Welcome to the Finance, Performance and Cyber Assurance Event

30th September 2019
Principal Hotel, York

CCGs working together

Airedale, Wharfedale and Craven CCG
Bradford City CCG
Bradford Districts CCG

The Roles of the Audit Committee and Finance Committee with regard to Finance and Performance

Bryan Millar

Audit Committee Chair at Airedale, Wharfedale and Craven CCG, Bradford Districts CCG and Bradford City CCG

Bryan Millar - NHS Career

Treasurers Department roles

- Newcastle Area Health Authority 1977 – 1984
- Northumberland Health Authority 1984 – 1986
- Bradford Health Authority 1986 - 1988

Senior/Management roles

- Northern Regional Health Authority 1988 – 1991
- North Tyneside Health Authority 1991 - 1993

Executive roles

- Director of Finance & Performance Management Northgate & Prudhoe NHS Trust 1993 - 1999

NHS Career continued...

Director of Finance

- Bradford Community Health NHS Trust 1999-2002

DoF/Deputy CEO

- Bradford S&W PCT 2002-2005
- Bradford Teaching Hospitals NHS FT 2005 - 2011

Chief Executive

- Bradford Teaching Hospitals NHS FT 2011 - 2014

Non-Executive roles

- Audit Chair, Bradford (& Craven) CCGs 2014 - present

Key governance related developments during this time

Early 1990s

- Internal Market
- Health Authority and GP commissioners
- Self governing Trusts

- Commercial governance models -
  - Board of Directors
  - Audit Committee
  - Remuneration Committee
  - External Auditor Appointments
  - Organisational Annual Accounts and Reports

Key governance related developments during this time

Mid/Late 1990's

- Board meetings held in public
- Clinical Governance

Early 2000's

- PCTs
- Foundation Trusts

- Democratisation - members, governors etc.
- Local appointment of External Auditors
- Quality Accounts
- Increasing development of Board Committees (Quality, Finance, Performance etc)
- CCGs
- Management of Conflicts of Interest
- Partnership commissioning arrangements

Audit Committee v Finance Committee

Audit Committee	Finance Committee
• Committee of the Governing Body • Well established, standardised role. • Core element of universal corporate governance arrangements • Holds Chair, CEO, CFO to account • Oversees Conflicts of Interest management • Independent	• Piecemeal development and implementation • Various models and scope of responsibility • May report to both Clinical Board and Governing Body (in CCGs) • Hybrid performance management/governance remit (e.g. where ToRs include both performance oversight and policy approval) • Accountabilities and independence clouded by mix of Exec/non-exec/Clinician membership • Conflicts of Interest may require active management

Complementary roles of Finance and Audit Committees (Cyber/IT)

IT Server Failure - Bradford CCGs

Pre - incident	Post incident - immediate/operational	Post-incident - long term/strategic
Audit Committee	Finance Committee	Audit Committee
• Regular review of risk registers • Identification of IT resilience risk • Development of Mitigation plans	• Approval of action plans (based upon previously identified mitigations) Authorisation of financial consequences • Oversight of action plan delivery • Monthly follow-up on behalf of Governing Body/Clinical Board	• Deployment of Internal Audit to review effectiveness and comprehensiveness of response • Review of updated risk registers and future-proofing of service delivery

Role of the Finance/Performance Committee in modern governance arrangements - key considerations

- Purpose and remit (oversight, assurance, decision making, policy, other?)
- Membership?
- Effectiveness?
- Added value?
- Boundaries/overlap?
- Transparency?

Finance, Performance and Cyber Assurance Event

Cathy Kennedy
Director of Operational Finance for Yorkshire and Humber
30 September 2019

NHS England and NHS Improvement

NHS England & NHS Improvement

Finance and Performance - Expectation of Providers & Commissioners

Content

NHS England and NHS Improvement (NHSE/I) Regulation Frameworks

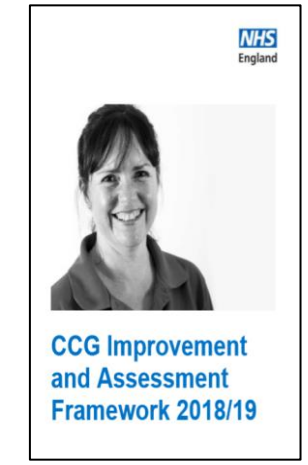
Escalation and Improvement

Emerging role of Systems

Regulation Frameworks

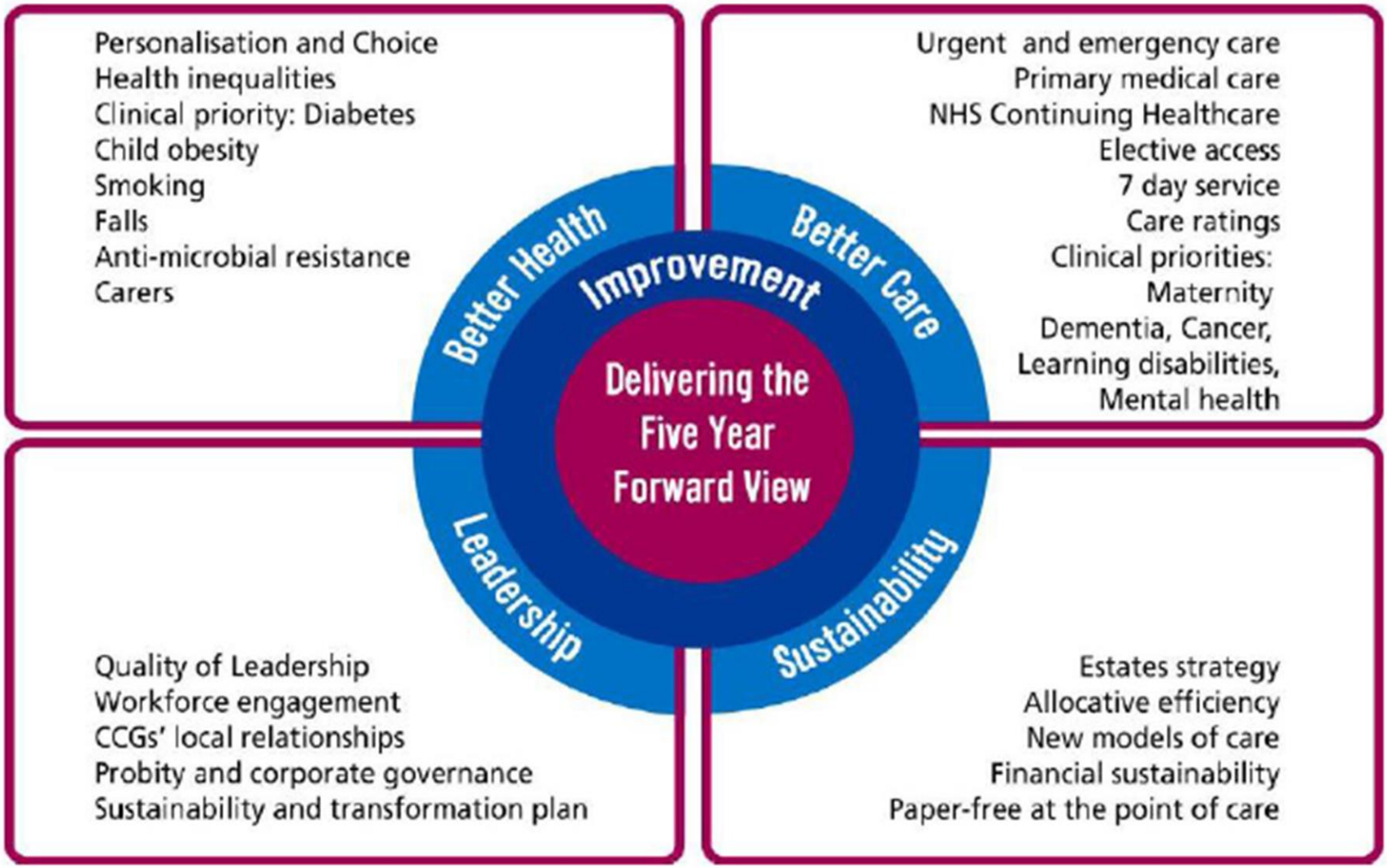
- Provider (NHSI) – Single Oversight Framework (Updated Nov 17)
    - Sets out how NHS Trusts and NHS Foundation Trusts are overseen.
    - Helps to determine the type and level of support needed to meet these requirements.
    - Objective is to help providers to attain and maintain Care Quality Commission ratings of 'Good' or 'Outstanding', meet NHS constitutional standards and manage resources effectively, working alongside their local partners

- CCG (NHSE) – Improvement & Assessment Framework (Updated 18/19)
    - Introduced in March 2016 – aligning key objectives and priorities informing the way NHSE managed its relationships with CCGs.
    - Designed to supply indicators for adoption in healthcare systems as markers as success.



Single Oversight Framework (SOF) themes

Improvement & Assessment Framework (IAF)



Organisation assessment

Provider

SOF Segments – NHSI continuous assessment

- SOF 1 Maximum Autonomy
- SOF 2 Targeted Support
- SOF 3 Mandated Support and Undertakings
- SOF 4 Special Measures

Use of Resources Assessment – NHSI support to CQC assessment

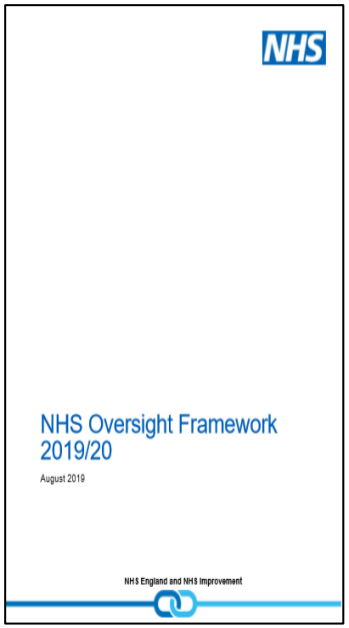
Commissioner

IAF Ratings – Annual NHSE assessment

- Outstanding
- Good
- Requires Improvement
- Inadequate

New NHS Oversight Framework for 2019/20

- Single NHS Oversight Framework for overseeing organisational performance and identifying where commissioners and providers may need support
- Pulls together provider SOF and commissioner IAF, no change to assessment processes
- No changes to business rules and minimal changes to metrics (addition of specific staff survey metrics)
- Oversight managed by new joint NHSE/I region teams
- Focal point for joint work, support and dialogue between NHSE, NHSI, CCGs, providers and STPs/ICSs
- Key change: **system based approach, working through and with system leaders**



Impact of integrated oversight

- NHSE/I is increasingly holding local (Place) system partners collectively to account for delivery of performance and financial plans where the overall local system is challenged

- NHSE/I is holding ICS systems (i.e. their collective constituent partners) to account for joint overall delivery of annual plans and performance

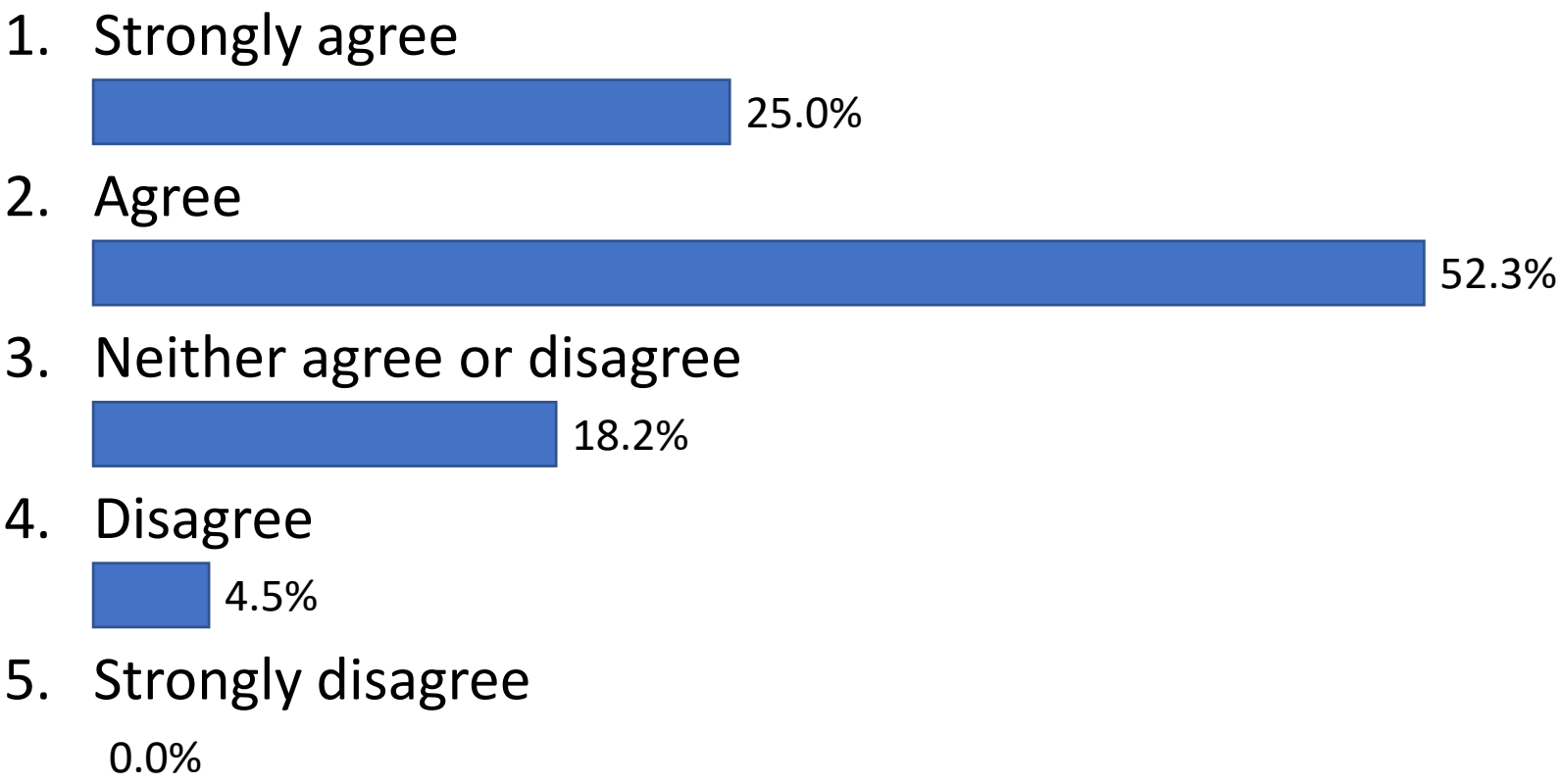
- Inconsistency in provider and commissioner finance, contract and performance planning/delivery is visible to the joint NHSE/I teams

- Chairs and NEDs will need to help to guide decisions of their Boards and hold the Executive Directors to account for delivery within the expectations of this new integrated oversight environment

This means that it is no longer acceptable for an organisation to plan or deliver performance requirements by taking decisions/actions that have an adverse impact on the wider system (local Place or wider ICS)

Vote Now

Integrated NHSE/I oversight framework and management arrangements will support better overall NHS performance than the previous separate NHSE and NHSI processes and teams



My organisation's board and senior leadership understand the new integrated oversight framework, and it's expectations for us and our partners, sufficiently well to take informed decisions and operate effectively in this new environment

Vote Now

1. Strongly agree

   0%

2. Agree

   5%

3. Neither agree or disagree

   60%

4. Disagree

   35%

5. Strongly disagree

   0%

Escalation and Improvement Support

NHS England and NHS Improvement

Key Escalation Triggers (Finance and Performance)

Emerging delivery issues

- Oversight framework metrics
- Operational plan trajectories
- Recovery trajectories
- Lack of prediction and mitigation of risks

Other factors

- Investigation findings
- Other regulator assessments e.g. CQC
- Engagement in system working and transformation
- Service and financial sustainability

What influences NHSE/I escalation decisions

- The extent to which an organisation or system is triggering a concern within the oversight framework
- Which trigger(s) are of concern
- Any associated circumstances the organisation or system is facing
- The degree to which the organisation or system understands what is driving the issue
- Whether there is a breach or suspected breach of provider licence conditions and/or commissioner regulations
- Organisation capability and the credibility of plans to address the issue
- Organisation governance and leadership track record
- View of system leaders (health and local authority)

Escalated Oversight arrangements

Escalated arrangements are established with the objective of supporting rapid and sustained performance recovery.

