three areas, namely **user access management**, **business continuity**, and **third-party and supply chain vulnerabilities**, demand immediate focus and remediation. Failure to address these control weaknesses not only exposes health and care organisations to significant reputational damage, regulatory sanctions, and potential non-compliance with NHS E contracts in the event of a data breach, but jeopardises the security of patient data - potentially putting lives at risk. We explore these in detail on **slide 6**.

This year's benchmarking results indicate a notable improvement in maturity levels based on a stable set of assertions, attributed to a sustained commitment to continuously improving information governance practices. It is encouraging to note improvements in securing **connected medical devices** and **resiliency testing**; meaning services are less susceptible to disruption should the unexpected happen, and staff/patient data is less at risk of loss or compromise from cyber-attacks or other incidents. In practical terms, organisations are better equipped to protect patient data and maintain services, but as new vulnerabilities emerge and the threat landscape continues to evolve, organisations cannot afford to become complacent.

85% of organisations only achieved a moderate assurance rating, with 130+ findings across 28 reviews. This year the high risk findings were again in **user access management**, putting these organisations at higher risk of failure with significant impact due to technical or process shortcomings with their access controls. Immature access controls enable inappropriate access directly to patient data. While access controls have been a high risk finding for a number of years, **patching controls** and **mandatory induction training for data security and protection** saw a steep reduction in compliance, signifying that logical access and security controls were ineffective, and that the 'new' staff operating the controls were unaware of their responsibilities, leading to a potential significant weakness in protecting patient data effectively.

Without a focus on improvements and investment in all of these areas of lower maturity, there is a real risk of a staff/patient data breach which could have significant consequences, such as regulatory and contractual non compliance and negative reputational impact for a Health and Care organisation. The move to the NCSC CAF will also create a need to mature assurance methodologies accordingly.

What does this mean for my organisation?

Based on the key themes identified, three important questions must be asked.

Are new joiners trained and supported to understand their personal responsibilities in protecting patient data?

Is leaver's access removed in a timely manner to protect against inappropriate access and are there appropriate password controls in place for privileged access accounts?

Do you have clear understanding of the patching controls in place for protecting your key systems?

Please feel free to provide your anonymous responses to these questions using the QR code provided.

Bringing it to life…

The 2023 Verizon Data Breach Incident Report found that 74% of breaches involved a human element and over 50% of all incidents reported to the ICO in Q4 2022 were caused by human error. Showing that ensuring staff are trained in and aware of the responsibilities for data protection continues to be of the highest level of importance.

Bringing it to life…

Over a third of all Data Breaches in the Verizon report were due to inappropriate access and immature access controls. Accessing data through unremoved leavers or unmonitored privileged access is a known attack vector for Cyber attacks and fraud, highlighting the importance of proper user access and management controls.

Bringing it to life…

According to the NCSC Cyber Security Breaches Survey 2023, keeping up to date with patching devices and addressing security gaps has fallen across all sectors by over 12% in the past two years while the percentage of breaches caused by malware accessing networks through unpatched software now equates to 14% of all breaches[1].

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

Focus Areas

We have collated our results from our benchmarking reports since 2018 and we have noted that three areas of focus have arisen as persistent themes. We have outline the requirements for each area, and the ways in which KPMG can support you in strengthening controls. Further details can be found on slide 13.

User Access

A consistent issue covering privileged access, leavers access revocation and password management. Every year the maturity of these controls has consistently been lower than other assertions. While this is not a new problem it is still a major attack vector for fraud and cyber attacks.

So what can we do?...

Controlling access to online resources is a foundational tenant of strong information security. Once viewed as an operational back-office issue, Identity and Access Management (IAM) is now gaining visibility due to numerous high-level breaches occurring due to failure to manage and control user access effectively. KPMG can help you with IAM services spanning assessment, strategy, implementation and operations.

Business Continuity and Disaster Recovery

During a period of increased strike action, over burdened resourcing and a rising volume of cyber attacks the importance of BC/DR controls continues to grow. However a lack of mapped Recovery Point and Time Objectives and inconsistent BC/DR testing has left these controls ineffectively designed and tested.

So what can we do?...

Recent cyber breaches highlight the increasing sophistication, stealth, and persistence of cyberattacks that the NHS are facing today. Alongside this threat are well publicised data centre and core application outages. KPMG have an Integrated Resilience Framework which can help an organisation understand how IT can support the wider organisation effectively prepare for and respond to Business Continuity incidents.

We also conduct threat-led Business continuity and resilience exercises, tailored to your needs, that will enable you to take proactive measures to maintain your compliance, improve your resilience and respond confidently in the future and support the move to a more integrated resilience approach.

Third Party and Supply Chain Risk

A key risk for any organisation which relies on third parties for IT applications or infrastructure. The risk has manifested itself as recently as August 2023 for the Met Police. In this incident a third party supplier suffered a security breach, which the Met are accountable for under data privacy legislation as the data controller. This has led to a negative reputational impact and possible financial repercussions.

