South East Coast Ambulance Service
NHS Foundation Trust

Agenda No	08/18

Name of meeting	Trust Board	
Date	26 April 2018	
Name of paper	Risk Report	
Responsible Executive	Bethan Haskins, Executive Director of Nursing & Quality	
Author	Andrew Lyons – Risk Management Improvement Lead Samantha Gradwell – Head of Risk	
Synopsis	This report updates the Board on the progress being made with risk management and an overview of the risk profile of the Trust.	
Recommendations, decisions or actions sought	To note and discuss	
Does this paper, or the subject of this paper, require an equality impact analysis ('EIA')? (EIAs are required for all strategies, policies, procedures, guidelines, plans and business cases).		**No**

INTRODUCTION

This report provides members of the Board with:

- Assurance the Risk Management Improvement Plan continues to address the issues and concerns detailed in the; Care Quality Commission (CQC) South East Coast Ambulance Service NHS Foundation Trust Quality Report, published on 5th October 2017.

- An overview of risks within SECAmb and how risk management is continuing to evolve.

ASSURANCE OF RISK MANAGEMENT IMPOROVEMENT PLAN

The Risk Management Improvement Plan objectives continue to be scrutinised weekly at the; Risk Management Task and Finish Group (TFG) and Compliance Steering Group (CSG) and an overview of progress was provided to the Audit Committee on 19th April 2018.

Clarifying the governance, roles and responsibilities are essential and this has been strengthened in the draft Risk Management Policy v10.0, which is scheduled for consultation/ engagement from the beginning of May 2018.

Following the external health check on the organisations risk management system (Datix) and subsequent report published in November 2017, the Datix risk management module has been re-configured to ensure it functions more effectively. In February 2018 the risk management profiles on Datix were revised to strengthen security access and the newly formatted risk register now enables risks to be managed more robustly from board to practitioner level.

On 17th January 2018 the Executive Management Board were presented with a Risk Management Update Report and subsequently agreed the standardised terms of reference (ToR) for each of the operational groups. For consistency each Chair has now been asked to incorporate the standardised narrative which describes the monthly management of risk covering:

- Progress of action(s)
- Adequacy of controls (controls assurance) when identified
- Risk grading reviewed
- Reasons for Principle Risk Lead failing to meet a review date
- Status review (Open or Proposed for Closure)

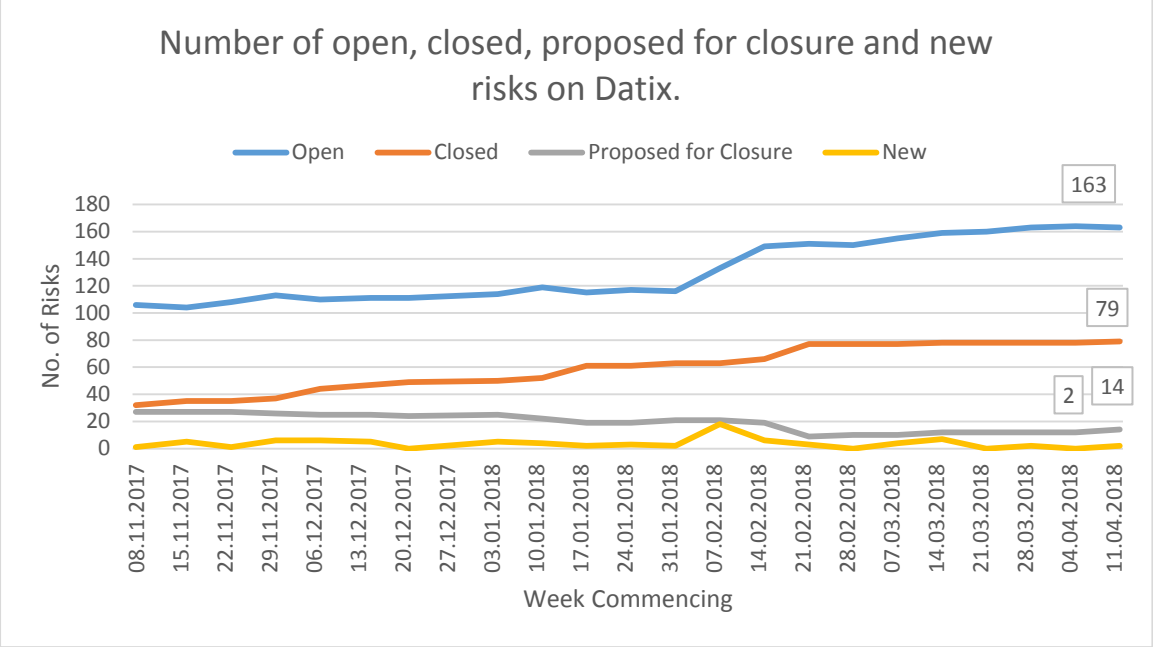
The Risk Management Project lead continues to develop capability by working with each of the chairs and this includes attending monthly meetings to ensure the model outlined above is embedded.