They could include some or all of:

- Recovery plans
- Greater regulator oversight and monitoring (seniority, frequency, detail)
- Targeted and mandated support
- SOF / IAF rating change
- Legal redress e.g. Undertakings (provider); Directions (CCGs)

The same issue would result in different regulator oversight escalation and intervention depending on the capability and governance demonstrated by the organisation

Examples of Support

- Focused service improvement initiatives e.g. maternal and neonatal health and safety collaborative
- Practical help to address key improvement priorities e.g. Emergency Care Improvement Programme
- Leadership development, coaching and mentoring
- Resources to help develop capability to improve and apply evidence-based improvement methodologies
- Resources to help improve quality, efficiency and productivity including the Rightcare, Model Hospital , Getting it Right First Time, Bronze Pack
- Targeted financial recovery support
- External specialist support
- ICS/STP transformation programmes
- Dedicated support and development for organisations in (or at risk of being in) licence breach, special measures or directions

The same issue will result in different NHSE/I-directed support depending on the capability and capacity for improvement demonstrated by the organisation and system (some of which the organisation may be required to fund)

Vote Now

My organisation has highly effective arrangements in place to predict and mitigate risks to delivery of the performance and financial expectations of NHSE/I

1. Strongly agree

2.9%

2. Agree

48.6%

3. Neither agree or disagree

40.0%

4. Disagree

8.6%

5. Strongly disagree

0.0%

Vote Now

I am confident that if performance were to be significantly off track on a key metric, our organisation can demonstrate the necessary attributes to minimise NHSE/I escalation and mandated support

1. Strongly agree

3%

2. Agree

35%

3. Neither agree or disagree

57%

4. Disagree

5%

5. Strongly disagree

0%

Emerging role of Systems

NHS England and NHS Improvement

Working as Systems

- Increasing emphasis on role of systems at local (Place) level and STP/ICS level in supporting improvement and delivery of the Long Term Plan across the NHS
- Relies on collaborative and partnership approach
- As systems mature they are expected to take greater shared responsibility for overall quality of care and use of resources for their population

• South Yorkshire and Bassetlaw	Wave 1 ICS
• West Yorkshire and Harrogate	Wave 2 ICS
• Cumbria and North East	Wave 3 ICS
• Humber Coast and Vale	STP

ICS role increases as partnership maturity, governance and capability is demonstrated, with commensurate reduction in NHS England and Improvement role

The LTP committed to every STP becoming an Integrated Care System (ICS) by 2020/21.

System Maturity Matrix

- Provides characteristics of STPs and ICSs at different levels of maturity along the following domains:
  - System leadership, partnerships & change capability
  - System architecture, financial management and planning
  - Integrated care models
  - Track record of delivery
  - Coherent and defined population

- A “thriving” ICS will be able to demonstrated robust governance, advanced progress and real system-working at all levels, across each of these components

- For Regions to use when determining whether a system is ready to become an ICS

What does this mean in practice – in year

Finance and performance oversight and improvement example

- ICS governance leads to cessation of NHSE/I routine IAF and QRM meetings, replaced by ICS-led quarterly local (Place) discussions
- If organisation performance is off-track the ICS leads escalated performance oversight and improvement, supported by NHSE/I teams*
- ICS operates 'offset' of individual organisation over-performance and under-performance within ICS overall control total and trajectories

** Up to the point of formal regulatory action which remains NHSE/I responsibility*

Transformation example

- Transformation funding is allocated to ICS
- The transformation programme, and the use of resources to support delivery, is determined by the ICS

What does this mean in practice – Planning

- Capital investment priorities are informed by STP/ICS through estate strategies and STP capital submissions
- ICS/STPs are responsible for NHS Long Term Plan (LTP) submissions for collective delivery and each organisation's trajectories within that
- More mature ICS's are leading the process, supported by NHSE/I teams (and vice versa)
- All commitments must be reflected as they have already been prioritised
- The application of some financial framework flexibilities will be influenced (determined?) by ICS's

Key elements of the Long Term Plan financial framework

Control Totals

- Organisational control totals
- STP/ICS system control totals

Financial Recovery Fund (FRF)

- FRF allocations will reflect ICS and organisation trajectories, supporting financial stability & improvement
- Size to be reduced over 5 year period

Financial trajectories

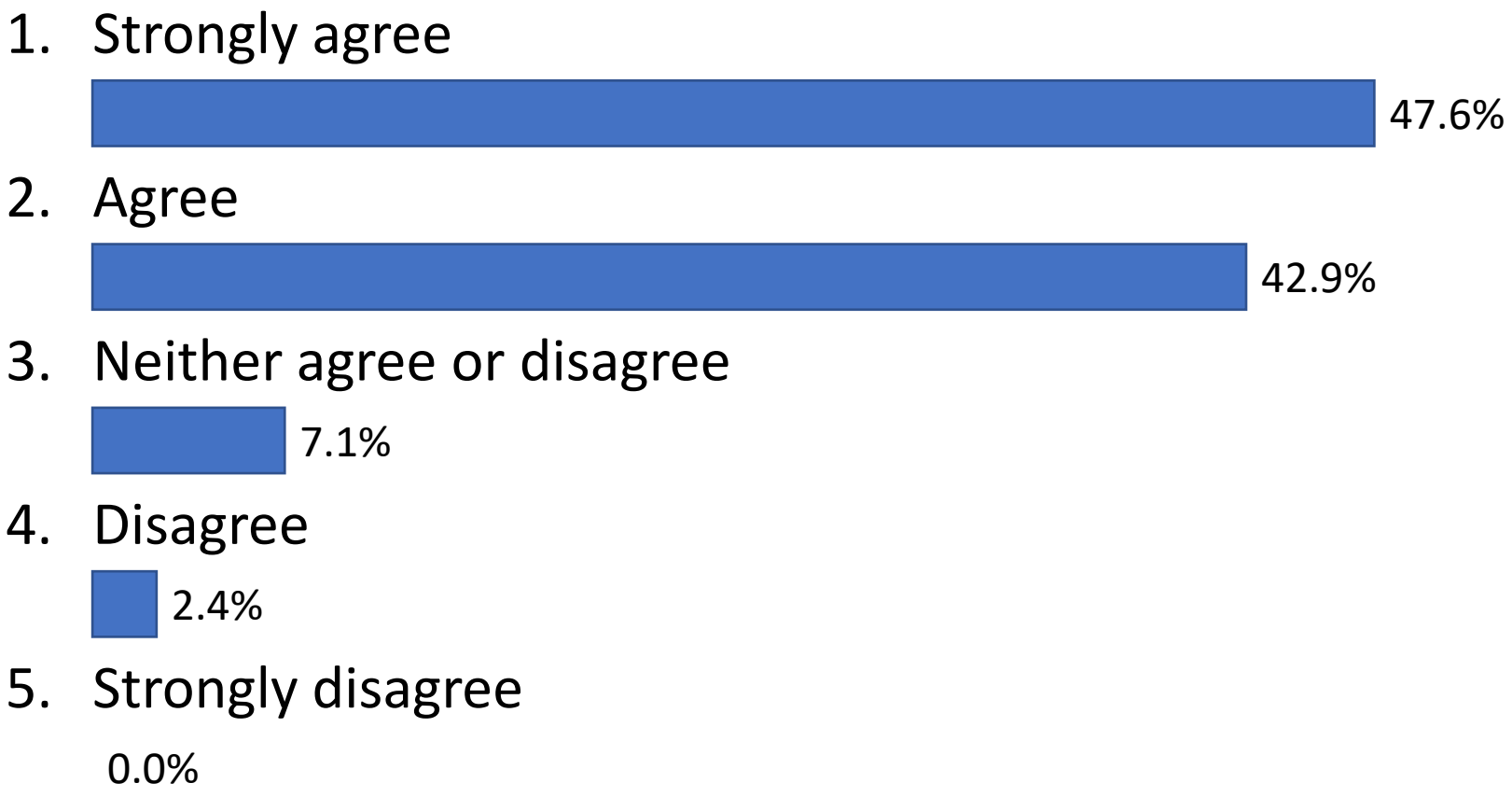
- ICS trajectory set nationally
- Organisation trajectories subject to ICS/STP discussions

Payment Reform

- Blended payment model
- Reform of CQUIN framework

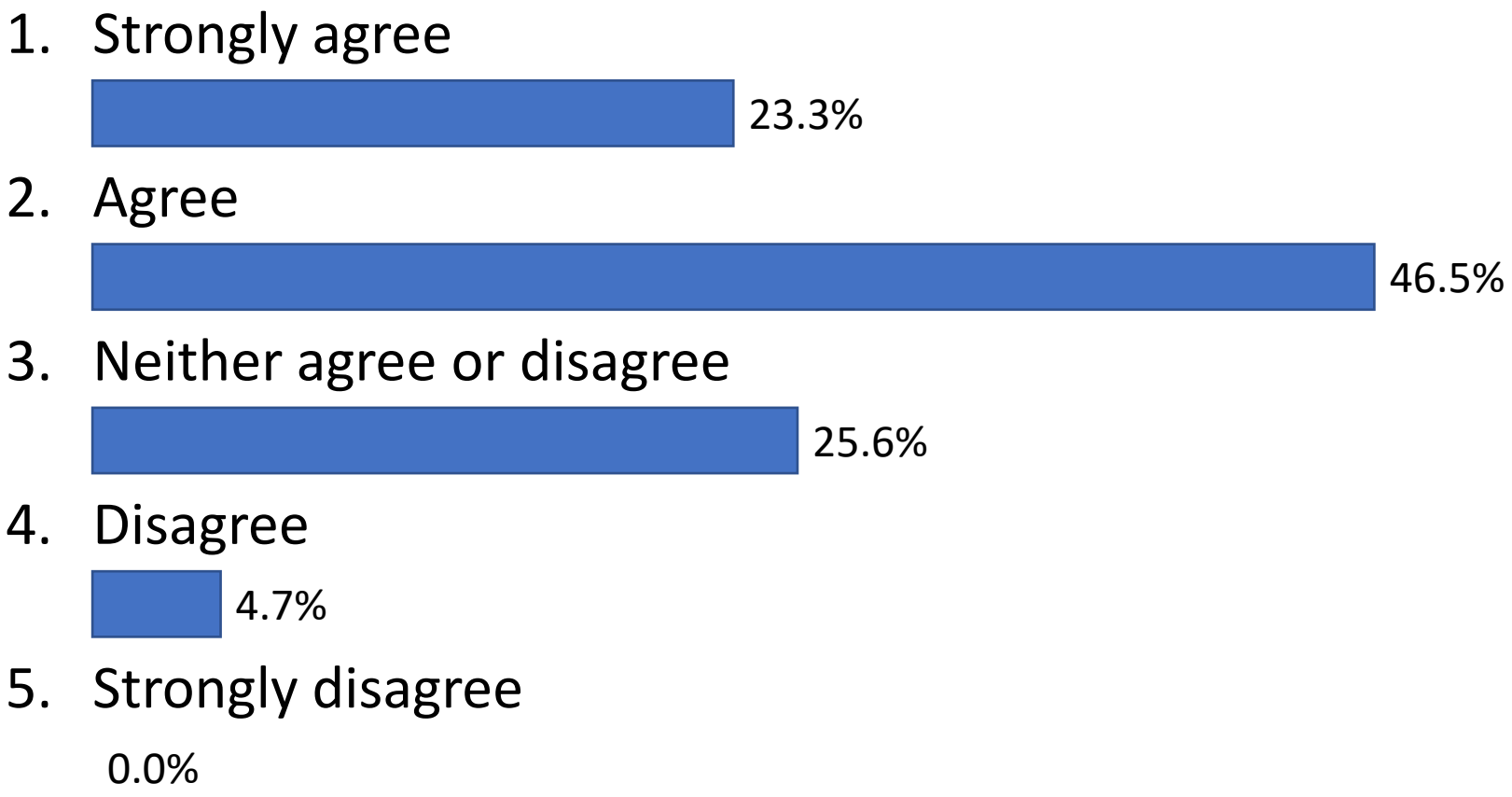
Vote Now

System working makes individual organisation governance and decision making more complex



Vote Now

System working will change the decisions that my organisation will take at board and operational level, and how it will take them



Any questions?

Assurance Framework Benchmarking

Elaine Dower & Jasper Cain

Background

- What have we done?
  - The objectives identified in Assurance Frameworks
  - The Risks identified by organisations
  - Finance and Workforce Risks
  - The design of Assurance Frameworks
- Why are we doing this?

Some highlights from the data

- Providers: 4-32 risks on BAF
- CCGs: 3-36 risks on GBAF
- Providers: Largest number of risks against Patient Care and Safety objectives
- CCGs: Largest number of risks against Commissioning objectives
- Financial Sustainability objective 2nd for both types of organisation.

- Scoring of Risks on AFs: - approximately 50% were ‘Medium’ risks for both Providers and CCGs.
- ‘Governance’ risks now most frequent category for Providers – these are risks identified against all categories of strategic objectives which have failures/poor governance as a ‘cause’ or ‘uncertain event’.
- For CCGs the most frequent category is Quality Assurance of Providers (followed closely by Partnership Working).

- A specific look at the Workforce risks identified that the biggest sub-category was ‘Staffing’ (numbers) for both Providers and CCGs.
- A specific look at the Finance risks identified that the biggest sub-category was ‘Sustainability’ for both Providers and CCGs

Risk Management

- Most clients identify the purpose of the AF as a strategic risk management tool.
- The definition of risk: “effect of uncertainty on objectives” (ISO 31000:2018).

Strategic Objectives

- It is not always clear what success would look like for the Strategic Objectives as written.
- Whilst this is understandable, it can often lead to a lack of clarity in the risk identified.
- Risks not specifically linked to an objective or risk descriptions are not written in a consistent way:

Assurance on Risk Management Processes

- How do you monitor the effectiveness of Risk Management systems and processes?
- A significant number of AFs do not easily facilitate this monitoring as they don't include fields such as:
  - Date risk identified
  - Initial, Current & Target Score
  - Risk appetite or Risk tolerance (and/or link between risk appetite and risk target score)
  - Visual tracking of score over time

Overall Assurance

Only 3/19 Provider BAFs and none of the CCG GBAFs identified an overall assurance level to provide a regular and visual assessment of the level of assurance the relevant Board/Governing Body Committee has taken from the controls and assurances outline and therefore the likelihood of mitigating the risk to target level and still achieving the associated strategic objective.

Use of Resources

John Cotterill
Business Associate
(seconded NHSI UoR assessor)

KLOE Areas

- Clinical Services
- People
- Clinical support services
- Corporate services, procurement, estates and facilities
- Finance

Key Messages

- The extent to which non-executive directors were involved in the NHSI assessment visit varied. Most often the Board Chair attended, at some trusts the Finance Committee Chair and Audit Committee Chair also attended.
- Actions to address UoR findings tend to be incorporated in wider ranging plans (e.g. CQC Action Plan).
- In some cases actions are being monitored and reported to service committees such as Workforce and Quality Committee.

Key Messages

- Trusts noted that UoR assessments are influencing NHSI's approach to supporting non-specialist hospital trusts.
- In some cases UoR reports are being used pro-actively as a further source of assurance and are feeding into Annual Governance Reports and external audit UoR assessments.

Top Tips

- Ensure that you understand the Model Hospital data and are able to give an explanation of the trusts position. Remember comparative high cost in itself is not necessarily a negative story. Consider what benefits there are to patients and stakeholders from the trust investment.
- Don't overlook the obvious. Relatively minor improvements can often have a significant benefit to patients.
- Don't treat the assessment as purely a finance related exercise. Finance is only one of the five KLOE areas, try and give equal weight to all five.
- Remember that the assessment is heavily based on performance over the last 12 months. Do not overly focus on governance issues (strategies/plans/etc). These are mainly covered elsewhere within the SOF.

Top Tips

- Make best use of the commentary.
- Learn from others – engage with local/similar trusts who have had assessments – what worked for them and what did not.
- Involve ‘patient facing’ staff in the assessment process. They are often best placed to relate how service delivery is benefiting patients – personal stories are powerful.
- Involve non-executive directors in the assessment day particularly in the introductory session. Identify a role within the presentation team e.g. give an overview of the area served by the trust and the demographics.