So what can we do?...

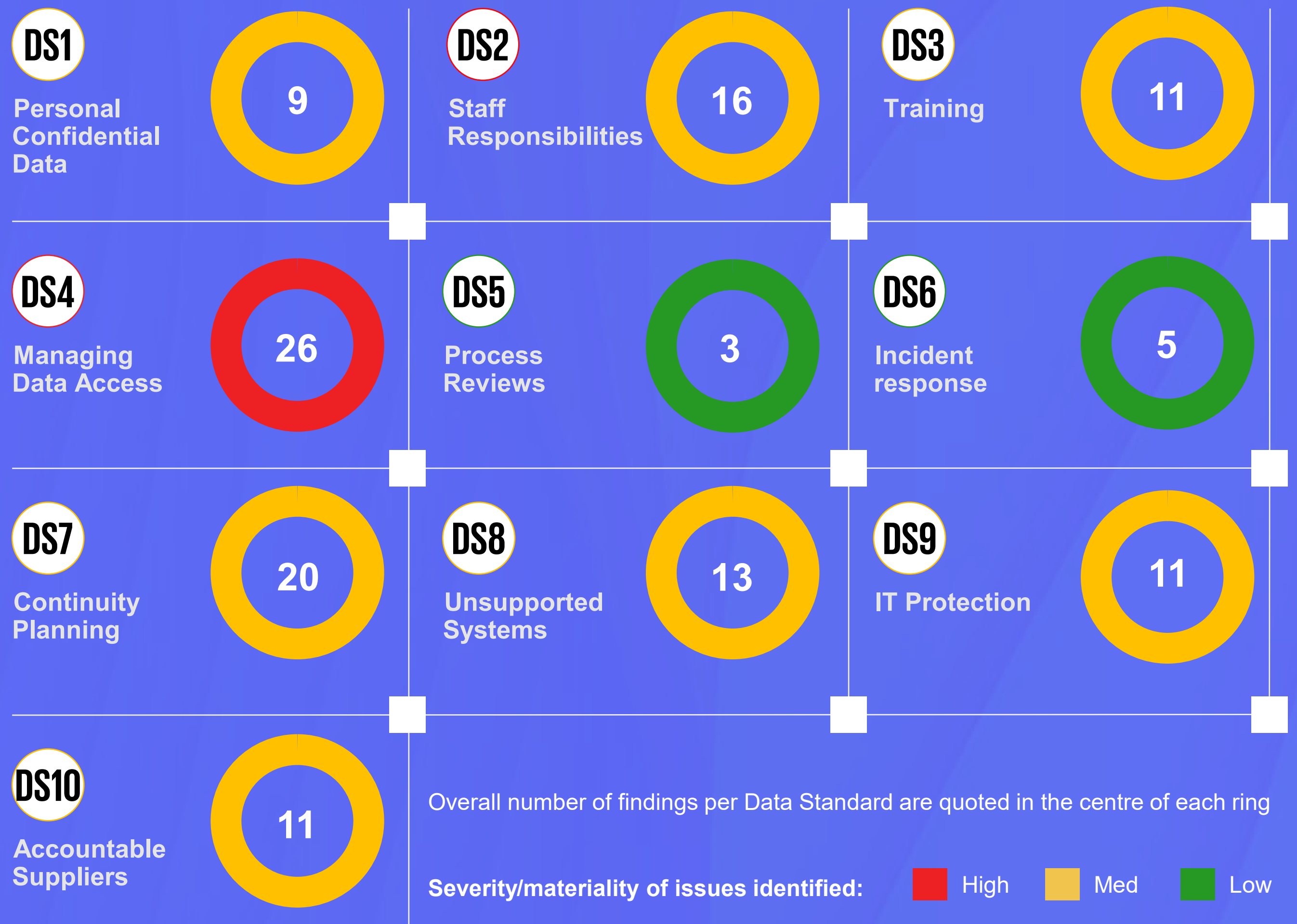
The increased reliance on third parties introduces risks and threats to a Trust's environment, intensifying the need for effective monitoring and appropriate controls to safeguard sensitive data and protect against cyber and privacy threats. KPMG can assess the Trust's readiness in mitigating risks associated with its third parties, review third party and supplier accreditations and look at how an organisation are managing procurement and due diligence of third parties and suppliers, ensuring that cyber security and data protection measures have been considered and aligned to industry best practice and regulatory requirements.

Heatmap

From the heatmap it is clear that organisations have effectively managed Process Reviews and developed an incident response process. However there is a disconnect between the incident response and the continuity planning which continues to be a significant area of lower maturity.

In light of the incoming CAF requirements, the lower maturity of continuity planning, combined with weaknesses in technical controls and staff understanding of their personal responsibilities highlights there is a real gap between the current controls maturity and the level of controls required under the CAF framework.

