



MEETING TITLE Trust Board		MEETING DATE 28/03/2019	
TITLE of PAPER	Risk Management Report with Board Assurance Framework (BAF), Corporate Risk Register and Risk function updates	PAPER REF	6.2
STRATEGIC OBJECTIVE(S)	All		
PURPOSE OF THE PAPER	The purpose of this paper is to provide: <ul style="list-style-type: none"> • detail of updates to the BAF and changes to the Corporate Risk Register • an update on security developments including action on violence and aggression against staff • an update on delivery of key information governance workstreams 		
For Approval	<input type="checkbox"/>	For Assurance	<input checked="" type="checkbox"/>
For Decision	<input type="checkbox"/>	Discussion/Information	<input checked="" type="checkbox"/>
AUTHOR / LEAD	Maxine M Travis, Head of Risk Rachel Monaghan, Associate Director of Performance, Assurance and Risk	ACCOUNTABLE DIRECTOR	Steve Page – Executive Director of Quality, Governance & Performance Assurance, Deputy Chief Executive
DISCUSSED AT / INFORMED BY : RAG, Operational Senior Management Team meetings, Trust Management Group. Quality Committee/Finance & Investment Committee March 2019			
RECOMMENDATIONS:	It is recommended that the Trust Board gains assurance from the robust processes in place to manage risk		
RISK ASSESSMENT		Yes	No
Corporate Risk Register and/or Board Assurance Framework amended		<input type="checkbox"/>	<input checked="" type="checkbox"/>
Resource Implications (Financial, Workforce, other - specify)		<input type="checkbox"/>	<input checked="" type="checkbox"/>
Equality Impact Assessment		<input type="checkbox"/>	<input checked="" type="checkbox"/>
Legal implications/Regulatory requirements		<input checked="" type="checkbox"/>	<input type="checkbox"/>
ASSURANCE/COMPLIANCE			
Care Quality Commission	1. All		
NHSI Single Oversight Framework	1. All		

1. PURPOSE/AIM

1.1 The purpose of this paper is to provide:

- detail of updates to the Board Assurance Framework (BAF) and changes to the Corporate Risk Register (CRR)
- an update on security developments including action on violence and aggression against staff
- an update on delivery of key Information Governance workstreams

2. BACKGROUND/CONTEXT

2.1 Risk is inherent in all Trust activities. Failure to manage risk could lead to harm to patients, staff or others, loss or damage to the Trust's reputation and assets, financial loss and potential for complaints, litigation and adverse publicity.

2.2 Effective risk management across all levels of the Trust is essential for safe and effective service delivery as well as pro-active planning for Trust development. This paper details the processes in place to effectively manage risk.

BOARD ASSURANCE FRAMEWORK

2.3 The BAF for 2018/19 is presented at Appendix 1. Quarterly risk level projections set out in the BAF reflect actions and milestones set out in Trust level and Directorate level business plans which are aligned to the strategic objectives and tracked on a quarterly basis.

2.4 For Q3, deviations in risk ratings against projections made at the start of the year are given below. A summary of key actions to mitigate risk and explanations for deviation from projected risk levels are presented on pages 4-5 of the BAF. Projections for Q4 and actual end position for the BAF 2018/19 are being finalised by Directors with support of the Risk Team.

Closedown and re-cast of the Board Assurance Framework

2.5 The annual process for closedown and re-cast of the BAF began in Q4 of 2018/19.

2.6 A presentation was made to TMG 13th February 2019 with recommendations for closedown and re-casting of the BAF 2019/20 and directors engaged a process of consultation on principal risks to delivery of their business plans.

2.7 The Board Development Meeting (BDM) held on 28th February 2019 considered the projected year-end position for 2018/19 and recommendations for re-articulation of principal risks to delivery of the Trust's ambitions for 2019/20.

2.8 The BDM reviewed the principal risks on the BAF 18/19 and proposed the following amendments:

1a) Inability to deliver national performance targets and clinical quality standards – was to be separated into two risks to specifically reflect requirements of ARP and IUC with explicit reference to patient outcomes and to enacting of major incident plans

2a) Lack of capability and capacity to deliver and manage change including delivery of CIPS – it was proposed to remove the reference to CIP delivery which will be addressed under the financial risk, and make reference to delivery of transformational change linked to our strategy

2b) Inability to deliver the plan for integrated patient care services owing to multiple service tenders – was to be reframed explicit to delivery of ICS in the context of the PTS West Yorkshire tender

3a) System-wide lack of availability of workforce and impact of changes to funding streams on provision of education and training – was to be rearticulated to reflect challenges of recruitment and retention of clinical workforce aligned to requirements of IUC

3b) Ineffective strategies for promotion of wellbeing – The BDM provisionally discussed removal or re-framing of this principal risk. The Director of Workforce has requested re-framing of the risk to reflect the highest impact challenges.