Investigations
Approach and lessons

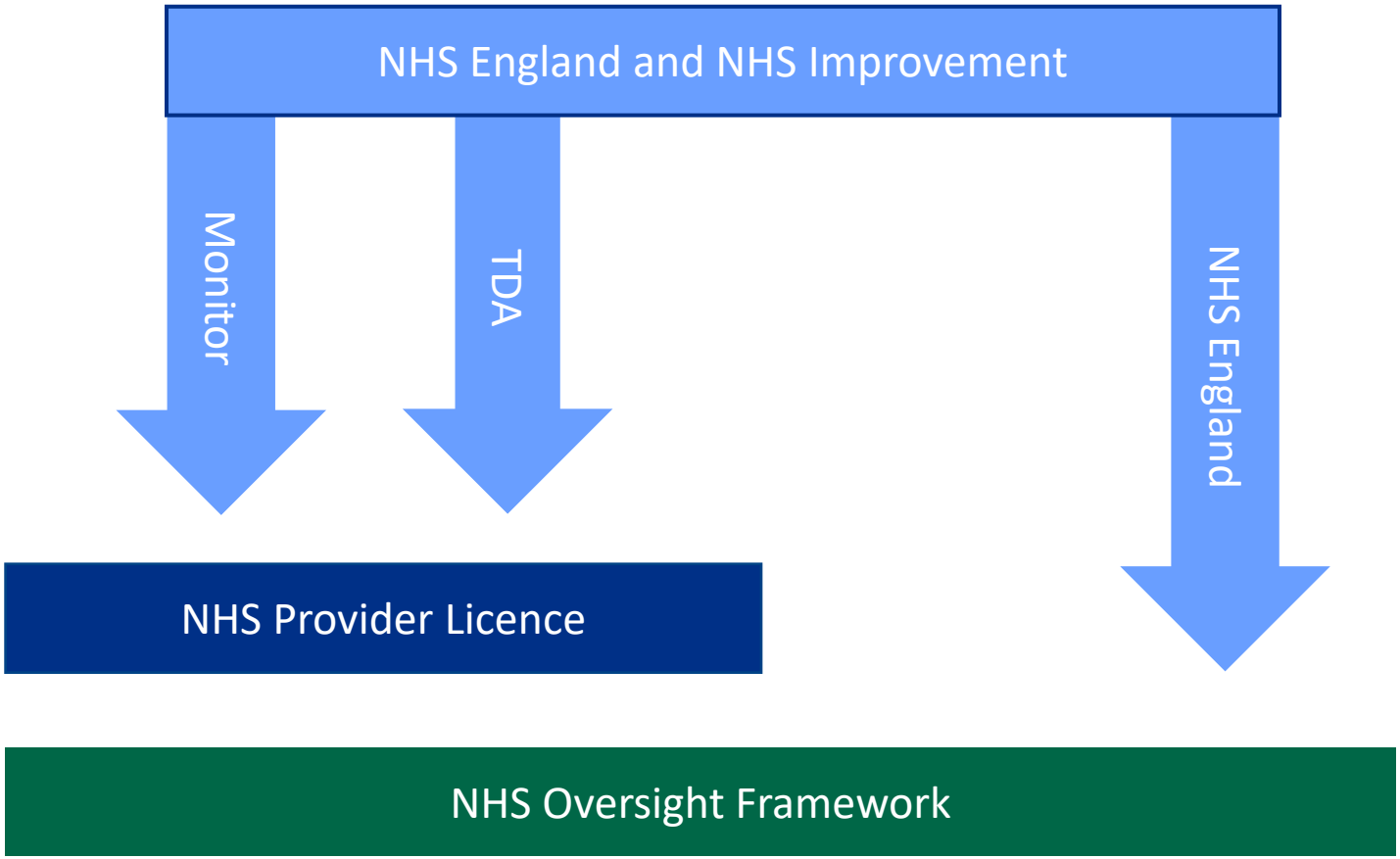
John Lester, Head of Investigations

NHS England and NHS Improvement

Agenda

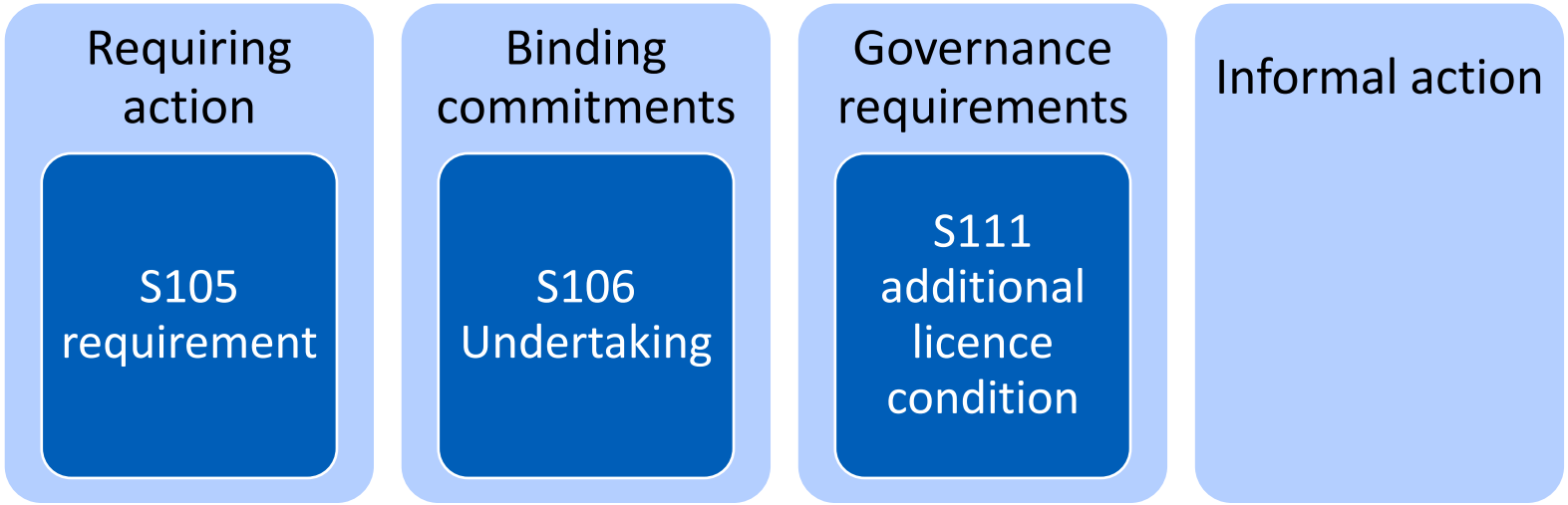
1. The regulatory framework
2. Triggers for an investigation
3. Investigation process
4. Lessons and themes

1. The regulatory framework



Regulatory tools

Foundation trusts



Trusts Informal actions / Statutory powers of direction

CCGs Support regime / Statutory powers of direction

2. Triggers

Finances

- Variance from plan
- Sudden deterioration
- Financial governance concerns

Operational performance

Longstanding failure to meet standards

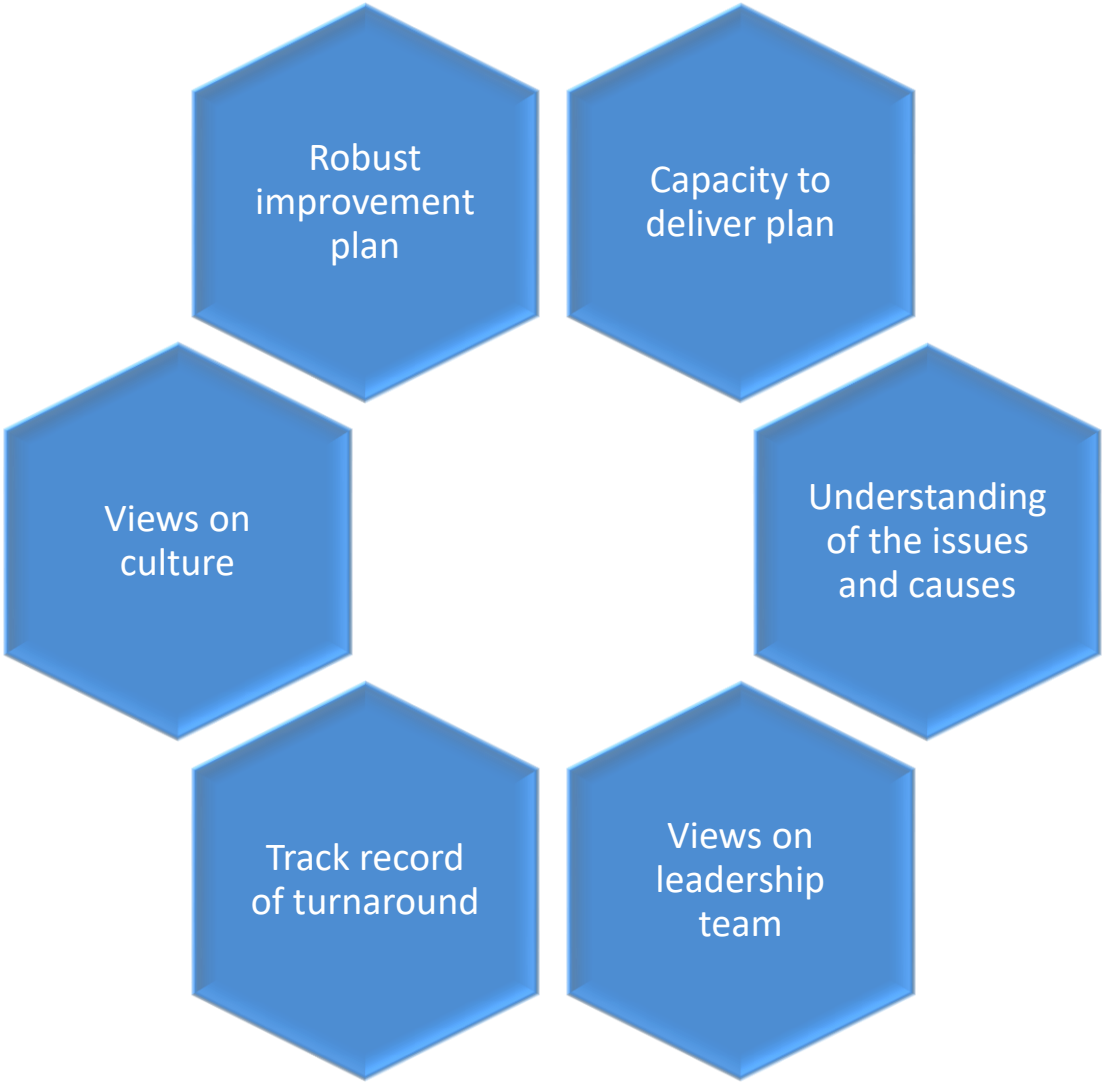
Sudden deterioration in performance

Quality

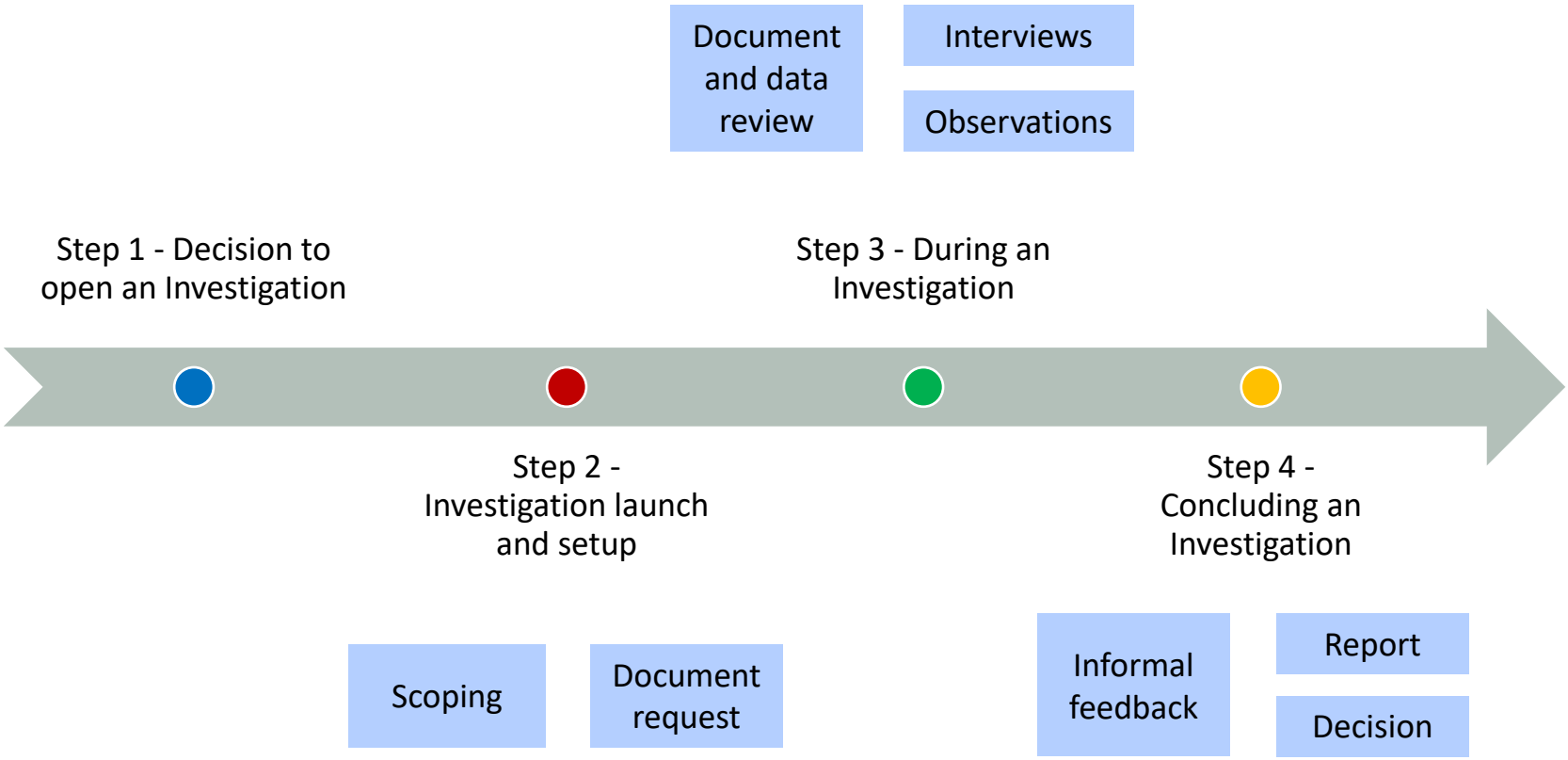
Lack of pace in implementing CQC requirements

Strategic change / leadership and improvement

Factors influencing the decision



3. Investigation process



A diagnostic approach

Interviews

What are we looking for?

- Understanding of drivers of performance issues
- Articulation of how issues are being addressed
- Insight into culture
- Understanding of governance
- Articulation of organisation vision, values, strategy
- Key risks and their mitigations
- Candour and insight