It will take a level of investment to close the gap and better secure patient and staff data going forward.



DS1 Personal Confidential Data 🟨 9

DS2 Staff Responsibilities 🟨 16

DS3 Training 🟨 11

DS4 Managing Data Access 🟥 26

DS5 Process Reviews 🟩 3

DS6 Incident response 🟩 5

DS7 Continuity Planning 🟨 20

DS8 Unsupported Systems 🟨 13

DS9 IT Protection 🟨 11

DS10 Accountable Suppliers 🟨 11

Overall number of findings per Data Standard are quoted in the centre of each ring

Severity/materiality of issues identified: 🟥 High 🟨 Med 🟩 Low

Key Statistics

64%

of participating Health and Care Organisations **did not achieve good maintenance of network access controls.** This creates a potential for inappropriate access to patient data and a known attack approach for Cyber and Fraud.

61%

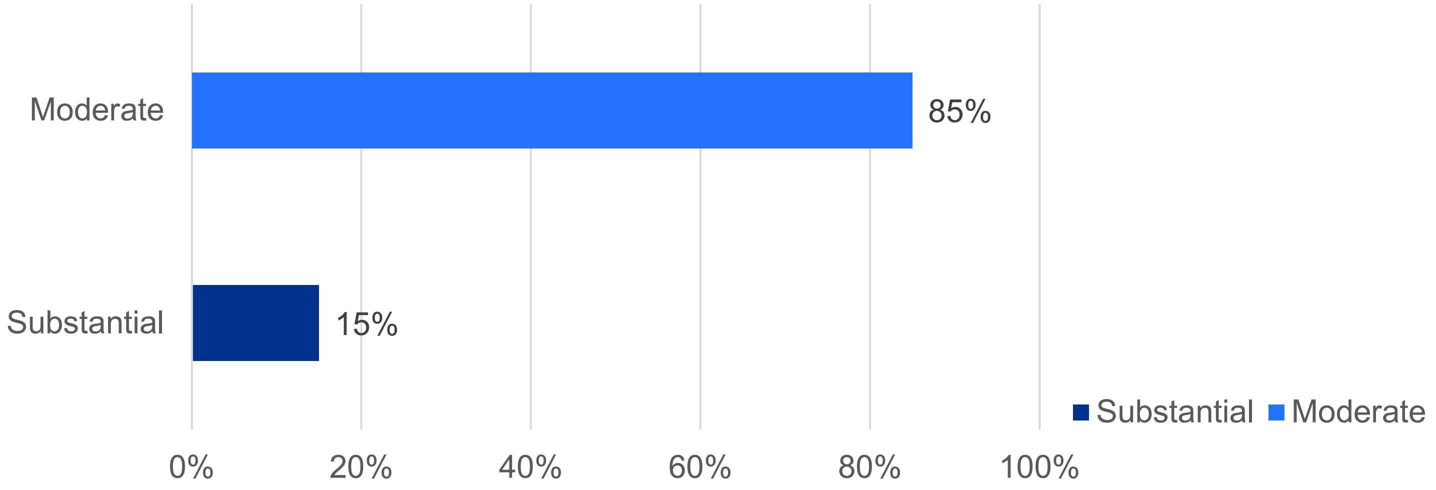
of participating Health and Care Organisations did not **conduct mandatory training for new joiners in a timely manner.** New employees may therefore not understand their personal responsibilities for data protection, while the organisation will still be accountable for any breach as the data controller.

50%

of participating Health and Care Organisations **failed to patch their key systems effectively.** Ineffective patching means systems and applications are vulnerable to cyber attack and unauthorised access to patient and staff data.

This chart shows how the level of assurance was distributed between the population of reports. The assurance levels are defined by NHS England.

It highlights that very few organisations receive substantial assurance and from our experience these organisations have relatively high resourcing in place including a Cyber Security Officer and a mature and stable controls set in place.



02

Collective Themes

- Access and Password Management
- New Staff Training Compliance
- Unsupported Systems

> “All organisations that have access to NHS patient information must provide assurances that they have the proper measures in place to ensure that this information is kept safe and secure.”

NHS England

DSPT Website
Help (dsptoolkit.nhs.uk)

Access and Password Management

What we found

Only **14%** of Health and Care Organisations were compliant with assertions 4.1, 4.2 and 4.5. The remaining majority were unable to identity and access control for it's networks and information systems whilst ensuring passwords are proportionate and suitable for the information being protected. All our high priority findings this year were in assertion 4.2.

Common root cause

- Inadequate monitoring and oversight of access controls, resulting in poor revocation of user access.
- Limited or no periodic review of privileged user access accounts.
- No defined high-strength password criteria for privileged accounts, social media accounts and infrastructure components.
- Lack of a log retention policy or appropriate retention schedules for the information held.