Going forward, an audit schedule described in the improvement plan will provide the Trust with assurance that risks are robustly managed within their associated group and a dashboard is being developed to provide a more detailed analysis of the risk register.

The data analysis from scheduled audits will determine which groups may require further support to ensure risks are being managed robustly.

An overview of the risk register detailed in graph 1 is presented each week at the TFG and CSG. This graph shows a constant trajectory, which is expected as the development of risk management progresses.

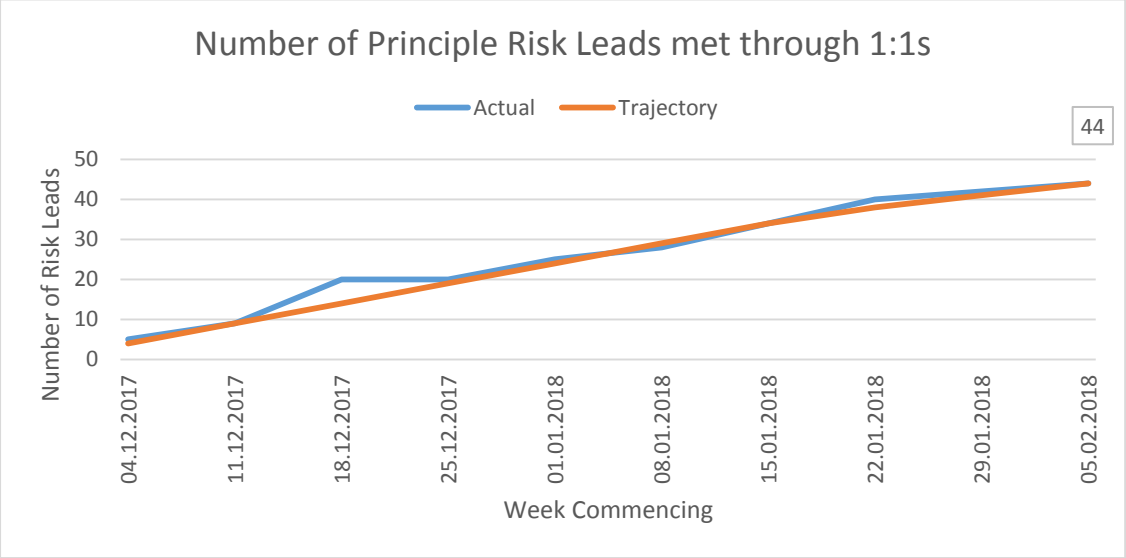
Graph 1



Between December 2017 and February 2018 the Risk Management Project Lead reviewed each of the open risks on Datix during 1:1 meetings scheduled with each of the Principle Risk Leads. A total of 44 review meetings took place and they were also used as a training and development opportunity, identifying areas that needed improvement, for example; narrative needed to more reflective and risk grading needed to be reviewed when actions became controls.

Graph 2 below illustrates meeting with each of the principle risk leads and is a further example of data presented each week at the TFG and CSG:

Graph 2



A scoping exercise was completed in January 2018 to ensure the previous organisational risks, which had been managed on the data base; SharePoint, had been migrated onto Datix. The outcome was that all risks have been appropriately transferred.

Another scoping exercise was completed in January 2018 to ensure any *local* operational &/or directorate risk registers that may have been operating, were migrated onto Datix. The outcome was that none were identified. On-going analysis however, has recently identified risk management gaps within both Health and Safety and Project management.

Health and Safety

- A baseline assessment has identified workplace inspections and health and safety inspections working practice and frameworks are inconsistent, including the recording of associated risks.
- The risk management procedure will include a section on health and safety risks recorded onto Datix.
- The identified gap has been recorded on the risk management improvement plan with key stakeholders involved, who are progressing this issue.

Project Management

- Risks with a grade of less than 8 are recorded onto individual project risk logs which are not stored onto a central register.
- The risk management procedure will include a section on project risks recorded onto Datix.
- The identified gap has been recorded on the risk management improvement plan with key stakeholders involved, who are addressing this issue.

The CQC visited on 19th January 2018 as part of their 'deep dive' to review the progress of risk management. Attendance included the Head of Risk, Risk Improvement Lead, Director of Nursing and Quality and the Chief Executive. Formal feedback from the CQC is not immediately expected, but the presentation outlining our progress and the subsequent discussions were very positive.