In addition, it was agreed that a clearer focus on embedding of the Diversity and Inclusion strategy is required.

3c) Ineffective strategies for leadership and engagement and a developed organisational culture – this is to remain on the BAF and be reframed to reflect the requirement to embed of strategies with a focus on excellence in leadership

4a) Impact on external system pressures and changes in the wider health economy - principal risk is to be split to reflect the focus on ICS and ICP, and a separate risk recorded to document response and influence of partnership working with regards to specific reconfigurations

5a) Inefficient joint working between corporate and operational services – this risk remains with efforts to continue to align corporate services to service line delivery through delivery of the Accountability Framework

5b) Financial performance that fails to deliver our Control Total in the context of the financial status of the wider health economy and national drivers – this risk is to be split to reflect an inward focus on ability to robustly manage financial performance and an outward focus on impacts on system financial performance

2.9 The draft BAF for 2019/20 will be reviewed at TMG in March 2019 prior to presentation to the Board in May 2019.

3. CORPORATE RISK REGISTER

3.1 The CRR is reviewed by the Risk Assurance Group (RAG) monthly and comprises strategic and operational risks across the Trust that have a current risk rating of 12 or above. The Corporate Risk Register is attached at Appendix 2.

3.2 CHANGES TO CRR SINCE PREVIOUS MEETING

3.2.1 Risks added to the CRR since last Trust Board.

Risk 1186: EU Exit

IF the EU Exit proceeds as a 'no deal' THEN YAS plans for continuity of business as usual could be impacted RESULTING IN potential for disruption to patient care

Risk Rating Amber (12)

Risk assessment has been conducted in accordance with national guidance, with areas of concern identified as supply chain for medicines, clinical and non-clinical consumables, external system impacts including other health and social care providers and transport network, and capacity within the EPRR Team to deliver regional and national expectations in respect of additional command and control capacity.

Risk 1188: Workforce PDR and Training Data – Patient Transport Service

If the ESR staff data is not made available to populate the PTS contractual quality reporting THEN YAS will be unable to provide assurance to commissioners that we are meeting contractual obligations RESULTING IN potential for YAS PTS to receive performance notices on all contracts

Risk Rating Amber (12)

Work is underway with Head of YAS Academy, HR and BI to identify and correct the issues with the data to ensure contractual reporting requirements are fulfilled.

Risk 1191: NHS Number matching

IF an NHS number match is not correct THEN an incorrect patient demographics and medical history will be recorded RESULTING IN potential for providing incorrect treatment

Risk Rating Red (16)

In the EOC the NHS number is matched against a limited set of demographics to the mini-spine. This has identified a number of incorrect matches with potential for patient harm. It has been agreed that an additional data field will be added to the search which should mitigate the risk.

3.2.2 Amends to risks on the CRR

Risk 1096: Friarage

This risk is to be re-framed based on a new QIA to capture proposed urgent reconfiguration arrangements. The Risk Team await the agreed QIA.

3.2.3 Risks removed from CRR since previous meeting

The following risks have been removed from the CRR since last TMG.

Risk 1009: General Data Protection Regulations

IF YAS does not implement all the requirements of the General Data Protection Regulations by 25 May 2018 THEN non-compliance will occur RESULTING IN investigations or audits by the Supervisory Authority (Information Commissioner's Office) which may require specific remediation within a specified time and could lead to administrative fines of up to €20 million or 4% total global annual turnover (whichever is higher).

A summary closure report has been provided to TMG for assurance. It is proposed that the risk is closed as processes to comply with GDPR are embedded in routine business. (see section 5 below)

Risk 1121: Purchase of Adastra Licences for new IUC/NHS111

If the tender timescale slips further then there is a risk the extension to the current Adastra license contract will run out resulting in no Adastra licenses to operate beyond end of March 2019




Statement of work and quotes with ICT for review, a new contract will be available by the end of February 2019 if progress is maintained. Risk reduced to Amber (9) and to be monitored locally.

Risk 1163: EOC Festive rota cover

IF EOC is unable to address the predicted staffing issues for the festive period THEN there will be insufficient EMD and Dispatch cover RESULTING IN impact on service delivery, failure to achieve SLA, potential inability to safely run all dispatch bays, delays in allocating resources and resultant delay in reaching the patient

Actions included voluntary cancellation of leave, approaching A&E Ops for cover and offering additional incentives as agreed by TEG mitigated the risk. Lessons have been learned for rota planning for 2019/20 and future years. Risk is closed.

- 3.3 The CRR is colour coded to indicate the risk is within the remit of the Quality Committee, Finance and Investment Committee or the remit of both committees.