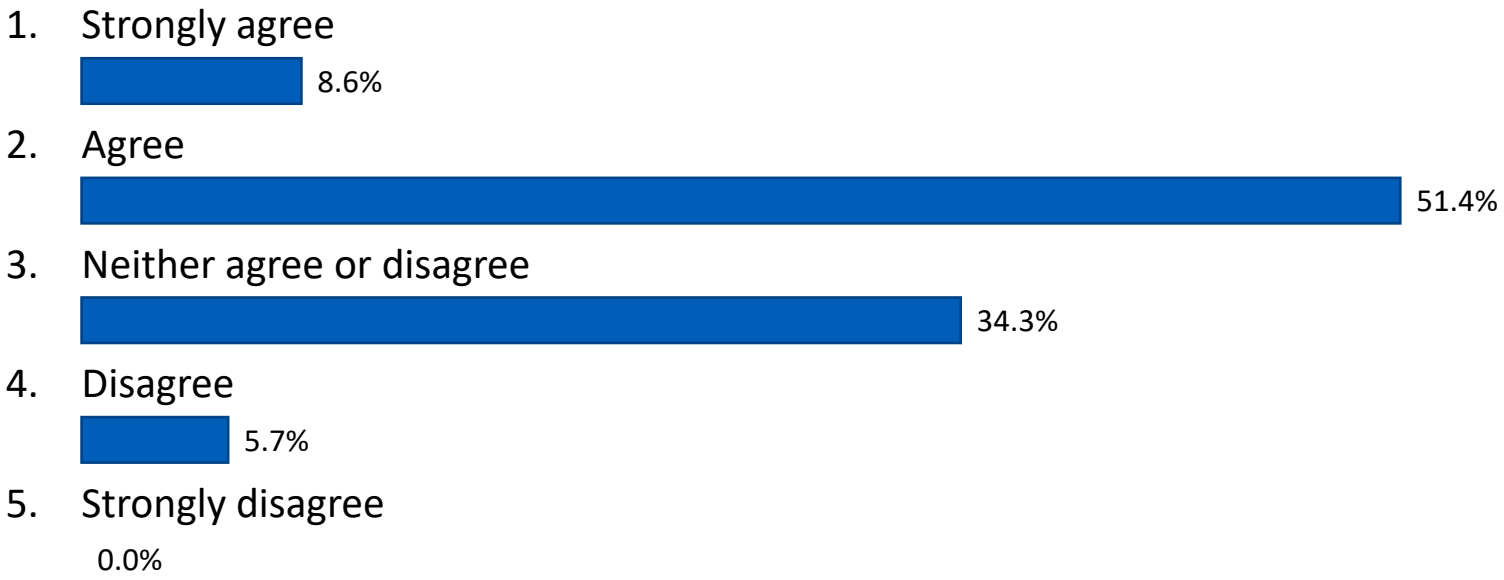
Vote Now

4. Lessons and themes

Governance

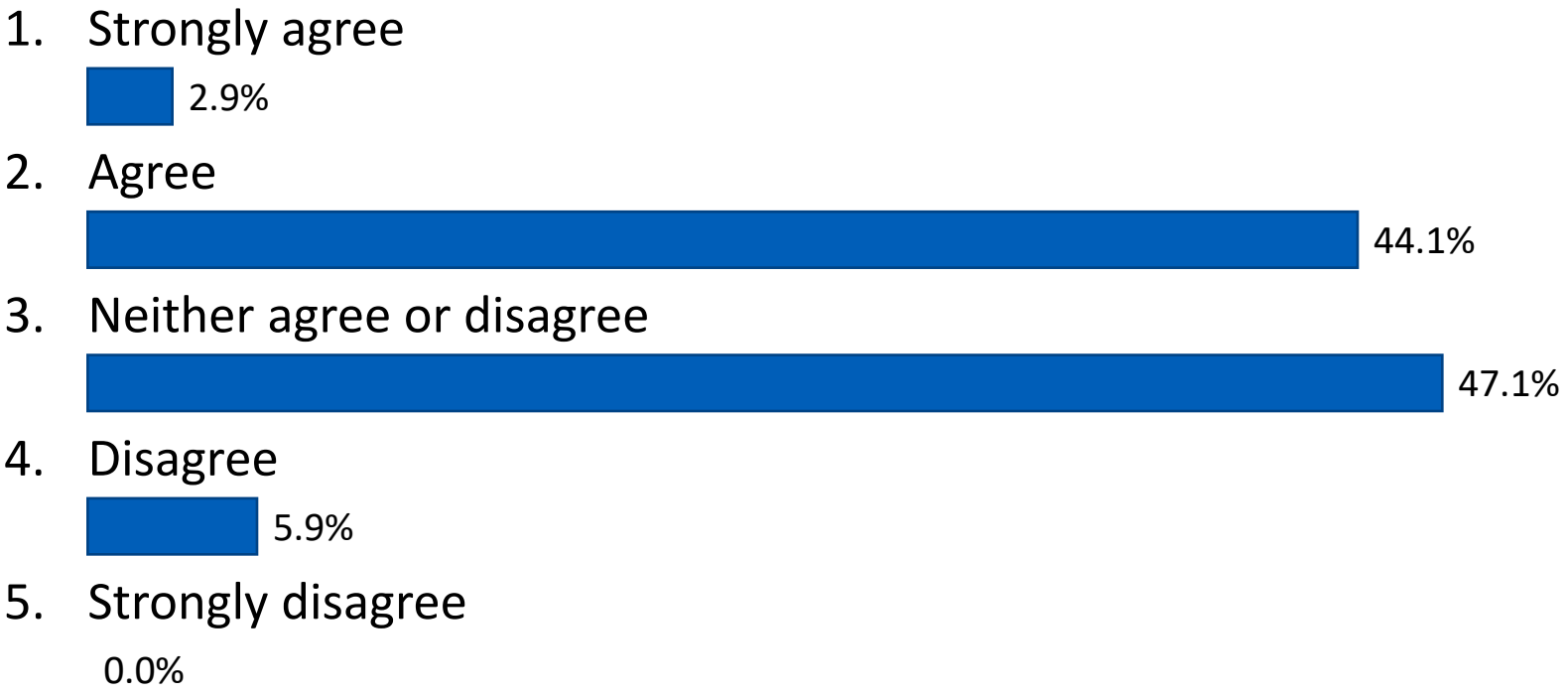
How would you rate committee effectiveness in your organisation?

The committee spends the right amount of time on each of its areas of business



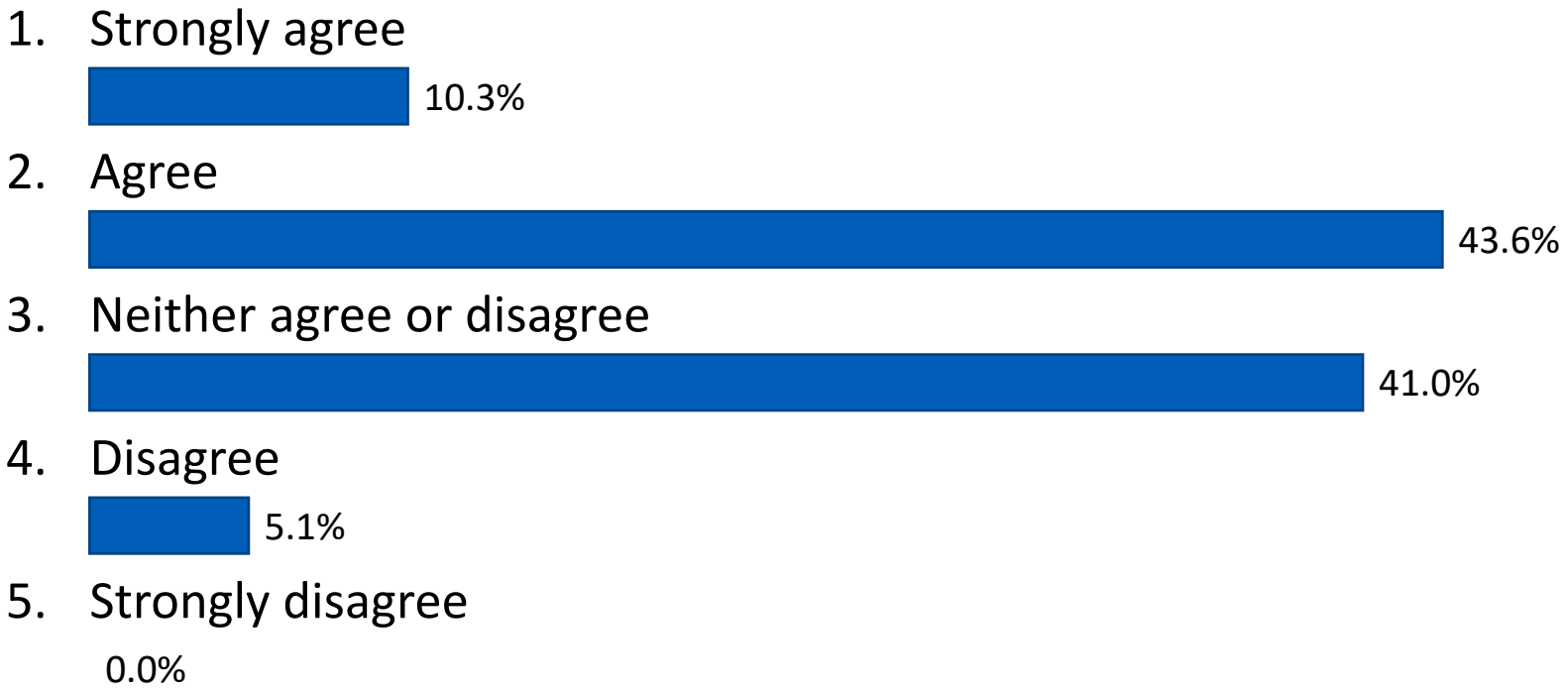
Vote Now

The committee does a good job in relation to risk management



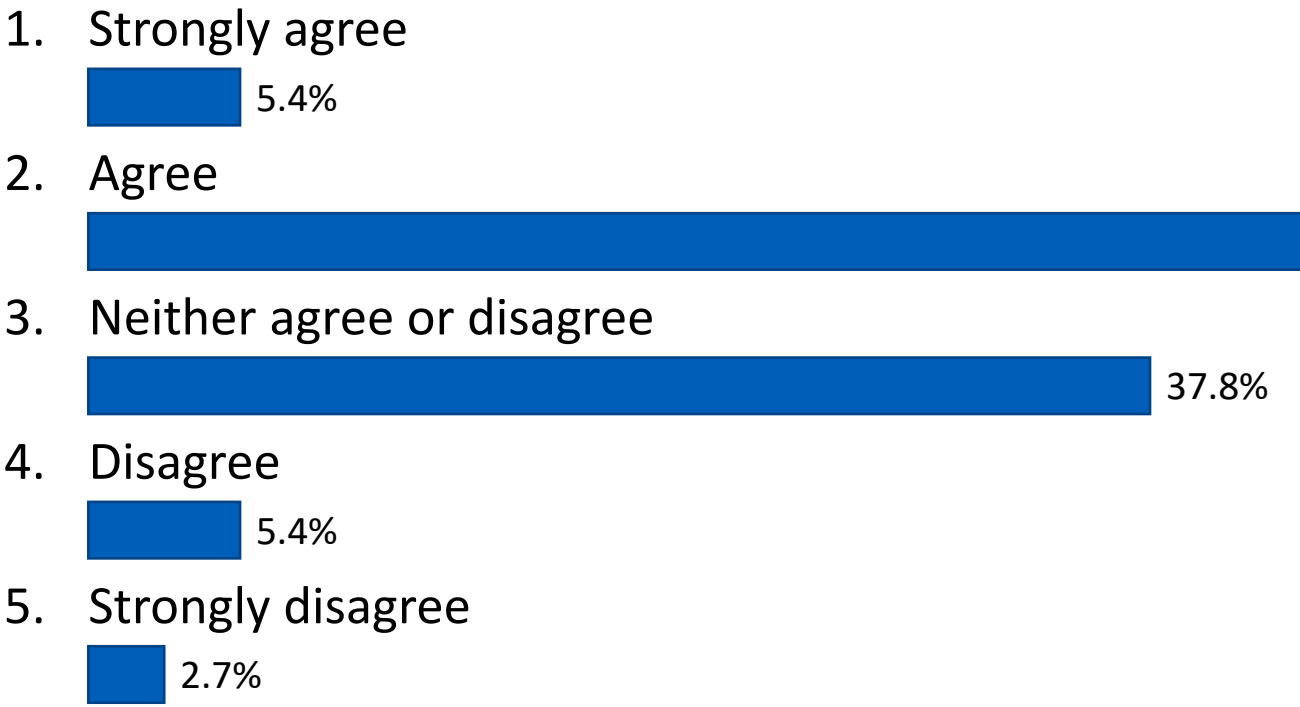
Vote Now

The quality of discussion and challenge is high



Vote Now

The committee has access to high quality information



You may want to consider…

- Quantity
- Clarity
- Timeliness
- Relevance
- Reliability

Governance

Agenda

- Linking to risk
- Strategic versus operational

Risk management

- Board Assurance Framework

Challenge and discussion

- Exec/NED relationships
- Identifying vs dealing with low assurance

Governance

Quality of information

- Board vs committee papers
- Detail vs brevity
- Forwards/backwards
- Drivers of financial position
- So what?

Cultural challenges

- Autonomy vs central control
- Reluctance to performance manage / challenge
- Sense of accountability
- Planning over action
- Engagement in finances

Sudden financial deterioration

Trust A	
16/17 plan:	£6m surplus
Forecast at M6:	(£27m) deficit

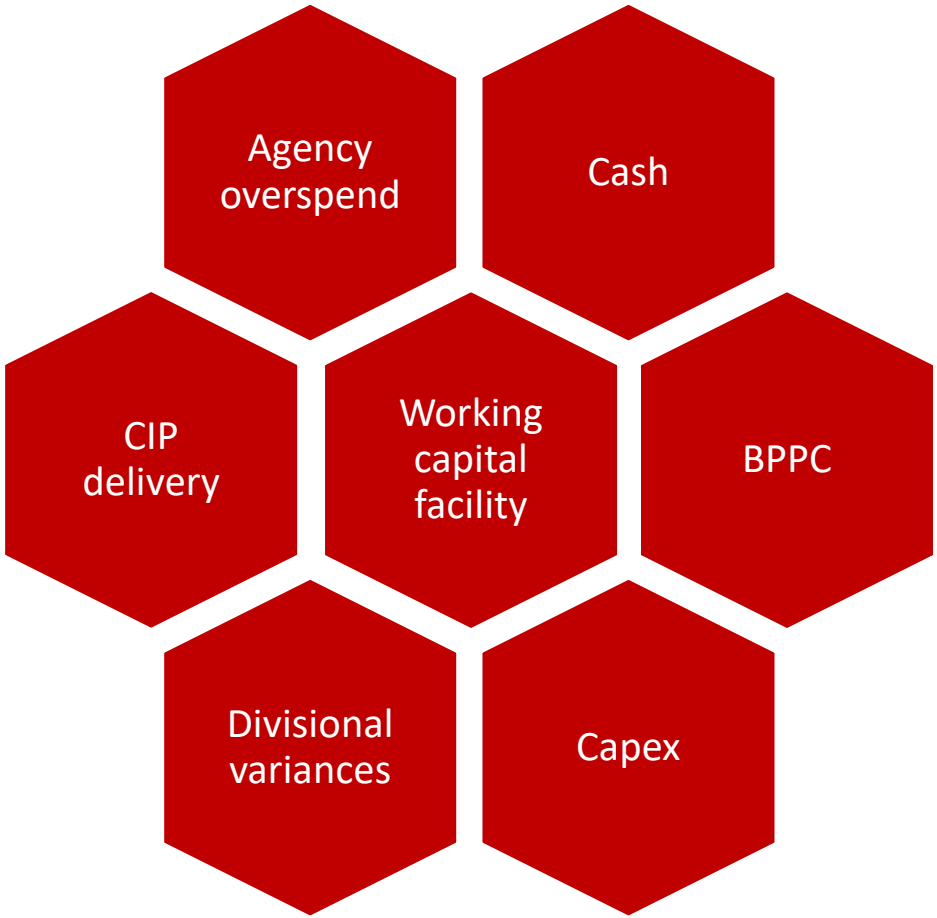
Trust B

M6 17/18: On track against £1m CT

M7: Reforecast to (£54m) deficit

Emergency loan finance

What were the red flags?



Board culture

- NED challenge curtailed by CEO
- Management of information shared with NEDs
- Executive to executive challenge actively discouraged
- Joint executive responsibility for finances discouraged
- FD had a ‘closed’ style
- Lack of escalation
- Reassurance over assurance
- Board not reflective or open to change

Financial reporting

- Underlying position
- Changes made to reports over time
- Risks and forecasts
- Commentary on performance trends and variances
- Planning information for committees
- Lack of aged debtors/creditors information
- Lack of cash flow reporting

Financial scrutiny

- No triangulation of individual areas of concern
- Cash risks not discussed
- Most execs had no exposure to Finance and Performance or Audit Committees
- Limited ad hoc NED attendance at other committees
- No financially qualified NEDs on F&P Committee
- Over-reliance on audit opinion for financial assurance

Financial scrutiny (cont.)

- Weaknesses in reporting from F&P to Board
- NED requests for information ignored and not followed up
- Ineffective divisional performance meetings
- Little financial scrutiny at ExCo

What changes have the trusts made?