Although the formal education programme is not scheduled to start until May 2018, raising the awareness of risk has already commenced, including a risk awareness poster placed on each Station/Make Ready notice board in January 2018. The poster included a new mailbox risk@secamb.nhs.uk enabling any potential risks to be reported to the risk team throughout the organisation (appendix 1).

OVERVIEW OF RISKS

Following the reconfiguration of Datix, SECAmb can more effectively report on the distribution of risks. The risk register now displays the following standardised criteria routinely downloaded from Datix and the information highlighted in brackets alongside the criteria is illustrated in graphs below:

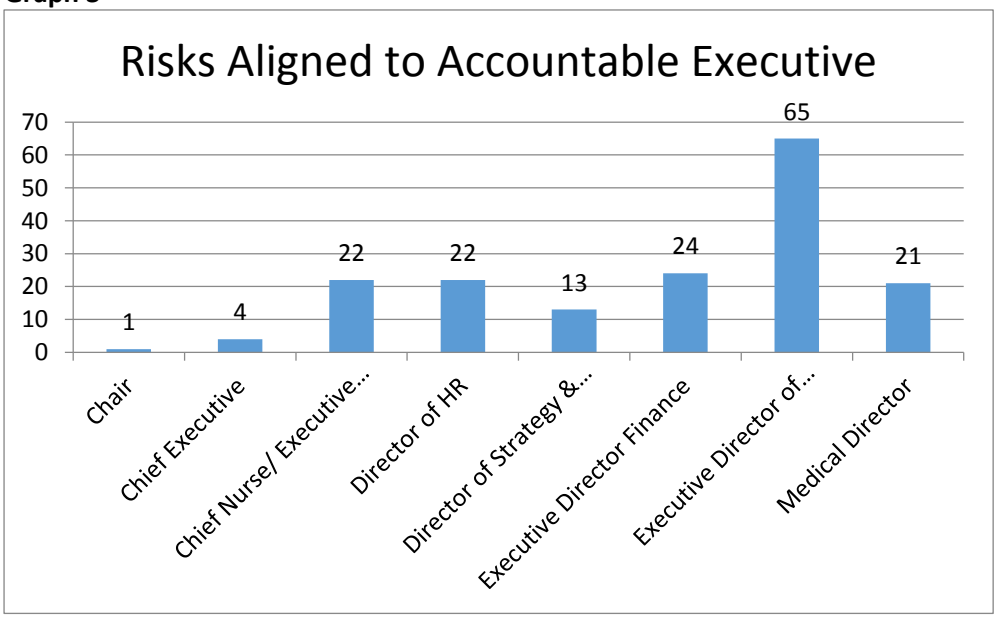
Risk Register Criteria

- Reference (Datix)
- Title
- Description
- Risk ratings
  - Inherent
  - Residual **(Graph 5)**
  - Target
- Controls in place
- Adequacy of controls
- Gaps in controls

- Mitigations planned / underway
- Dates
  - Opened
  - Last review
  - Next review
  - Closed
- Accountable Executive **(Graph 3)**
- Principle Risk Lead **(analysis shows 11 leads have 6 or risks they are managing)**
- Group / Board **(Graph 4)**
- Board Committee **(Graph 5)**
- Strategic Goal **(Graph 6)**