Quality Committee	
Finance & Investment Committee	
Both	

4. SECURITY DEVELOPMENTS

- 4.1 The Trust's declaration against the NHS Protect Security Management Standards Self Review Tool (SRT) was submitted in November 2016 and YAS has continued to base our annual security workplan around key areas of identified risk within the self-assessment.

Site security

- 4.2 A comprehensive programme of Site Security Risk Assessments was conducted in 2018/19 which has enabled prioritisation of remedial works and requests for capital funding based on security risk and critical assets and infrastructure. The findings have been reported through Trust Management Group and to Executive Security Review Group for assurance.

4.3 These risk assessments will form the basis for a prioritised and tiered approach to recommendations for investment in site security infrastructure which will have a robust evidence-base and rationale for prioritisation.

Staff safety

4.4 There is a national focus on provision of training to mitigate the risks of violence and aggression and YAS Local Security Management Specialist (LSMS) is involved in with the National Ambulance Security Group (NASG) in the development of these standards including training in ‘restraint’ or ‘safer holding techniques’.

4.5 The aim is to provide a high level of training to all staff, based upon the needs of their role, using a risk based approach with accredited and appropriately trained tutors, to deliver a system of training and practice that ensures the Trust is fulfilling its statutory duty to provide suitable and sufficient training to its staff in areas of identified risk.

4.6 The LSMS is working to ensure training is developed across the sector to allow for consistency and portability and with conformity with agreed national standards.

Risk Management processes

4.7 YAS Risk Team continue to strengthen our internal governance arrangements and support for staff who are victims of violence and aggression. The Data Flag and warning letter process has seen the greatest increase in sanctions, and the Trust has received a number of apologies from perpetrators which have been conveyed to the crews and publicised in accordance with best practice standards. We are pleased to report a year-on-year increase in sanctions for perpetrators of violence in aggression which is shown in the table below:

Type of sanction recorded on Datix	2016/17	2017/18	2018/19 9mths
Community service order	4	4	3
Custodial sentence	1	5	2
Fines	2	7	10
Internal sanction, data flag/warning letter issued	7	113	119
Police cautions / verbal warning	3	4	1
Suspended prison sentence	-	4	1
Total	17	138	136

4.8 March 2019 sees the launch of a support booklet for staff who are victims of violence and aggression, and a checklist for their managers. This resource has been developed collaboratively by the Risk Team, colleagues from Legal Services, Operations Directorate, PTS, FTSU Guardian and Staff Side.

4.9 The Risk Team attended the joint Yorkshire Ambulance Service and College of Paramedics Best Practice day on the 12th March 2019 where approximately 180 frontline staff attended. The team met with frontline staff and made them aware of the support available from the Risk Team following an incident as part of the security support booklet launch campaign.

- 4.10 This launch coincides with a survey to victims of violence and aggression who have reported an incident in the last quarter to understand if the support they received from the Risk Team was sufficient and if we can offer anything further. The survey will then continue be run prospectively to capture feedback and learn to continue to improve the support we provide.

Security Portal

- 4.11 The new Security Alerts portal is now active with structured risk-based alerts being added as indicated and work is underway to promote and communicate this portal, and to increase the culture of pro-active security around intelligence. The LSMS is engaging with other LSMS's across the NASG as well as regionally within the healthcare sector, and with our local Police Forces to gain relevant intelligence to inform portal alerts. The portal was demonstrated at the Best Practice Day mentioned above.

5. GENERAL DATA PROTECTION REGULATION

- 5.1 When the GDPR came into force from 25 May 2018, the Information Commissioner's Office (ICO) advised that *"if you are already complying with the terms of the data protection act (DPA) 1998, and have an effective data governance programme in place, then you are already well on the way to being ready for the GDPR"*.
- 5.2 Prior to GDPR, YAS already had robust and effective Information Governance arrangements with associated policies and procedures based on requirements of the DPA 1998 that had been embedded over a number of years. These arrangements, along with a network of engaged Information Asset Owners and the collective support of Information Governance Working Group gave YAS a positive starting point in terms of implementing GDPR.
- 5.3 A detailed action plan was put in place to implement the new General Data Protection Regulation (GDPR) structured around the 12 key workstreams:
- i. Raise Awareness
 - ii. Capture and Review Records of Processing Activity (ROPA)
 - iii. Determine the Legal Basis for Processing
 - iv. Demonstrate Compliance with Consent Requirements
 - v. Comply with more stringent Transparency and Fair Processing Requirements
 - vi. Manage Children's Rights
 - vii. Support Individual's Rights
 - viii. Manage Subject Access Requests (SARs)
 - ix. Detect, Report and Investigate Personal Data Breaches
 - x. Carry out Data Protection Impact Assessments (DPIAs)
 - xi. Implement Data Protection by Design and Default
 - xii. Appoint a Data Protection Officer (DPO)
- 5.4 In February 2019 we provided assurance to Trust Management Group that delivery of the action plan was completed with ongoing adherence to the regulation being business as usual.