What should you do to achieve compliance?

- ✓ Define password criteria for all user account types and ensure default passwords are changed.
- ✓ Ensure leaver accounts are removed in a timely manner.
- ✓ Perform periodic user account reviews, including a focus on privileged accounts.
- ✓ Establish robust processes for managing privileged accounts. Implement multi-factor authentication where possible to enhance security.
- ✓ Ensure logs are retained for at least six months and a formal policy is in place to support.

NDS 4 – Managing Data Access

Assertions tested:

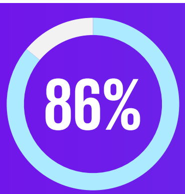
4.1 The organisation maintains a current record of staff and their roles.

4.2 The organisation assures good management and maintenance of identity and access control for it's networks and information systems.

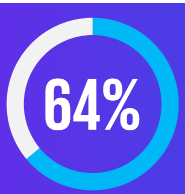
4.5 the organisation ensures that passwords are suitable for the information protected.

Our findings covered:

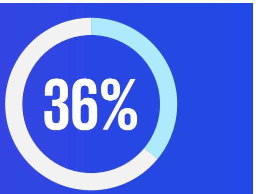
- User audit
- Log retention
- Leavers' access
- Password policy and technical controls to enforce
- Multifactor authentication for privileged user access
- Default passwords and social media accounts



of participating Health and Care Organisations failed at either 4.2 or 4.5.



of participating Health and Care Organisations either do not have appropriate log retention schedules or do not remove leaver's access in a timely manner.



of participating Health and Care Organisations do not have appropriate password management criteria for privileged and social media accounts.

New Staff Training Compliance

What we found

Only 39% of Health and Care Organisations had effectively managed all new joiners completed their data security and data protection induction training shortly after joining the organisation.

Common root cause

- The importance and urgency of completing the training may not be effectively communicated to the new staff.
- There may be limited consequences for non-compliance, and new staff members may not perceive the critical requirement for the repercussions or accountability measures required to encourage training completion.
- The training materials or resources provided to new staff may not be adequate or easily accessible.

What should you do to achieve compliance?

- ✓ Review the list of new starters and send mandatory learning deadline reminders on a regular basis.
- ✓ Monitor the compliance of new joiner training completion to ensure training is completed by all new joiners in line with the Trust policy.
- ✓ A full review of the policy and an enforcement procedure being discussed and decided upon during a meeting where senior management is present.
- ✓ Identify non-compliance of induction training and escalate to line managers or IG.

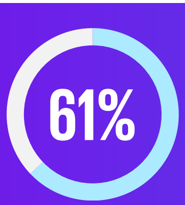
NDS 2 – Staff Responsibilities

Assertions tested:

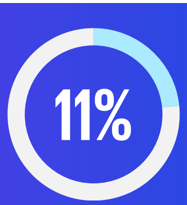
2.1 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.

Our findings covered:

- Data security and data protection induction training compliance.



of participating Health and Care Organisations did not have their all new joiners completed induction training within agreed timeline.



fall in compliance from 21/22 – 22/23. The single biggest fall in level of compliance of any assertion tested.

Unsupported Systems

What we found

Only **50%** of Health and Care Organisations had an adequate patching policy and effectively kept their supported systems up-to-date with the latest security patches.

Common root cause

- Lack of documented and well-defined patching policy.
- Inadequate documentation of the risk acceptance provided by a senior information risk officer (SIRO).
- The absence of a classification system for prioritisation of patches (based on severity or criticality) can hinder effective patch management.
- Lack of registration of the NCSC Early Warning Service.
- Lack of evidence to support new sub assertions 8.3.6 – 8.3.8

What should you do to achieve compliance?

- ✓ Draft and approve a comprehensive patching policy that outlines responsibilities, patch classification process, and patching schedule.
- ✓ Clearly document the SIRO's risk acceptance for patching activities to delegate obligations accordingly and to streamline the decision-making processes.
- ✓ Review and update the Patching Policy on a regular basis.
- ✓ Register with the NCSC Early Warning Service to monitor malicious activities that may have been detected in information feeds.

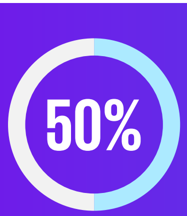
NDS 8 – Unsupported systems

Assertions tested:

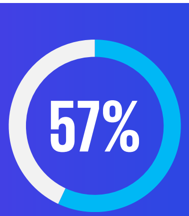
8.3 Supported systems are kept up-to-date with the latest security patches.

Our findings covered:

- Patch management procedure and policy
- SIRO's risk acceptance
- Implementation of Advanced Threat Protection (ATP)
- Server estate and desktop estates compliance on supported versions of operating systems (OS)
- NCSC Early Warning Service



of participating Health and Care Organisations did not document their patching policy or did not



of participating Health and Care Organisations either did not have 95% server estate or 98% desktop estate on supported versions of OS.

