



Insight - Board Assurance Framework

Veran Patel , Director - Healthcare
veran.patel@tiaa.co.uk

September 2025

The NHS continues to navigate a period of transformation—nationally, regionally, and within individual organisations. As strategic priorities evolve and operational pressures intensify, boards are increasingly challenged to maintain clarity of focus while anticipating and managing emerging risks. In this context, we conducted a review of 15 Board Assurance Framework (BAF) reports across Integrated Care Boards (ICBs), Providers, and Community Trusts. Our analysis covered 147 risks and aimed to identify common themes and examples of practice for you to consider. There is no “right” or “wrong” BAF, as each is developed to meet the specific requirements and risk management arrangements of the organisation it serves. Whether you are refining your own BAF or considering how to adapt to the shifting healthcare landscape, we hope this analysis contributes to help guide your next steps.

Veran Patel, Director of Health & Social Care



Key observations across all BAFs

Cyber Risk Visibility - Not all BAFs explicitly referenced cyber risks—This is worth considering given the growing national threat and the rise of AI-enhanced cyber-attacks. It is acknowledged that an organisation may be satisfied that the risk can be managed operationally. A notable example of practice includes the rollout of National Cyber Security Centre (NCSC) training—highlighting a proactive approach to cyber resilience.

Risks

- Risk Score Tracking - One BAF tracked risk scores over the past three months and flagged risks that had remained on the register for over a year, supporting longitudinal oversight.
- Risk Trajectory Mapping – One BAF included risk trajectory forecasts. For instance, a target score of 9 in 12 months may seem to be contradicted by a projected score of 12—offering valuable foresight for board discussions.
- Enhanced Risk Narratives Some BAFs provided detailed rationales for risk scores, identify emergent risks, and outline “Future Opportunities.” It is best practice to include horizon scanning for strategic risks.
- Emergent Risk Example: “Ongoing uncertainty regarding funding re-allocation to support the NHS 10-Year Health Plan.”
- Future Opportunity Example: “Growth opportunities from outside the ICB as a trusted provider.”

Risk Appetite - Where defined, reputational risk appetite varied across all BAFs, including:

- “Seeking” – willing to accept reputational risk with controls.
- “Cautious” – limited acceptance if fallout is controlled.
- Three of the fifteen BAFs did not include risk appetite alongside current and target risk scores—limiting the strategic context for risk evaluation.

Controls – The vast majority of controls listed were manual and there is scope to automate controls much further.

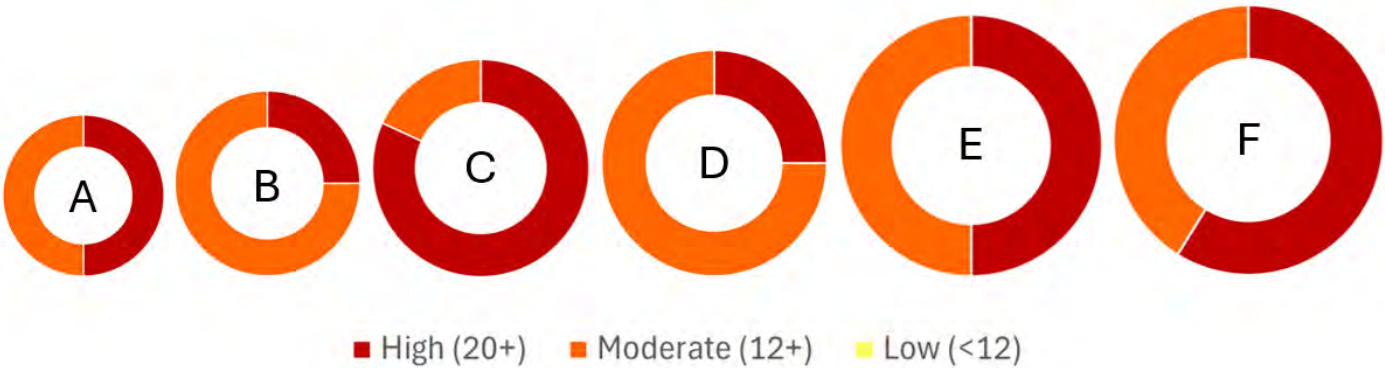
- Two BAFs provide a Controls Assurance rating for each key control, rated as Level 1 (Management), 2 (Oversight) and 3 (Independent) – this reflects the 3 lines of defence model which is a widely accepted framework for managing risk and providing assurance within organisations.

Key Findings from Acute and Mental Health Provider Trusts - specific BAF Review

Number of risks and ratings for Provider Trusts

Note the size of the circles reflects the total number of risks.

Note that there was inconsistency in the scoring across the BAFs so we have taken the following scoring to define the overall score of 15+ High, 8+ Moderate .