New leadership

Finance report redesign

Cross committee membership

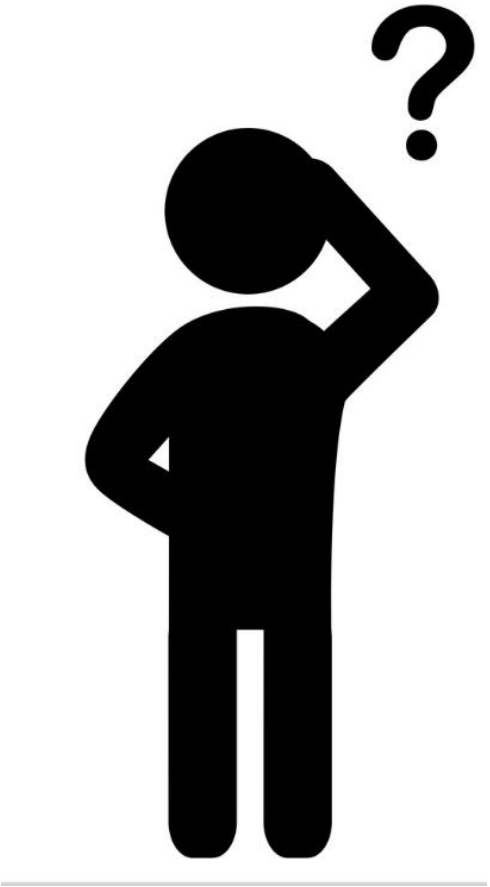
Chair involvement in committees

F&P refocus

Improved divisional meetings

Better comms

Questions



Panel Discussion

Chair: **Bryan Millar,** Audit Committee Chair at Airedale, Wharfedale and Craven CCG, Bradford Districts CCG and Bradford City CCG

Panellists:

Cathy Kennedy, Director of Operational Finance (Yorkshire & Humber) at NHS Improvement and NHS England

John Lester, Head of Investigations at NHS Improvement and NHS England

Paul Barnes, Head of Operations and Engagement - Cyber Security at NHSX

John Mallalieu, Lay Member - Finance and Performance at Calderdale CCG

Chris Thompson, Audit Committee Chair, HDFT

360 ASSURANCE

AUDIT YORKSHIRE
The journey to excellence

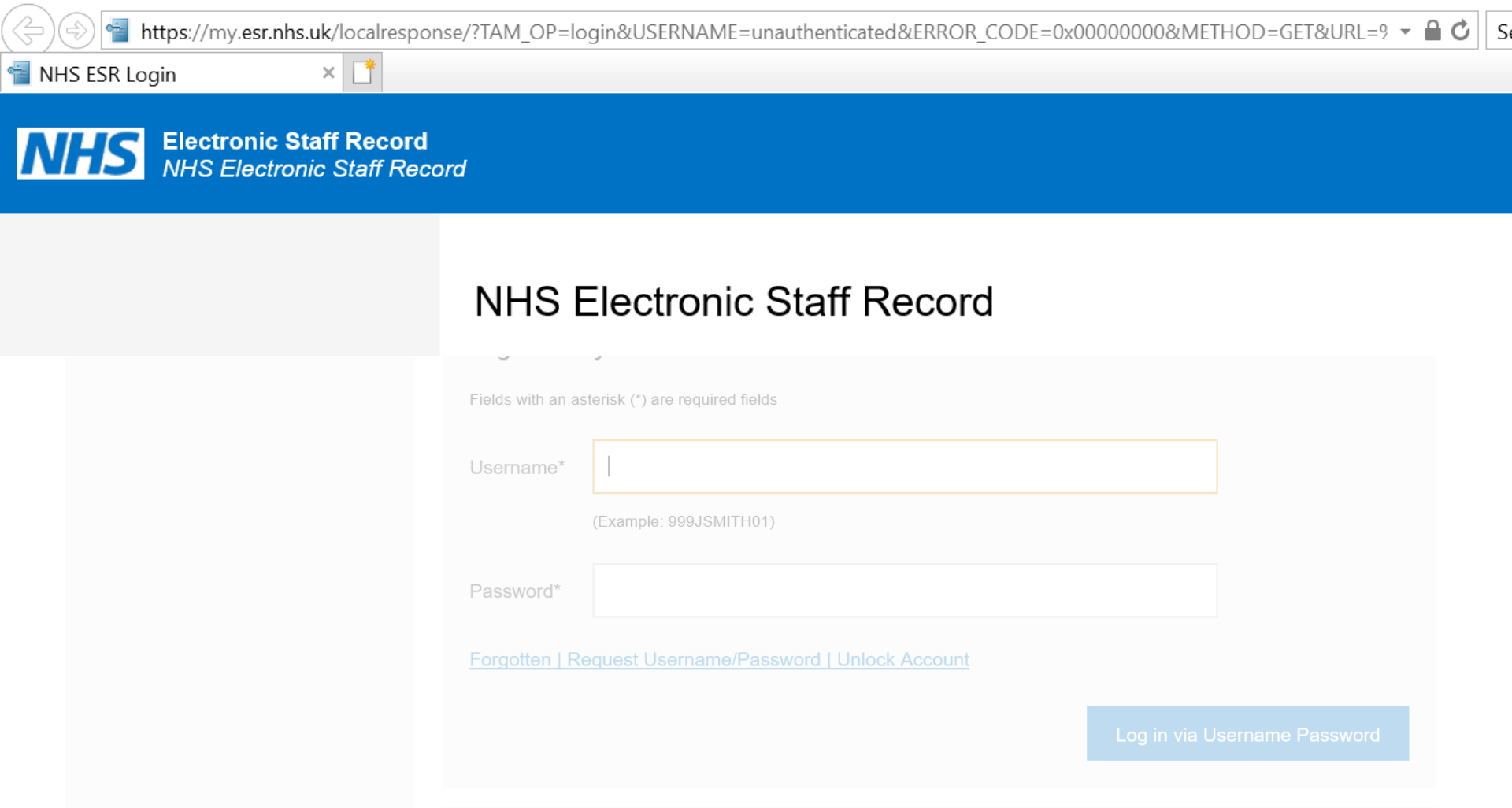
Avoiding the Bait

Andy Mellor

&

Tom Watson

Accessing ESR



Vote Now

Real or Fake?

1. Real

54%

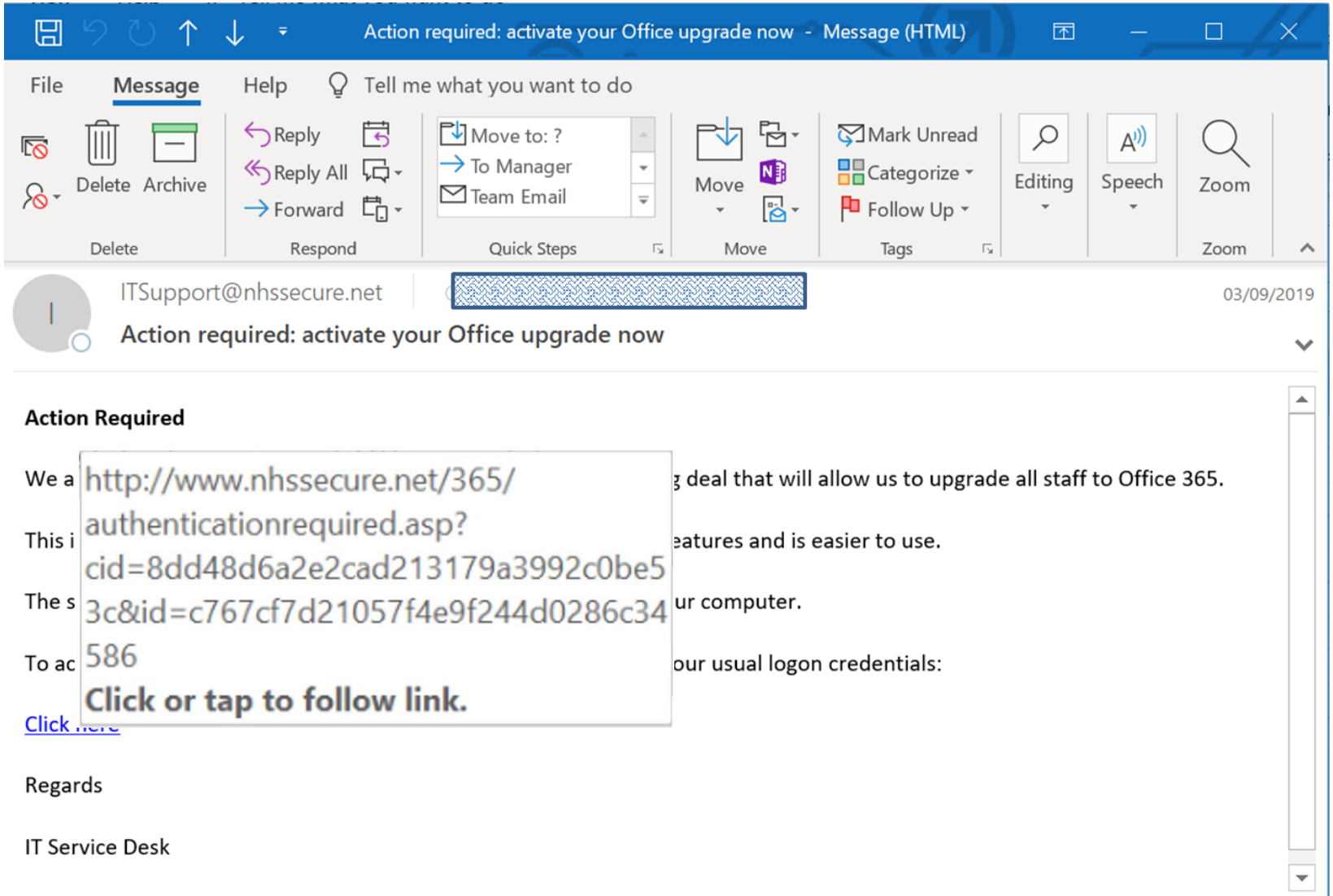
2. Fake

17%

3. Don't know/ can't tell

29%

A mundane email



Vote Now

Real or Fake?

1. Real


14.3%

2. Fake


77.1%

3. Don't know/ can't tell


8.6%

ESR on a mobile device

Vote Now

Real or Fake?

1. Real

11%

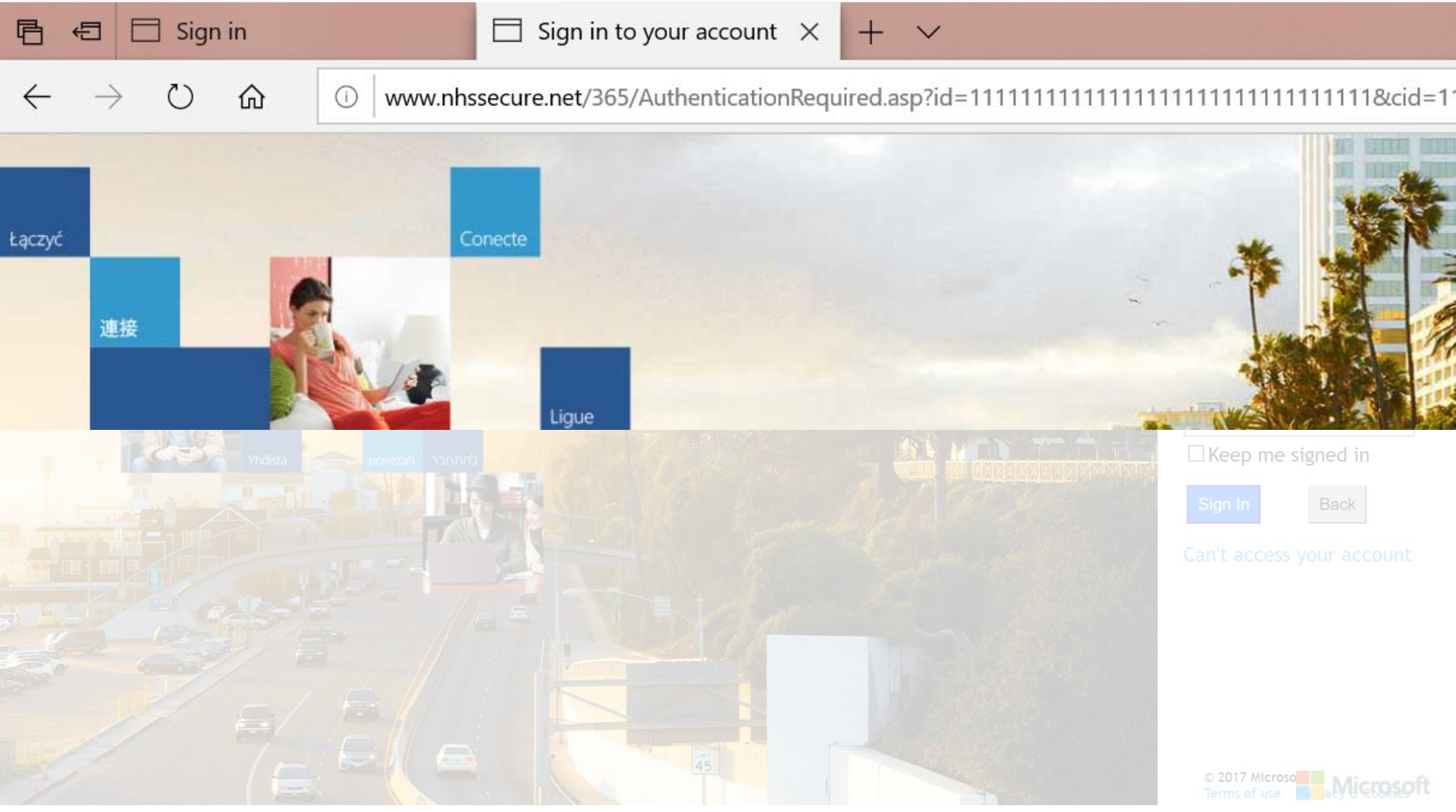
2. Fake

50%

3. Don't know/ can't tell

39%

Activating your office licence



Vote Now

Real or Fake?

1. Real


3%

2. Fake

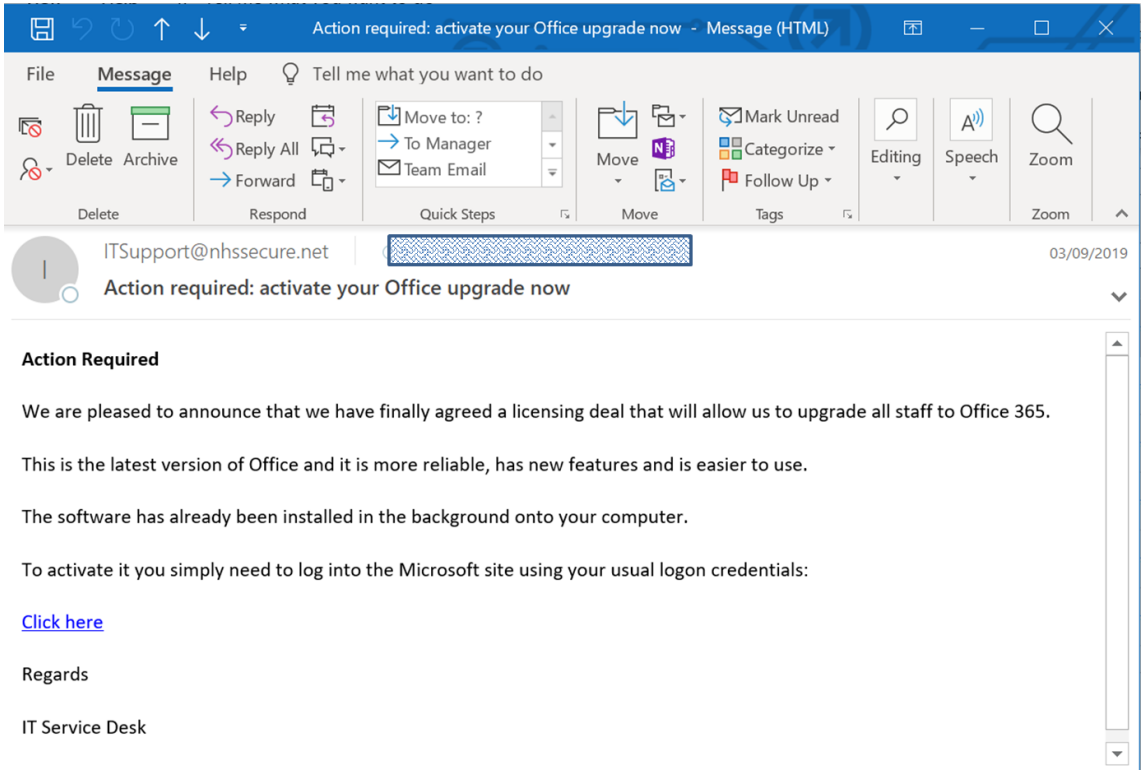

86%

3. Don't know/ can't tell


11%

What were the website clues?

What were the email clues?



- Unexpected?
- Who from…
- … is sender spoofed?
- Who to?
- What are you being asked to do?
- Sense of urgency?

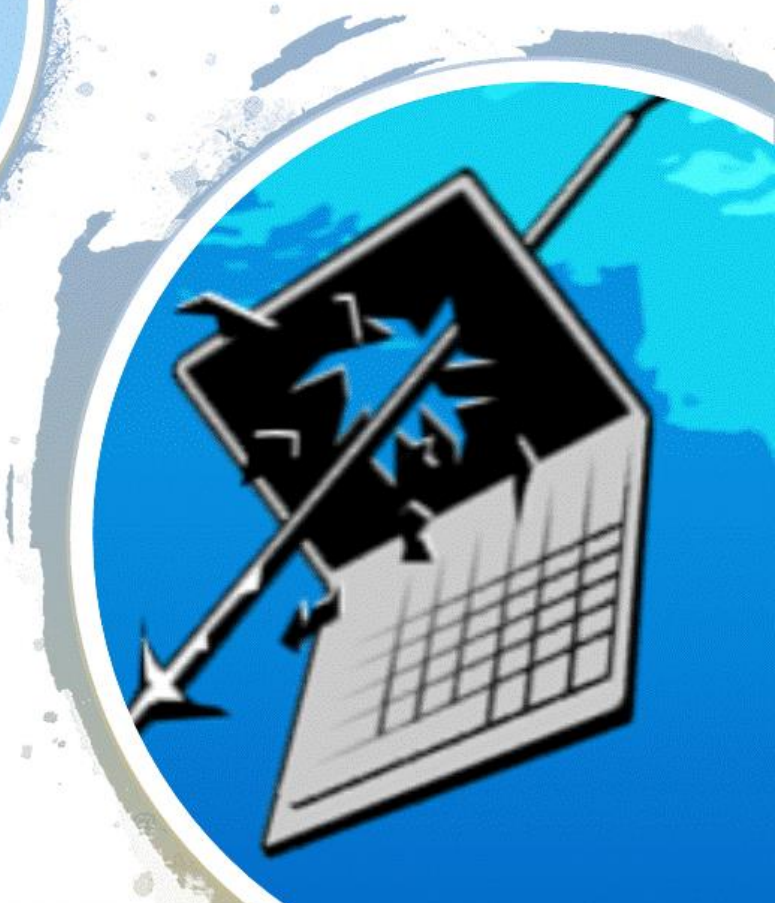
360 ASSURANCE

AUDIT YORKSHIRE
The journey to excellence

www.360assurance.co.uk @360Assurance

www.audityorkshire.nhs.uk @AuditYorkshire

The risk to you?