Comparison to previous years

We have highlighted the most relevant findings from the 2022/23 assessment, and included comparison with our previous 2021/22 benchmarking report. This identifies persistent vulnerabilities and noteworthy challenges, including areas not subjected to testing in the 2022/23 cycle.

🟢

Finding 1

Sensitive System Protection

This year, nearly half of participating Organisations were unable to provide adequate evidence to demonstrate that systems which handle sensitive information or key operational services are protected from exploitation of known vulnerabilities. (9.3)

KPMG Insight

Just over half of organisations passed this assertion, compared to only one in five in 21/22 due to a better understanding of ‘new sub assertions’ in their second year of testing.

🟢

Finding 2

Incident Response and Continuity Planning

In 22/23 two thirds of participating Organisations completed an effective test of the continuity plan, and had adequate management processes in place to reduce the risk during and after an incident. (7.2 & 7.3)

KPMG Insight

In 21/22 only one third of organisations successfully met 7.2 and 7.3 requirements. In 22/23 RPO and RTO controls remained immature but evidence of Business Continuity testing improved significantly.

🔴

Finding 3

Access and Password Management

Almost 90% of participating Organisations failed at either 4.2 or 4.5. Two thirds did not have appropriate log retention schedules and over a third did not have password criteria for privileged and social media accounts. (4.2 & 4.5)

KPMG Insight

In 21/22 one in three organisations complied with standard 4,in 22/23 this low compliance level halved again. Leavers controls and privileged access have seen significant drops in the maturity of these controls.

🔴

Finding 4

New Joiner Training Compliance

Almost two thirds of participating Organisations did not conduct mandatory training for all new joiners in a timely manner. (2.1)

KPMG Insight

Compliance dropped by over 10 compared to 21/22. A drop in compliance was partly caused by operational pressures such as strike action, back logs and seasonal pressures.

🟢

Finding 5

Vulnerability Management

82% of participating Organisations had a proportionate monitoring solution to detect cyber events on systems and services and implemented transactional monitoring techniques. (6.3)

KPMG Insight

Compliance improved from just over half in 2021/22 to almost nine in every ten in 2022/23. This indicates a more effective approach to identifying and addressing vulnerabilities.

🔴

Finding 6

Third Party / Supplier Management

Almost half of all Organisations had not completed the required list of suppliers, products and services they deliver, and the contract durations. (10.1)

KPMG Insight

Compliance fell by 10% from last year and with the increasing reliance on third party solutions this highlights a significant area of concern.

Improved maturity 🟢 **Lower maturity** 🔴

03

Appendices

> Data from across the whole population, is used to monitor and improve care, and it's one of the great strengths of our health service.
>
> But we all know that our health and care information is sensitive, and needs to be kept safe.

NHS Digital website

[How data is used to improve health and care - NHS Digital]

Background and approach

Background

The recent political climate has driven unprecedented digital transformation throughout health and care, magnifying the importance of managing and handling personal identifiable information legally, securely, efficiently and effectively. In April 2023, the National Cyber Security Centre (NCSC) issued guidance informing readers about the threat to UK industry and society from cyber tools and services[2].

The Data Security and Protection Toolkit (DSPT) was updated in response to the changing digital landscape for 2022/23, and continues to provide the means for Health and Care Organisations to self-assess their ability to meet a national benchmark for information governance against the National Data Security Standards. It also provides valuable insight into the technical and operational data security and data protection control environment and relative strengths and weaknesses of those controls.

The assertions mandated for testing by NHS Digital* (NHS D) in 22/23 remain the same as 21/22, with minor updates to sub assertions and evidence requirements. As a result, our report has assessed the shift in compliance (as well as emerging risks) year-on-year, providing insight into where limited time and resources could be effectively focused.

*NHS Digital merged with NHS England in February 2023.

Methodology

Confidential benchmarking study with 28 Health and Care Organisations to assess their current state performance against thirteen mandatory DSPT assertions.

Aggregated and analysed the results to identify areas of priority and challenge.

Presented the analysis and KPMG's interpretation of the results, as contained within this report.

Benchmark Approach

This year's submission deadline was 30 June 2023 and our KPMG benchmark covers the period April 2022 – June 2023.

Our DSPT benchmark gives readers of this report a point in time view of performance against the DSPT across the UK, at the time our reviews were conducted.

Prior to 2018, NHS Digital would publish the scores of the submissions following the deadline, however under the section 254 Direction they were unable to do so last year, or going forwards. As such our report is a means to understand the sector, what good looks like, and where you sit as an organisation when compared to your peers.

[2] https://www.ncsc.gov.uk/information/cyber-essentials-technical-requirements-updated-for-april-2023?ref=hackernoon.com

Assertions benchmarked in the 22/23 audit year

We have provided below the list of the standards assessed this year, alongside the compliance level of Health and Care Organisations assessed by KPMG as identified at the time of the review through the average percentage of compliance.