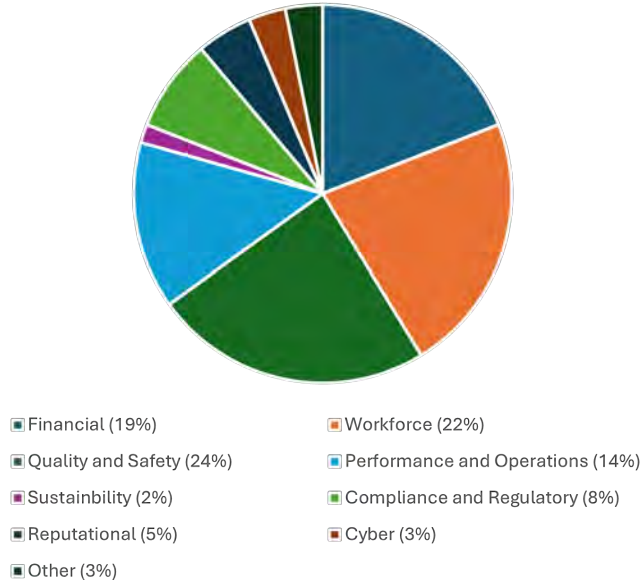


	Consequence				
	1 Negligible	2 Minor	3 Moderate	4 Major	5 Catastrophic
Likelihood					
5 Almost certain	5	10	15	20	25
4 Likely	4	8	12	16	20
3 Possible	3	6	9	12	15
2 Unlikely	2	4	6	8	10
1 Rare	1	2	3	4	5



Risk Category Distribution

Breakdown of Risk Category (Provider)



Key Insight: A clustering of risks around Quality/Safety, Workforce and Financial.

Assurance & Controls

Assurances: All Provider Trust BAFs included both internal and external assurances.

- 1 BAF provides an overall Assurance rating for the strength of Assurances over the controls relating to each of the strategic risks. The Assurance ratings are Substantial, Reasonable, Limited, Not Assured. This BAF also includes a rating on the Adequacy of Controls using Adequate or Inadequate ratings.
- Two BAFs provide a Controls Assurance rating for each key control, rated as Level 1 (Management), 2 (Oversight) and 3 (Independent) – this reflects the 3 lines of defence model which is a widely accepted framework for managing risk and providing assurance within organisations.
- One of the BAFs provides for an “SRO level of assurance” for each principal risk.



Action Plan Progress RAG Rating	
Blue	Completed & embedded and added to controls or assurances
Green	Completed & ongoing and / or not yet fully embedded
Amber	In progress & on track

Control Mechanisms

Control Type	Count	Examples
Manual Controls	61	Manual exception reporting, collation and analysis of surveys, meetings and policies
IT-Enabled Controls	2	Power BI dashboards, Cybersecurity monitoring tools

Strategic Implications for Provider Trusts

- **Risk Saturation:** High volumes of High risks may suggest a need for prioritisation and potential recalibration of risk appetite in order to focus the Board's attention.
- **Control Maturity:** Heavy reliance on manual controls indicates an opportunity to expand digital assurance mechanisms.
- **Assurance Clarity:** Variability in how assurance is presented (positive/negative, gaps) suggests consideration of developmental work across BAFs.



Please refer to the Annex for more detailed information on the reviewed Board Assurance Frameworks



Veran Patel , Director - Healthcare
veran.patel@tiaa.co.uk



Annex

Focus on Quality and Patient Safety across Trust BAFs

To assist the Audit Committee as we have aggregated and summarised the key risks and their drivers as they relate to quality and patient safety. Each BAF will be different as it caters to the unique arrangements of the Trust, however, it may be worth checking these against your own BAF.

Risk Area	Core Risks	Key Drivers
1. Access to Care	- Service closures affecting antenatal/postnatal care - Delays in planned and urgent treatment - Growing waiting lists - Patients accessing inappropriate services	- Estate reduction (e.g. closure of centres) - Demand-capacity mismatch - Fragmented service pathways - Weak clinical leadership and integration
2. Clinical Safety	- Missed high-risk maternal/fetal conditions - Inadequate monitoring and continuity - Avoidable harm events - Poor clinical outcomes	- Disrupted care continuity - Pressure on frontline services - Weak incident learning systems - Gaps in clinical oversight
3. Governance & Assurance	- Weak floor-to-Board oversight - Poor triangulation of data - Regulatory non-compliance - Unclear or duplicative standards	- Underdeveloped reporting frameworks - Fragmented assurance processes - External regulatory complexity - Limited internal governance capacity
4. Health Inequalities	- Poor outcomes for vulnerable groups - Late or missed access to care - Inequity in service provision - Failure to address wider determinants	- Insufficient targeted resources - Lack of system-wide collaboration - Poor adaptability of services - Limited strategic influence
5. Patient Experience	- Anxiety due to disrupted services - Negative care experiences - Lack of lived experience in service design - Loss of public trust	- Disruption in continuity and access - Weak engagement mechanisms - Inadequate co-production with service users - Poor responsiveness to feedback
6. Legal & Regulatory Compliance	- Breaches of MHA/MCA obligations - Unlawful deprivation of liberty - Delays in statutory reviews - Enforcement action and reputational harm	- Failure to meet statutory responsibilities - Process delays and gaps - Limited legal oversight - Competing operational pressures
7. System Partnerships	- Weak collaboration with partners - Failure to transform clinical pathways - Fragmented service delivery - Missed innovation opportunities	- Poor strategic alignment - Limited engagement with ICS/local partners - Lack of shared vision and leadership - Financial and operational constraints
8. Emergency Preparedness	- Insufficient hospital capacity - Delays in emergency response - Lack of resilience planning - Risk to service continuity	

Annex

We have aggregated the key controls and provide examples in relation to quality and patient safety.