360 ASSURANCE

AUDIT YORKSHIRE
The journey to excellence

Ignore | Delete | Junk | Mark as Spam | Mark as Not Spam | Add Friend | Reply | Reply All | Forward | Meeting | More | MAC - Member ... | To Manager | Team E-mail | Move | Rules | OneNote | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Zoom

Delete | McAfee Anti-Spam | Respond | Quick Steps | Move | Tags | Editing | Zoom

From Tim Thomas <no-reply@linkedin.com>
To Andy Mellor

Sent Mon 23/09/2019 16:34

You have unread messages from
Tim Thomas

Hi buddy – could you please spare a couple of minutes to complete a survey for me? http://tinyurl.com/37gcEy

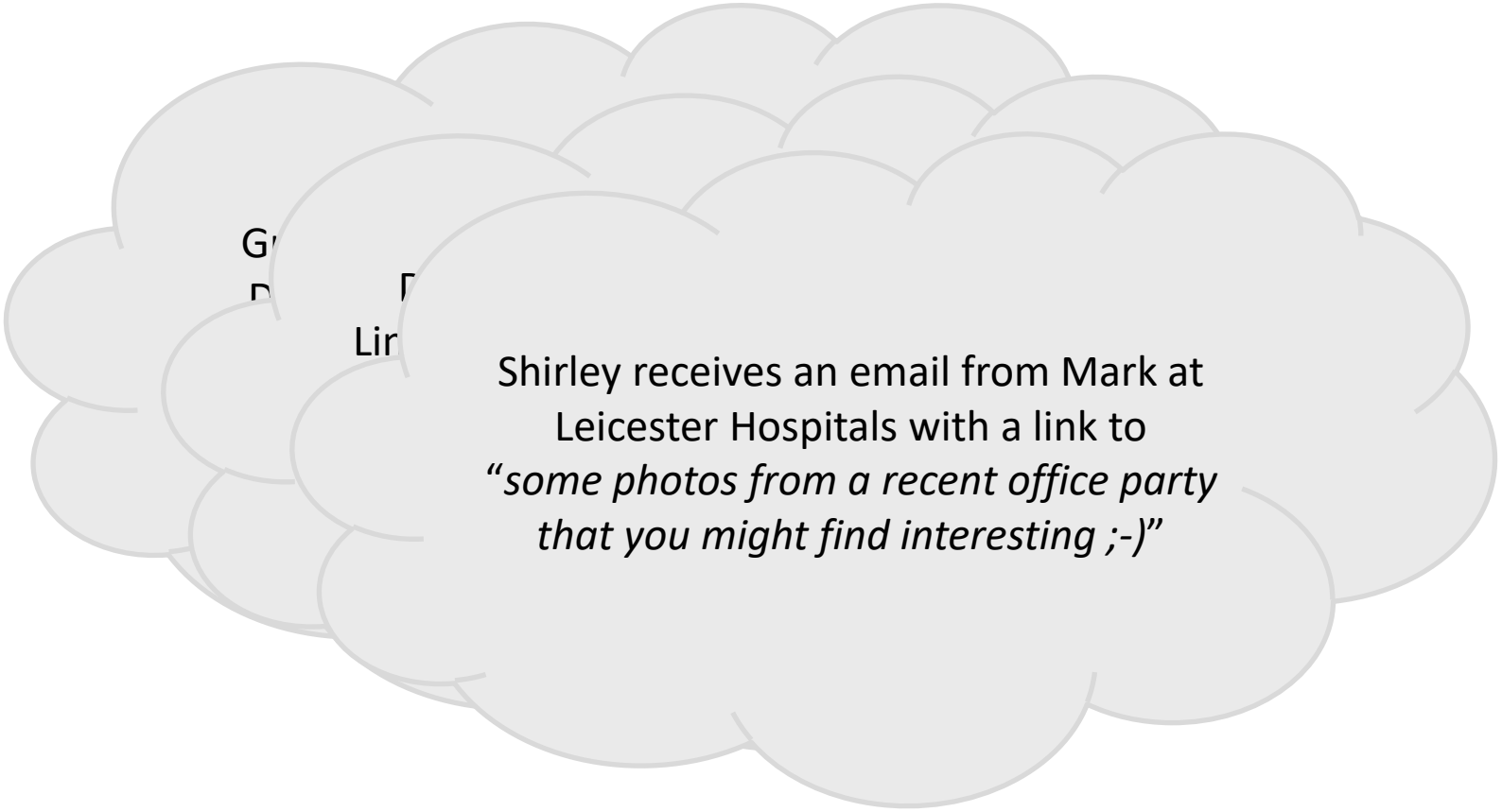
Reply

Opportunity is always within reach. **Get the LinkedIn app.**

iOS . Android

Unsubscribe | Help

What if…

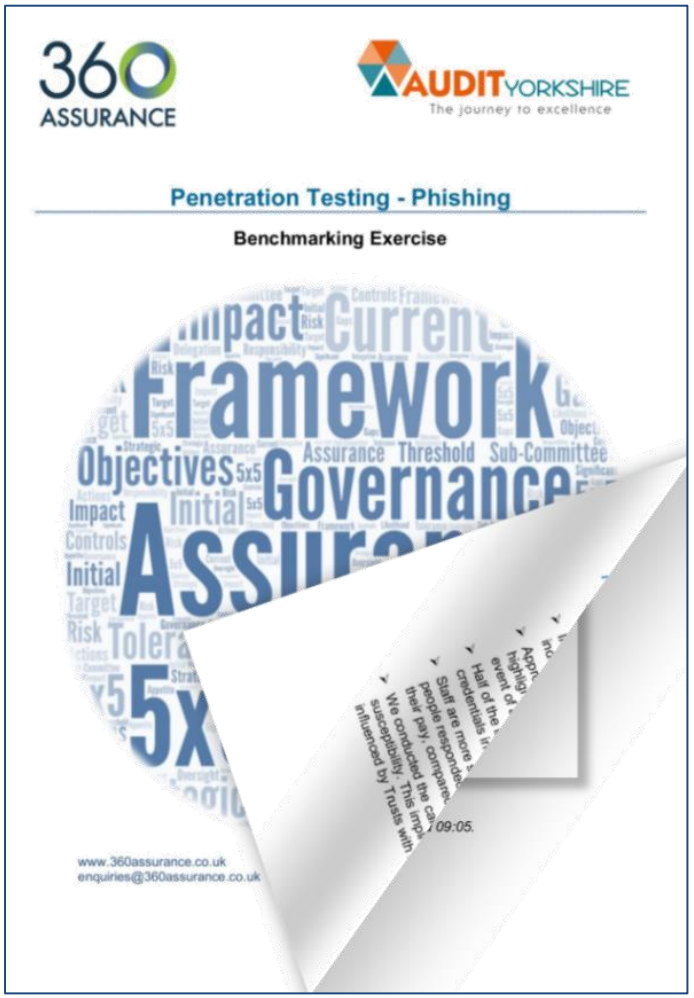

Shirley receives an email from Mark at Leicester Hospitals with a link to
"*some photos from a recent office party that you might find interesting ;-)*"

… and what have we found?

- Users remain susceptible to phishing emails
- Response rates vary from 5% - 15%
- A small number of users are generally susceptible to harvesting their credentials – and it might only take one to compromise a network
- Users respond surprisingly quickly to phishing attacks!

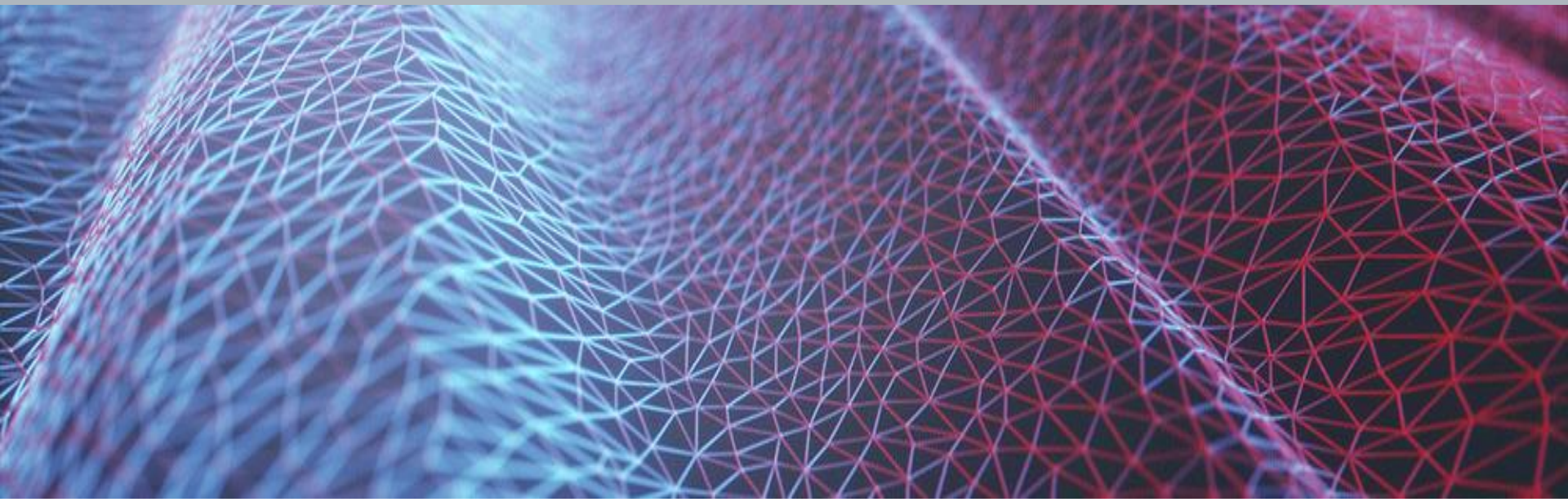
- Mandatory training doesn't eliminate the risk

- Is the NHS culture/ response sufficiently tough, compared to industry?



Cyber Assurance

Managing cyber security at a strategic level



Paul Barnes, Head of Operations & Engagement

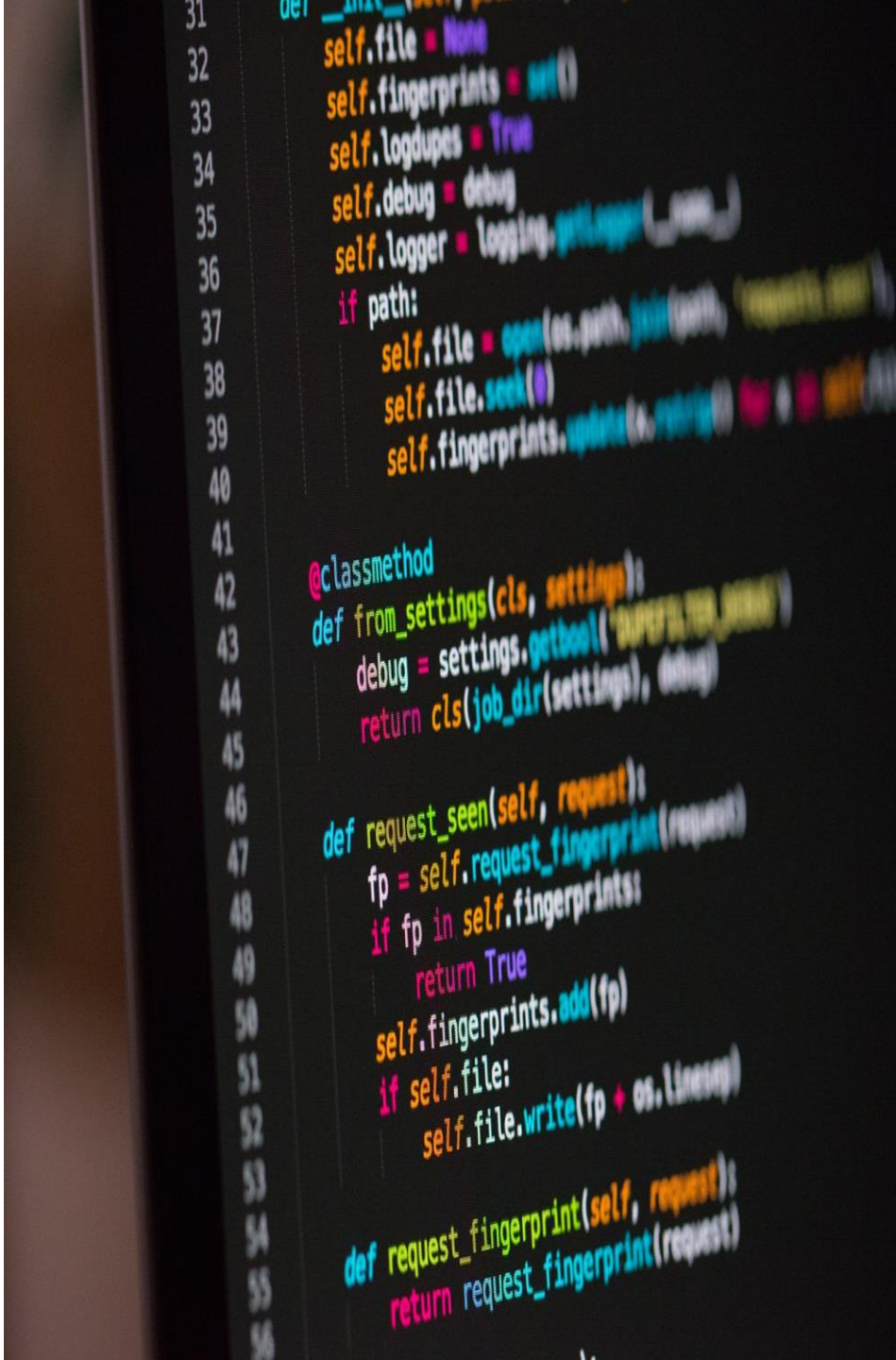
30 September 2019

Session overview

- Threat landscape and cyber risk
- Board framework – 7 key principles
- Regulation
- Support for NHS organisations

NHSX overview

- A new joint team focused on accelerating the digitisation of health and care
- Bringing together expertise and talent from multiple ALBs
- Providing consistent and coherent digital policy
- Leading the development of strategy, programme and project delivery



NHSX Cyber Security Team

What we do:

- Lead a programme to strengthen cyber resilience across health and care to ensure organisations comply with relevant standards
- Raise awareness and understanding of cyber security risks and issues, promote funding opportunities and NHS Digital services
- Provide assurance on requirements for reporting and incident planning

How we do it:

- Work in partnership with NHS Digital and other arms length bodies
- Engage with NHS England and NHS Improvement regional teams – ensuring that organisations are clear about their roles and responsibilities

Why we do it:

- To improve and enhance cyber security and promote awareness of the importance of keeping patient data safe and secure
- To ensure that NHS organisations protect patient data and are able to respond effectively in the event of a data breach
- To build public trust and support safe patient care

Vote Now

How would you rate your knowledge of cyber security?