Data Security Standard 1

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

64%

Assessed Sub Assertions:

1.3.1
1.3.2
1.3.3
1.3.4
1.3.5
1.3.6
1.3.7
1.3.8
1.3.9

Data Security Standard 2

All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

39%

Assessed Sub Assertions:

2.1.1

Data Security Standard 3

All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit.

54%

Assessed Sub Assertions:

3.4.1
3.4.2

Data Security Standard 4

Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

64%

Assessed Sub Assertions:

4.1.1
4.1.2
4.2.1
4.2.3
4.2.4
4.5.1
4.5.2
4.5.3
4.5.4

Data Security Standard 5

Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

89%

Assessed Sub Assertions:

5.1.1

Assertions benchmarked in the 22/23 audit year

We have provided below the list of the standards assessed this year, alongside the compliance level of Health and Care organisations assessed by KPMG as identified at the time of the review through the average percentage of compliance.

Data Security Standard 6

A confidential system for reporting data security and protection breaches and near misses is in place and actively used.

82%

Assessed Sub Assertions:

6.3.1

6.3.2

6.3.3

6.3.4

Data Security Standard 7

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.

64%

Assessed Sub Assertions:

7.2.1

7.2.2

7.3.1

7.3.2

7.3.4

7.3.5

7.3.6

Data Security Standard 8

No unsupported operating systems, software or internet browsers are used within the IT estate.

50%

Assessed Sub Assertions:

8.3.1

8.3.2

8.3.3

8.3.4

8.3.5

8.3.6

8.3.7

8.3.8

Data Security Standard 9

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.

57%

Assessed Sub Assertions:

9.3.1

9.3.3

9.3.4

9.3.5

9.3.6

9.3.7

9.3.8

9.3.9

Data Security Standard 10

A list of suppliers, the products and services they deliver, and the contract durations is in place.

57%

Assessed Sub Assertions:

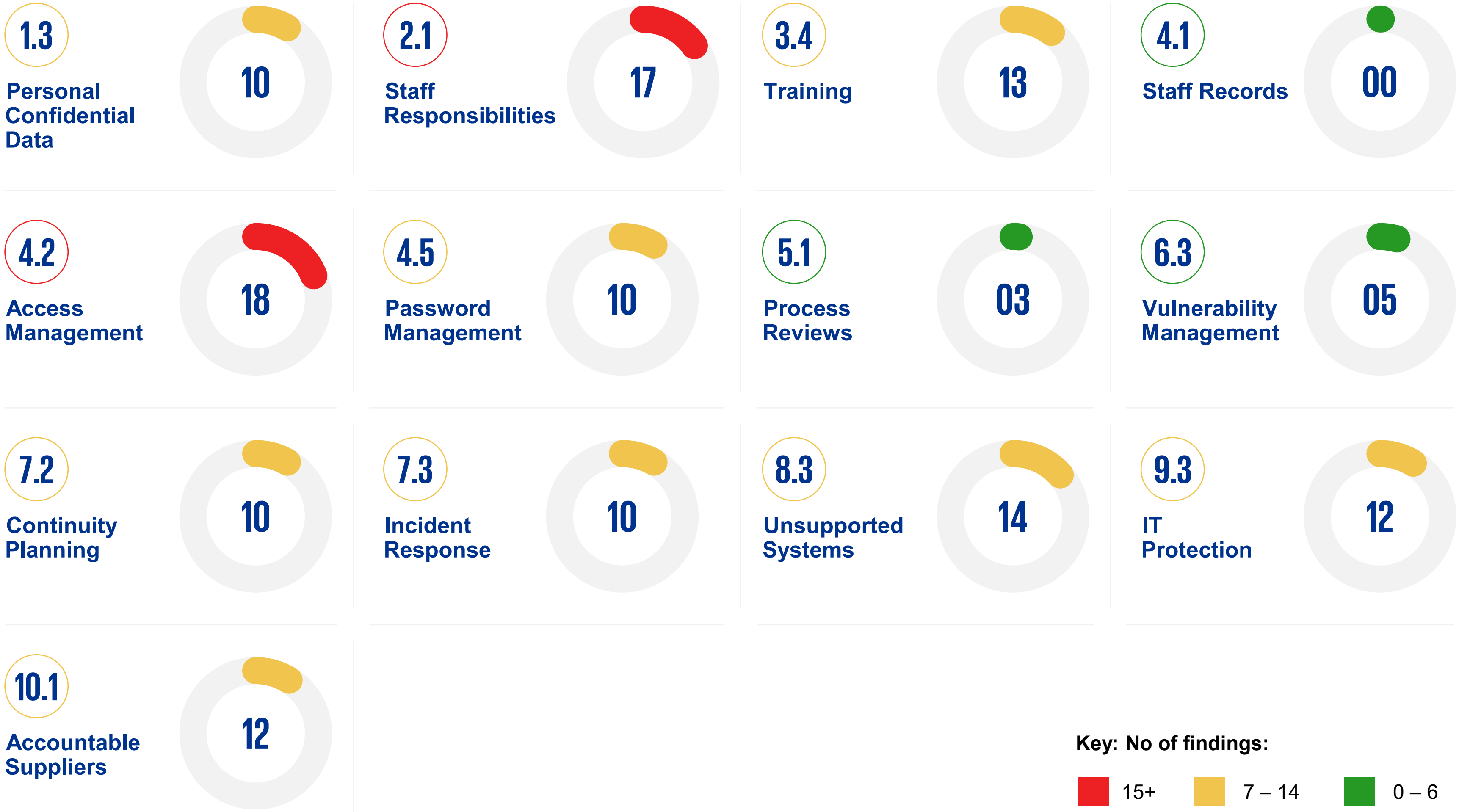
10.1.1

What we found by assertion: FY22/23 Findings

A view per assertion reviewed

We have highlighted how many findings there were by each assertion, and included a RAG rating for reference to show common areas of focus following the 2022/23 submission.

The RAG rating show high maturity in staff records, process review and vulnerability management and low maturity in access management and staff responsibilities (induction training).



1.3	Personal Confidential Data	10
2.1	Staff Responsibilities	17
3.4	Training	13
4.1	Staff Records	00
4.2	Access Management	18
4.5	Password Management	10
5.1	Process Reviews	03
6.3	Vulnerability Management	05
7.2	Continuity Planning	10
7.3	Incident Response	10
8.3	Unsupported Systems	14
9.3	IT Protection	12
10.1	Accountable Suppliers	12

Key: No of findings:

🟥 15+ 🟨 7 – 14 🟩 0 – 6

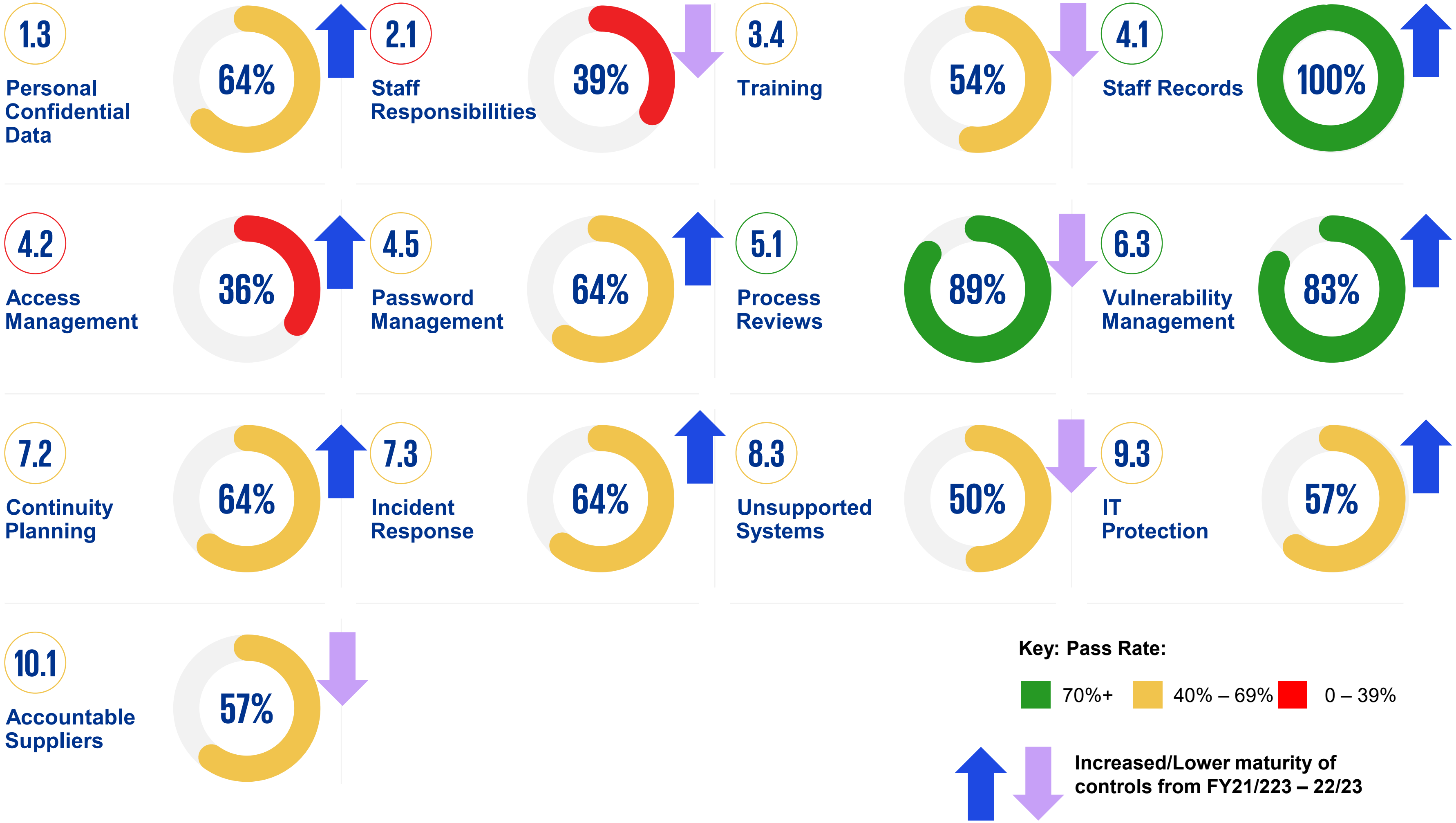
What we found by assertion: FY22/23 Pass Rate