6. DATA SECURITY AND PROTECTION TOOLKIT

- 6.1 From April 2018 the new Data Security and Protection Toolkit (DSPT) replaced the Information Governance Toolkit (IG Toolkit) to form part of a new framework for assuring that organisations are implementing the National Data Guardian's ten data security standards and meeting their statutory obligations on data protection and data security. The DSPT also supports evidencing the key requirements under the General Data Protection Regulation (GDPR).
- 6.2 The DSPT Toolkit requires compliance with assertions which are designed to be concise and unambiguous. Certain evidence items are considered a minimum baseline expectation which an organisation must have in place. These are indicated as "mandatory" elements for Ambulance Trusts and account for 100 of the 151 assertions. The use of the "mandatory functionality" aims to ensure attention is focused on those highest priority elements of data security and information governance, whilst providing an opportunity for organisations to evidence improvement over time against the recommended elements.
- 6.3 Our programme of internal audits in this and the previous year provide evidence of assurance in relation to risk management, information governance processes, ICT data security. Additionally a number of internal audits are currently underway by the Internal Audit function that will provide assurance and additional supporting evidence for the DSPT, these include IM&T Risk Management, Network Device security and management, Data warehouse control, ICT business continuity, and a 'Pen' test for ePR.
- 6.4 Our Internal Auditors, Audit One, are currently undertaking a review of a sample of mandatory DSPT assertions, reviewing our statements and a representative sample of supporting evidence to provide assurance that the Trust's annual DSPT declaration is properly supported by underlying processes, data and evidence to meet the ten Data Security Standards.

Data Security Awareness Training

- 6.5 Data Security Awareness training is a mandatory assertion within the DSPT. The requirement is that:

At least 95% of all staff, have completed their annual Data Security Awareness training in the period 1 April to 31 March

- 6.6 This is a challenging requirement for the ambulance sector, and the view of Ambulance Trusts within the National Ambulance IG Group (NAIGG) that responded to a question from the YAS Risk Team is that they will not achieve the 95%. Most aim to achieve 85% and asking their senior management group to sign off the compliance level prior to submission of the DSPT.
- 6.7 YAS continue to work toward optimising our compliance which sits at 90.89% as of 18.3.2019 and have recognised the risk of not achieving the full % compliance requirement on the Corporate Risk Register.

- 6.8 The Trust is on track to deliver the final publication self-assessment which will be reported by 31st March 2019 and will be used by the CQC for use as part of the Well-Led inspection to identify how the organisation is assuring itself that the standards are being implemented.

7. CHANGES TO THE INVESTIGATORY POWERS ACT

- 7.1 The Investigatory Powers Act 2016 (IPA) regulates the powers of public bodies to carry out surveillance and investigation, and covers the interception of communications data.
- 7.2 From 1st November 2018 a number of changes were made to the scope of the IPA and public bodies have been required to make three submissions to the Home Office between January and March 2019 to confirm formal readiness.
- 7.3 It is not envisaged that these changes will have an operational impact on the Trust as YAS has not enacted previous legislation, however the Trust is required to acknowledge the changes and ensure appropriate levels of awareness amongst key personnel within the ICT and Information Governance Team should use of the IPA be necessary.
- 7.4 To this end, the IG Team has made the required Home Office submissions, the final being required by 28th March 2019; these are signed of by the SRO, Steve Page, Executive Director of Quality, Governance and Performance Assurance, Deputy Chief Executive. A standard operating procedure to enact the legislation is in final draft, agreed by IG and ICT and will be presented to TMG for formal approval in April 2019.
- 7.5 The Trust is required to have processes in place to be compliant with the new regime by the transition date of 17 April 2019 and there are no concerns that this deadline will not be met.

8. PROPOSALS/NEXT STEPS

- 8.1 Agreement of the BAF Q4 end position with Directors and creation of a final draft of the BAF 2019/20
- 8.2 Review of the Corporate Risk Register will continue through the corporate governance cycle
- 8.3 Continue to progress the Security workplan and mitigate security-related risk.
- 8.4 Deliver the mandatory requirements of the DSP Toolkit and submit by 31st March 2019
- 8.5 Ensure preparedness for transition to new arrangements for enacting IPA legislation.

9. RECOMMENDATIONS

- 9.1 It is recommended that Trust Board gains assurance from the robust processes in place to manage risk.

10. APPENDICES/BACKGROUND INFORMATION

10.1 Appendix 1: Board Assurance Framework

10.2 Appendix 2: Corporate Risk Register