1. Excellent/detailed understanding

2. Average

3. Some limited knowledge

4. No knowledge of cyber

The threat environment across health and care: March-Sept 2018

50%

More attacks compared to the same period in 2017

3.52m

Intrusion attacks against health and care globally

15.7m

New pieces of malware identified globally

~5.5bn

Potentially malicious emails have been blocked by the NHS alone

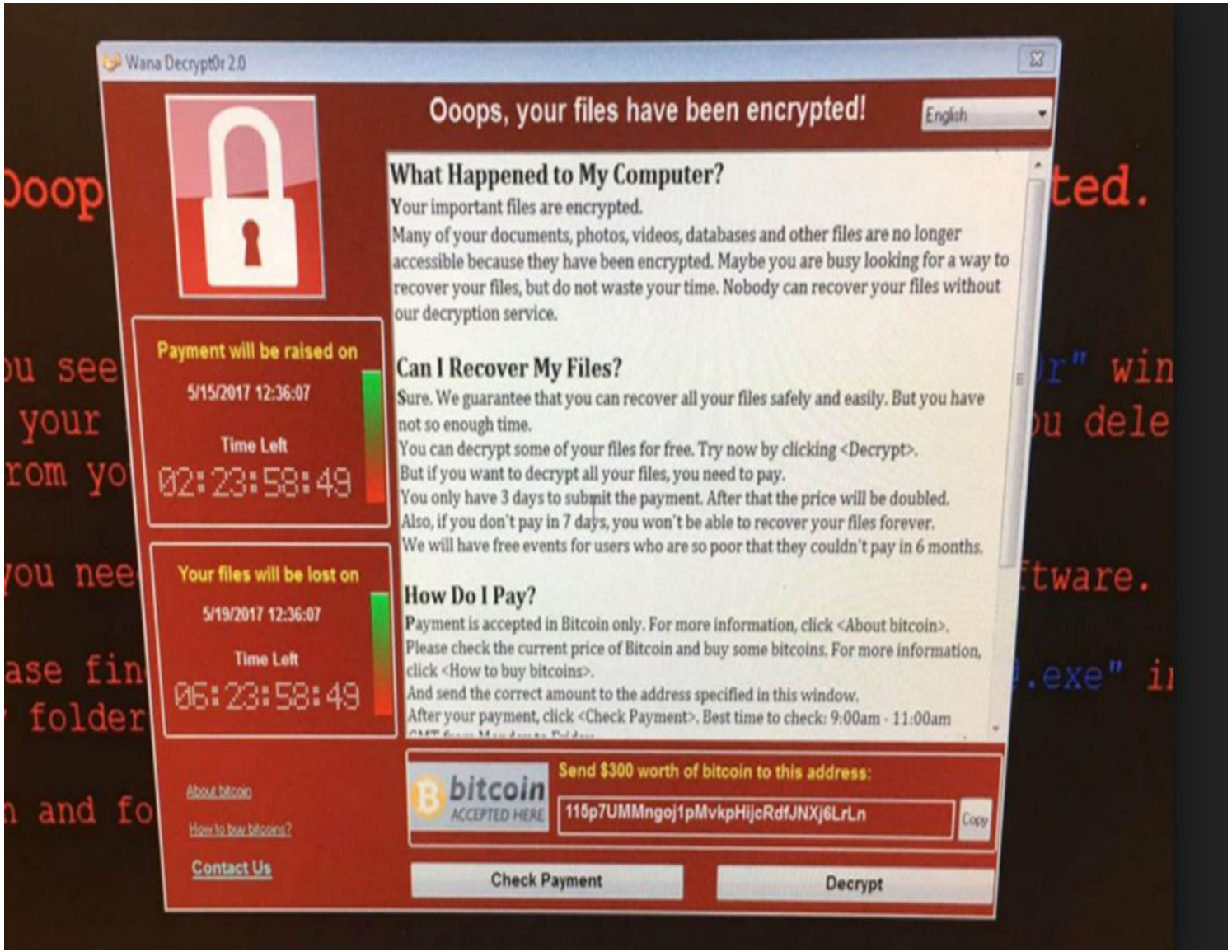
Cyber Security Operations Centre

NHS Digital's Data Security Centre prevent, detect and respond to cyber attacks in real time.

In the last 3 months alone, the centre has **prevented:**

- **Over 21 million potential cyber attacks**
- **640 million phishing attempts**

WannaCry Ransomware Cyber Attack



Impact of WannaCry

80 out of 236 Trusts affected

595 out of 7454 GP practices affected

19,000 patient appointments cancelled

Estimated cost of the breach - **£92 million** in direct costs and lost output

Vote Now

Are you aware of the Network and Information Systems (NIS) regulations and their application to the health sector?

1. Yes

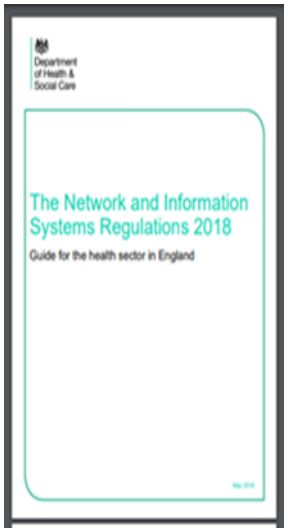
24%

2. No

76%

Regulation

General Data Protection Regulations (GDPR)



Network and Information Systems (NIS) Regulations

Sustainable cyber security: 7 key principles

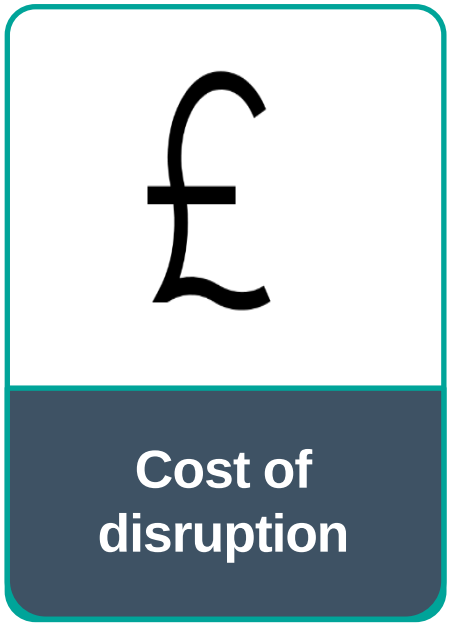
Alignment to NHS Digital Information Security, Risk Management & Code of Practice

- **ISO27001/2:** Specification framework for development and assessment of Information Management systems
- **ISO31000:** Is a Risk management principle-based framework that provides a process for managing risk
- **ISF Good Practice for Information Security:** Business orientated information security controls framework & guidance
- **NCSC Guidance notes:** relevant ad-hoc guidance and advice for UK CNI & Government entities
- **General Data Protection Regulation GDPR Adherence:** relevant provision of safeguarding of personal data
- **Well-Led Framework:** organisation wide framework for managing digital change including security
- **COBIT 5:** Governance orientated globally recognised framework and a focus on maturity models

Sustainable cyber security: 7 key principles

A comprehensive framework will enable a sustainable and proportionate approach to Cyber Security

Quantifying cyber risk



Vote Now

Is cyber security discussed at your Board meetings?

1. Yes, it is on the Board agenda as a standalone topic

2. Yes, it is on the Board agenda alongside other business risks

3. No

4. Not sure

Well-led framework

1 Is there the **leadership capacity** and **capability** to deliver high quality, sustainable care?	2 Is there a clear vision and credible **strategy** to deliver high quality, sustainable care to people, and robust plans to deliver?	3 Is there a **culture** of high quality, sustainable care?
4 Are there clear responsibilities, **roles** and systems of accountability to support good governance and management?	**ARE SERVICES WELL LED?**	5 Are there clear and effective processes for managing **risks**, issues and **performance**?
6 Is appropriate and accurate **information** being effectively processed, challenged and acted on?	7 Are the **people**, who use services, the public, **staff** and **external partners engaged** and involved to support high quality sustainable services?	8 Are there robust systems and processes for **learning**, continuous **improvement** and **innovation**?

Well-led aligned to the cyber framework

1 Enable leadership to have **transparency** of progress in cyber security, areas of risk, and areas of **high performance**.	2 The **strategy** must be informed by the metrics provided through audit.	3 Creating a **culture** of **improvement** and **knowledge sharing** across CCG and STPs to share cyber lessons learnt.
4 Identifying **roles** and **responsibilities** and providing information relevant to specific stakeholders.	**ARE SERVICES WELL LED?**	5 Common Cyber Security **reporting metrics** across the NHS.
6 **Evidence based metrics** support accurate information that can be acted on.	7 Audit can act as the **communication mechanism** between local IT departments, local leadership, and the wider NHS ecosystem.	8 **Auditing** performance with **evidence based metrics** enables improvement and identification of **improvement** areas.

Seven Key Principles	Question	Links to 'Well-Led' Framework
Leadership, Governance, & Culture	Who on the board is accountable for Cyber Security? Do we have an endorsed Cyber Security Strategy?	[4] Are there clear responsibilities, roles and systems of accountability to support good governance and management?
Improving Clinical Quality and Efficiency	Number of Critical Security Incidents in the Past 90 Days that have impacted clinical care? Have we considered the security implications that support us in meeting our clinical priorities?	[3] Is there a culture of high quality, sustainable care?
Enabling Service Integration	Have we identified the risks across connecting organisations, and the mitigating actions needed to manage those risks? How many third party technology providers have access to our networks and/or systems through an integration? Have third party suppliers been through an endorsed security maturity review as part of the procurement on-boarding process?	[4] Are there clear responsibilities, roles and systems of accountability to support good governance and management? [7] Are the people, who use services, the public, staff and external partners engaged and involved to support high quality sustainable services?
Understand Key Threats	Is external threat intelligence being used to inform the security risks? How many systems are currently being actively monitored for vulnerabilities and threats?	[6] Is appropriate and accurate information being effectively processed, challenged and acted on? [8] Are there robust systems and processes for learning, continuous improvement and innovation?
Assuring Processes & Controls	How many Personally Identifiable Information (PII) records do we hold? What evidence can we provide that controls are in place to manage and secure those records?	[5] Are there clear and effective processes for managing risks, issues and performance?
Business Continuity - Effective Cyber Response	Do third party supplier contracts include clauses for Incident Response? Do we have a Cyber Security Incident Response plan?	[1] Is there the leadership capacity and capability to deliver high quality, sustainable care? [2] Is there a clear vision and credible strategy to deliver high quality, sustainable care to people, and robust plans to deliver? [4] Are there clear responsibilities, roles and systems of accountability to support good governance and management?
Proportionate Investment	Is there sufficient investment in Cyber Security projects to meet our service transformation?	[1] Is there the leadership capacity and capability to deliver high quality, sustainable care? [2] Is there a clear vision and credible strategy to deliver high quality, sustainable care to people, and robust plans to deliver?

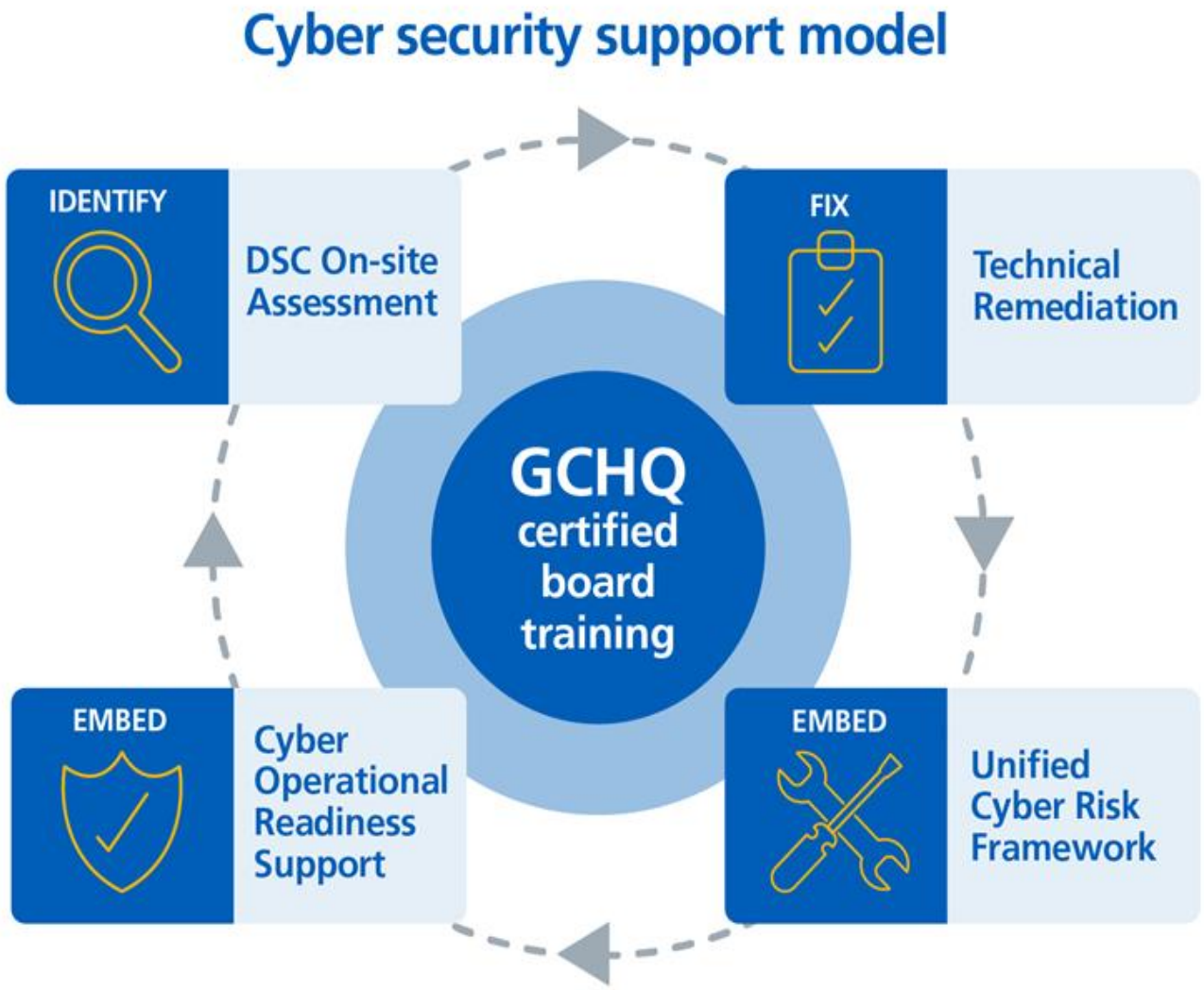
Seven Key Principles	Question	Follow-up questions (e,g, Audit or Risk Committee)
Leadership, Governance, & Culture	Who on the board is accountability for Cyber Security? Do we have an endorsed Cyber Security Strategy?	Are there security projects embedded as part the key service transformation initiatives?
Improving Clinical Quality and Efficiency	Number of Critical Security Incidents in the Past 90 Days that have impacted clinical care? Have we considered the security implications that support us in meeting our clinical priorities?	What are the resolutions that have been put in place to prevent these Critical Security Incidents from happening again?
Enabling Service Integration	Have we identified the risks across connecting organisations, and the mitigating actions needed to manage those risks? How many third party technology providers have access to our networks and/or systems through an integration? Have third party suppliers been through an endorsed security maturity review as part of the procurement on-boarding process?	Has risk tree analysis been done with and across partner organisations? Do we know who our suppliers are? Do we know what systems are most critical so that the realistic level of threat can be evaluated? Are Cyber Security requirements being included in new contracts
Understand Key Threats	Is external threat intelligence being used to inform the security risks? How many systems are currently being actively monitored for vulnerabilities and threats?	Do we act on CareCERT Alerts? Do we have processes and the ability to act and report on High alerts with 48 hours? Where no accountability exists is this explicit? What are our main threats? What training have staff received? Have unsupported systems been removed? How do we know if our plans are proportionate and if threats are real? What is the management risk appetite? Is Cyber Security included in our risk management process?
Assuring Processes & Controls	How many Personally Identifiable Information (PII) records do we hold? What evidence can we provide that controls are in place to manage and secure those records?	Do we know in which systems this data is being held and where? What is our status with the IG Toolkit / DSPT? Do we understand the monetary value of the data being held? Do we understand the clinical value of the data being held?
Business Continuity - Effective Cyber Response	Do third party supplier contracts include clauses for Incident Response? Do we have a Cyber Security Incident Response plan?	In the event of an incident who is responsible/accountable and for what? Where no accountability exists is this explicit? Procurement strategy – have we reviewed out strategy and existing contracts for Cyber Security risk?
Proportionate Investment	Is there sufficient investment in Cyber Security projects to meet our service transformation?	What is our spend on cyber Security as a percentage of our overall budget and is this an appropriate percentage? How does this benchmark against other similar NHS Organisations and across other industry areas?

Assurance questions – start with the basics

- Is there an accountable lead within the organisation for cyber risk?
- Has the Board undertaken cyber awareness training?
- Does the Board have assurance that cyber risk is built into wider business continuity planning?
- Have business continuity plans been tested?