Control Type	Summary of Controls	Examples
Governance & Oversight	Structures and committees providing strategic and operational oversight of quality, safety, and performance.	Quality & Safety Committee, Finance & Performance Committee, Board oversight, Quality Sprint Team
Strategic Planning & Programmes	Long-term initiatives and strategic pillars aimed at improving care, reducing demand, and aligning priorities.	Trust Strategy, Target Operating Model, Healthy Local People pillar, Capacity to Care Programme, Waiting List Improvement Programme
Quality Assurance & Reporting	Mechanisms to monitor, triangulate, and report on quality indicators, incidents, and outcomes.	Integrated Quality and Performance Report, Medical E-Governance Dashboards, Annual Complaints Report, Learning from Deaths Report, Clinical Harm Reviews, Patient Safety Incident Response Framework Reports
Patient Safety Systems	Frameworks and tools to manage safety culture, incident response, and mortality reviews.	PSIRF implementation, Datix, NHS SPINE, Mortality Scrutiny Panel, Safety Alerts, Early Warning Trigger Tool
Workforce & Clinical Practice	Controls ensuring safe staffing, clinical competence, and adherence to best practice.	Roster Check & Challenge, Supervision, Appraisals, Mandatory Training, Clinical Guidelines, Patient Safety Training
Legal & Regulatory Compliance	Structures and processes to ensure adherence to MHA, MCA, DoLS and statutory obligations.	Mental Health Legislation Group, Mental Health Legislation Committee, Mental Health Law Team, Section 117 Reviews, CQC MHA Reviewer responses, Legal Process Audits
Service User Engagement	Mechanisms to hear from and respond to patients, carers, and families to improve experience and co-production.	Patient stories at Board, Friends & Family Test, People Participation Team, Family Liaison Officers, Listening into Action
Performance & Access Monitoring	Systems to track access, waiting times, and operational metrics across services and localities.	Service User Tracking List (SUTL), Daily bed reviews, Weekly waiting times meetings, Demand & Capacity Planning, Recovery Plans

Annex

We have reviewed the assurances and common examples included, which may assist in identifying sources of assurance for your own Trust BAF.

Assurance Line	Definition	Examples from BAFs and other notable practice
First Line: Management Assurance	Operational controls and day-to-day management activities that deliver services and manage risks.	Project management structure for Target Operating Model, Divisional Delivery Oversight Group reports, Incident reporting via Datix, Roster monitoring and shift fill rates, Safe staffing reviews and confirm/challenge panels, Quality Impact Assessments (QIA) in programme proposals, Locality leaders tracking key metrics and escalating risks, Training (mandatory, role-specific, MHA/MCA), Policies in place (e.g. NICE, PSIRF), Clinical audit plans and outcomes, Risk review meetings (Divisional), Patient Safety Oversight Group (PSOG), Operational risk escalation (e.g. DoLS expiry, Section 117), Weekly Safety Group chaired by Chief Nurse.
Second Line: Oversight & Monitoring	Functions that monitor, review, and support management, ensuring controls are effective and risks are managed.	Quality Committee oversight of IQPR and incidents, Tier 4 quality governance subgroups, Triangulation of Learning and Continuous Quality Improvement Forum, Performance Delivery and Oversight Group, MEG audit reviews, Statutory training compliance monitoring, Learning from Deaths Action Plan Management Group, Internal Learning from Deaths Forum, Mortality Scrutiny Panel, Suicide Prevention Strategy, IPC Board Assurance Framework, ICB representatives attending governance forums, Quality metrics stress-tested with performance data, Mock CQC visits and service visit framework, Executive and non-executive director visits, Patient and carer stories at Board and Committee, Friends & Family Test results monitored, DNA rates monitored by clinicians.
Third Line: Independent Assurance	External or independent evaluations that provide objective assurance to the Board.	CQC inspections and engagement meetings, CQC MHA Reviewer visits, Human Tissue Authority, UK Accreditation Service, Joint Advisory Group on Gastrointestinal Endoscopy, MHRA accreditations, Royal College of Psychiatrists Quality Network accreditation, Internal audit on CQC compliance readiness, National patient surveys (e.g. Community Mental Health Survey), Friends & Family Test (FFT), Advocacy service, NHS England development programmes (e.g. Patient Safety Specialists, Safer Staffing), Participation in National QI Prescribing Observatory, ICS workstreams on SMI and health inequalities, Niche audit assurance on mortality data.