A view per assertion reviewed

We have highlighted the pass rate per assertion, and included a RAG rating for reference to show common areas of focus following the 2022/23 submission.

In FY 21/22 we assessed the same assertions as FY 22/23 as per NHS England's guidance, and have highlighted the change in maturity of controls year-on-year.

Access management and staff responsibilities are the assertions with the lowest pass rates. From this slide it is clear that access management shows a sight improvement on last year, although still a significant issue, where as staff responsibilities saw a significant drop in compliance.



Key: Pass Rate:

🟩 70%+ 🟨 40% – 69% 🟥 0 – 39%

↑ ↓ **Increased/Lower maturity of controls from FY21/223 – 22/23**

What we found by assertion: FY21/22 Pass Rate

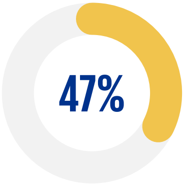
A view per assertion reviewed

We have highlighted the pass rate per assertion, and included a RAG rating for reference to show common areas of focus following the 2021/22 submission.

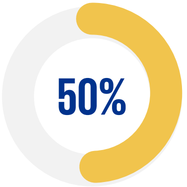
In FY 21/22 we assessed the same assertions as FY 22/23.

Last year the lowest areas of compliance were Access and Password management, Incident response (Business Continuity testing) and IT Protection. After receiving additional focus last year all four areas saw improvements in 22/23.

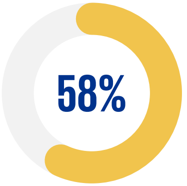
1.3 Personal Confidential Data



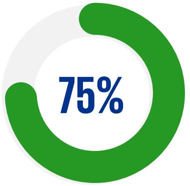
2.1 Staff Responsibilities



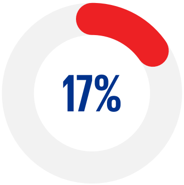
3.4 Training



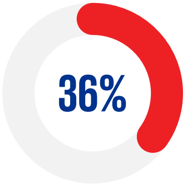
4.1 Staff Records



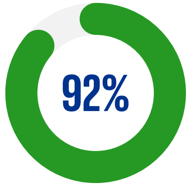
4.2 Access Management



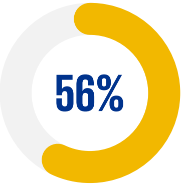
4.5 Password Management



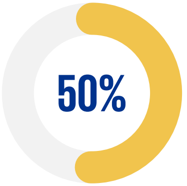
5.1 Process Reviews



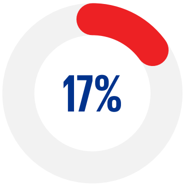
6.3 Vulnerability Management



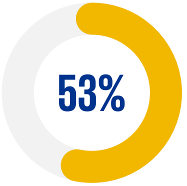
7.2 Continuity Planning



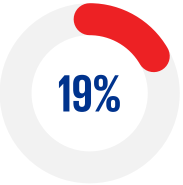
7.3 Incident Response



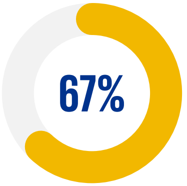
8.3 Unsupported Systems



9.3 IT Protection



10.1 Accountable Suppliers



Key: Pass Rate:

🟩 70%+ 🟨 40% – 69% 🟥 0 – 39%

Disclaimer

About this Report

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG

Contacts:

Raj Cheema

Digital Healthcare
Partner

M +44 (0)7795 354 415
E: rajvir.cheema@kpmg.co.uk

Tim Colclough

Technology Risk
Senior Manager

M +44 (0)7887 826 733
E: tim.colclough@kpmg.co.uk

Louisa Villeneuve

Technology Risk
Manager

M +44 (0)7786 688 294
E: louisa.villeneuve@kpmg.co.uk

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.

kpmg.com/uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Document Classification: KPMG Public

CREATE: CRT150477A

Benchmarking Feedback Survey