Support package

Support from NHS Digital



Additional support from NHS Digital

- Simulated phishing tool – now available from NHS Digital. To register email: cybersecurity@nhs.net
- Face to face training for Senior Information Risk Owners (SIROs)
- Online learning available for clinicians and Information Asset Owners
- Coming soon – NHS Secure Boundary

Support from NHSX

- Dedicated awareness sessions for your Boards at STP/ICS or organisational level
- Access to subject matter experts
- Cyber Associates Network – to keep you ahead of the game
- Support with incident testing and drills

Additional resources

- NIS Regulations Webinar
- NIS Regulations and the health sector guide
- NAO Guidance for Audit Committees on cyber and information security
- ‘Exercise in a Box’ available from the National Cyber Security Centre
- Board Toolkit available from the National Cyber Security Centre
- National Data Guardian – 10 data security standards

Summary

1) Make use of the centrally funded products and services and other resources from the National Audit Office and National Cyber Security Centre

2) Link cyber risk to operational and strategic risk – integrate into existing governance structures

3) Ongoing training and awareness for Board members – engage them in cyber simulations and drills

Email contact

The programme team would welcome your comments and feedback and can be contacted by email: **england.cyber@nhs.net**

To engage with any of the centrally funded NHS Digital services, please email: **cybersecurity@nhs.net**

NHS
Counter Fraud Authority

Working together to counter fraud in the NHS

Paul Tiffen
Head of Quality & Compliance

The NHS Counter Fraud Authority (NHSCFA) is a special health authority tasked to lead the fight against fraud, bribery and corruption targeting the NHS.

Who we are

- **Our mission** is to lead the fight against fraud affecting the NHS and wider health service, and protect vital resources intended for patient care.
- **Our vision** is for an NHS which can protect its valuable resources from fraud.

What we do

- An intelligence-led organisation
- We investigate high-level, complex NHS fraud and work closely with local counter fraud specialists

What we do

- We develop targeted fraud prevention solutions
- We set standards for NHS counter fraud work
- We raise awareness of NHS fraud and encourage people to join us in fighting it
- We use technology and data analysis to support ongoing investigations, inform the intelligence picture and guide fraud prevention steps

Nature and scale of the problem

Estimated annual loss to the NHS from fraud:
£1.27 billion

That figure may change as our intelligence picture is developed and sharpened.

NHS staff frauds (payroll) - £94.6m

General Practice- £88m

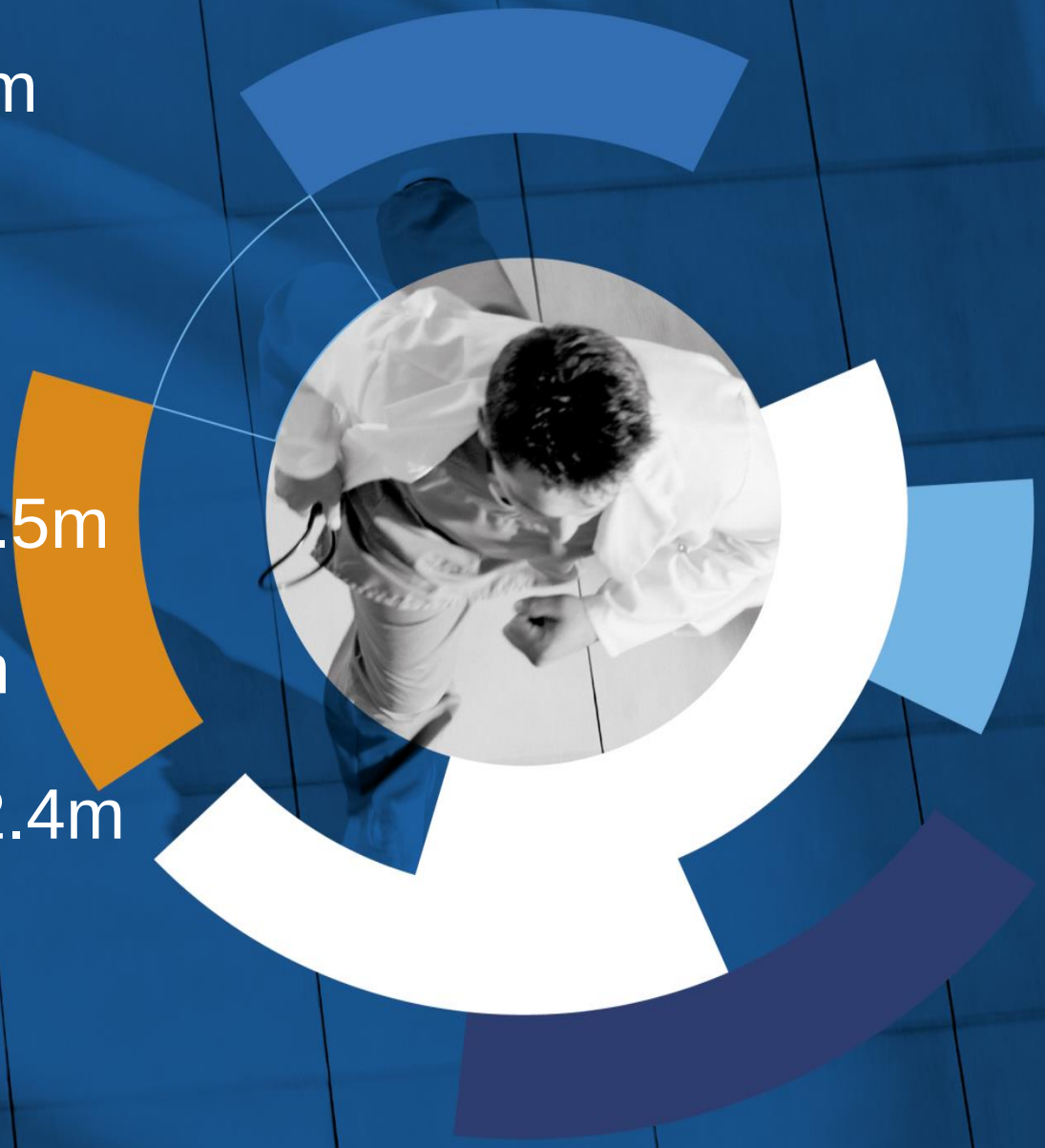
Procurement- £351m

EHIC- £21.7m

Dental contractor- £93.5m

Patient fraud- £251.7m

Optical contractor- £82.4m



Working in partnership

While it is the NHSCFA's responsibility to lead the fight against fraud in the NHS we cannot do this on our own.

Everyone has a part to play in fighting fraud.

You also have a key role in fighting fraud.

Key counter fraud roles in the NHS

- Local Counter Fraud Specialist
- Director of Finance/ Chief Financial Officer
- Audit Committee and its Chair

Increasing NHSCFA influence and counter fraud compliance across the NHS

Greater and more effective engagement of NHS audit and risk committees

Greater exchange of data and information to counter fraud across the NHS

Exploring the development of a framework contract for counter fraud services

What can you do?

1. **Be risk based**
   Take a risk based approach to fraud that is linked to NHSCFA's standards

2. **Be responsible**
   Have a director of finance fully engaged with the counter fraud agenda, with a clearly defined responsibility for managing the process, who discharges it effectively

3. **Be engaged**
   Have a fully engaged audit committee, who provide demonstrable support, direction and (crucially) monitor the service and hold it to account if it doesn't deliver

4. **Be realistic**
   Adopt a realistic approach to the resources and work required to counter fraud

5. **Be assured**
   Obtain assurance they have in post a competent LCFS with the relevant and up to date skills to carry out the operational work on its behalf

Procurement fraud case study

- Former locksmith employed by Guys and St Thomas' NHS FT found guilty of fraud by abuse of position.
- Defrauded the NHS of almost £600,000.
- Abused his position to commission his own company to carry out work for Guys and St Thomas' Hospital charging extortionate mark-ups of up to 1,200%.
- Led lavish lifestyle from the proceeds of his crime.

Our priorities for 2019-20

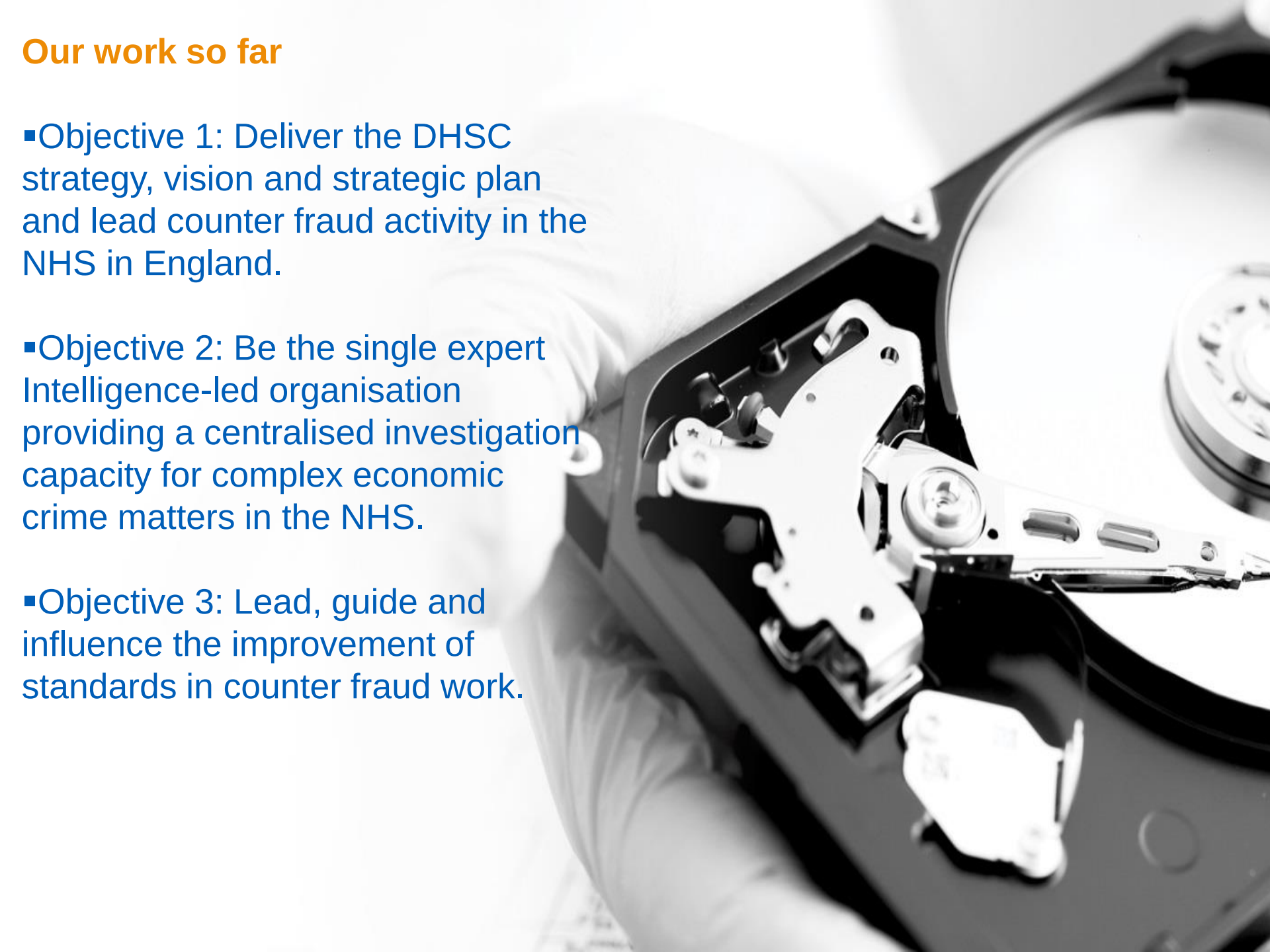
- Fraud in relation to Community Pharmaceutical Contractors
- Procurement and commissioning fraud
- Fraud in relation to General Practice contractors
- Improving fraud outcomes in the NHS

Our work so far

- Objective 1: Deliver the DHSC strategy, vision and strategic plan and lead counter fraud activity in the NHS in England.

- Objective 2: Be the single expert Intelligence-led organisation providing a centralised investigation capacity for complex economic crime matters in the NHS.

- Objective 3: Lead, guide and influence the improvement of standards in counter fraud work.



Our work so far

- Objective 4: Take the lead and encourage fraud reporting across the NHS and wider health group.

- Objective 5: Invest in and develop NHSCFA staff.

A new counter fraud role in the NHS

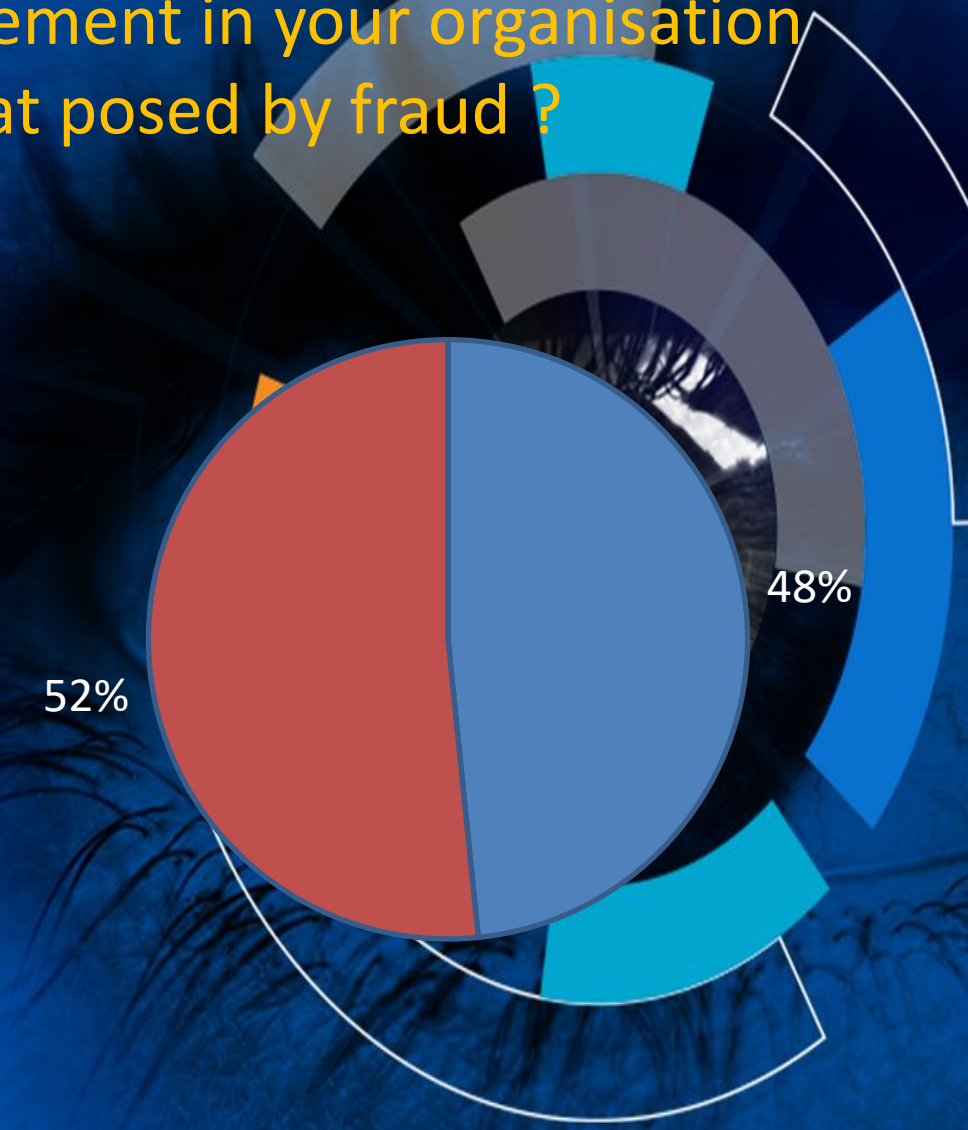
- Counter Fraud Champion
- Gateway e-learning package
- Questions

George Squire
e learning Developer

Vote Now

In your opinion to what extent does the typical member of senior management in your organisation consider the threat posed by fraud ?

- They are proactive, they are well aware of possible fraud threats and this informs their day to day work.
- They are reactive, they consider fraud threats if an when concerns are brought to their attention.



What is a Fraud Champion ?

- Promotes awareness of fraud, bribery and corruption
- Understands the threat posed from fraud, bribery and corruption
- Understands best practice on countering fraud
- Understands cross-government fraud initiatives and engages their organisation and any associated organisation in those initiatives.

The Fraud Champion e learning package

- Nominated Counter Fraud Champions
- Accessed through NHSCFA Learning Management System
- Gives information and guidance
- What we want Fraud Champions to know and why

Vote Now

In your opinion to what extent is the typical member of senior management in your organisation aware of fraud initiatives ?

1 They are well aware of fraud initiatives both within the NHS and the wider public sector.

13.3%

2 They are well aware of fraud initiatives within the NHS.

66.7%

3 They are rarely aware of fraud initiatives.

20.0%

The Fraud Champion e learning package

Describes:

- what Fraud is,
- the fraud landscape,
- relevant internal stakeholders,
- guiding principles
- fraud prevention

Summary

- NHSCFA leading the fight against NHS fraud
- Everyone has a part to play – especially you as Audit Committee Chairs
- Tell us what you need – we want to help
- A new counter fraud role Fraud Champions

FINAL QUESTIONS & CLOSE