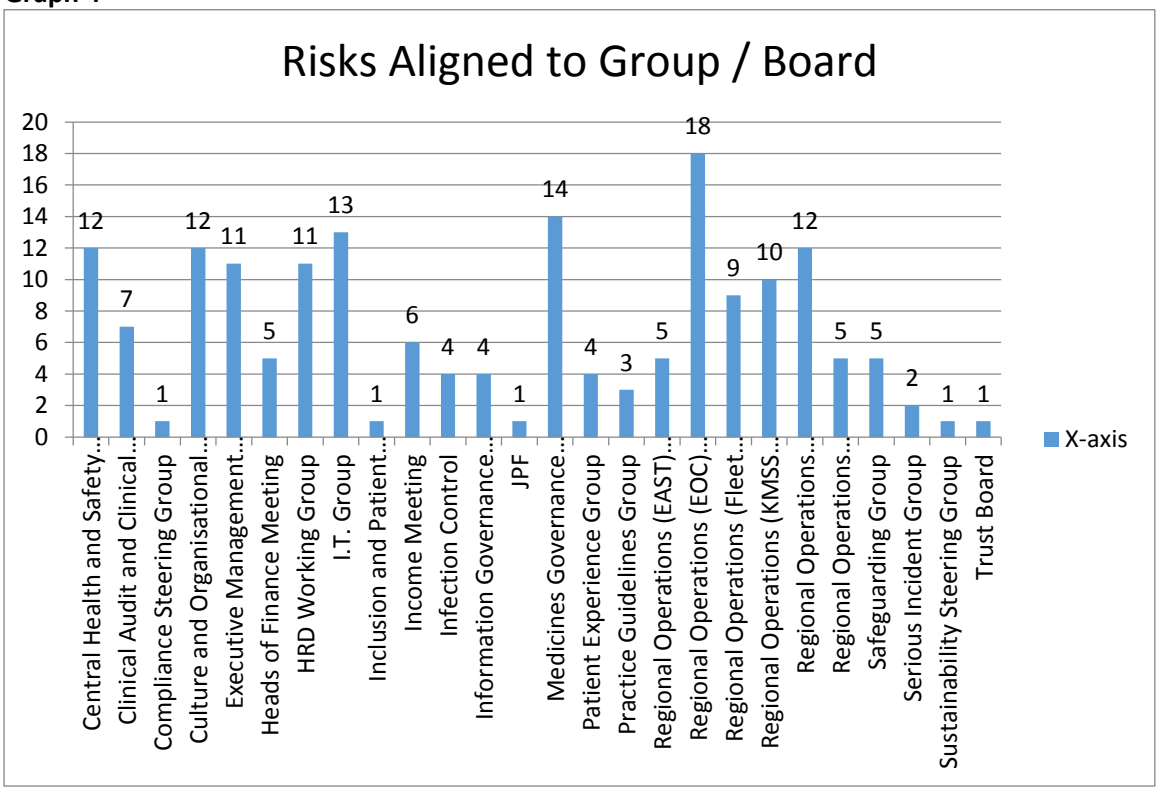
Graph 3 shows the largest number of organisation risks are aligned to the Executive Director of Operations on Datix, which is expected. This data can be further broken down to show how these risks are distributed across each of the Regional Operational Area.

Graph 3



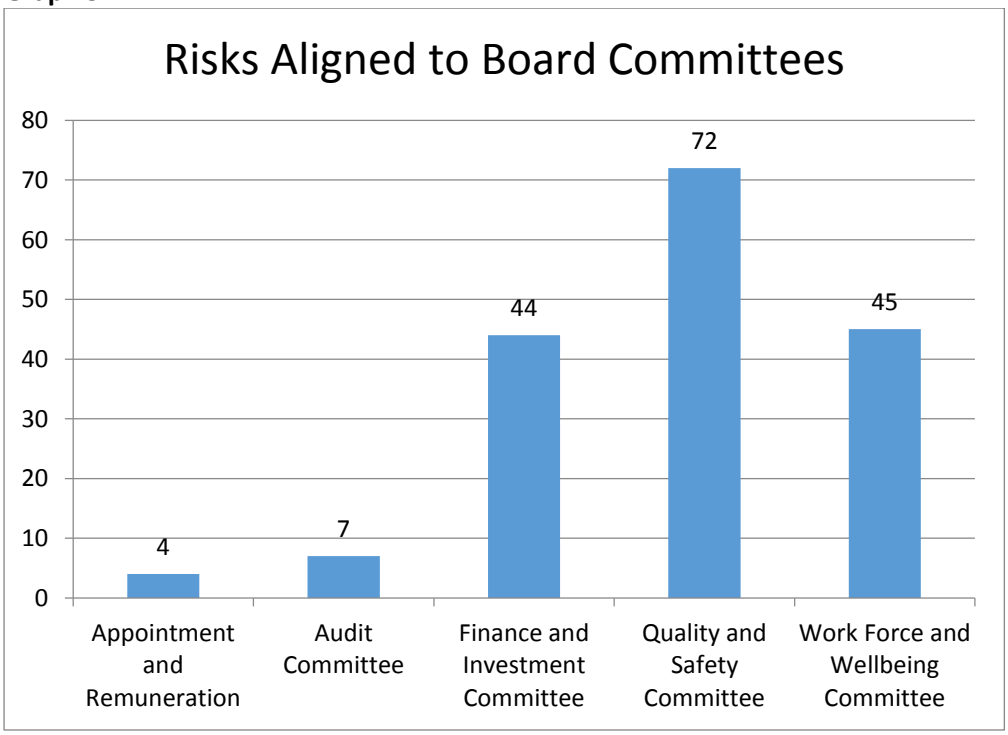
Graph 4 shows a good distribution of risks across the organisation Groups and Boards, with responsibility for reviewing these risks undertaken in accordance with their terms of reference.

Graph 4



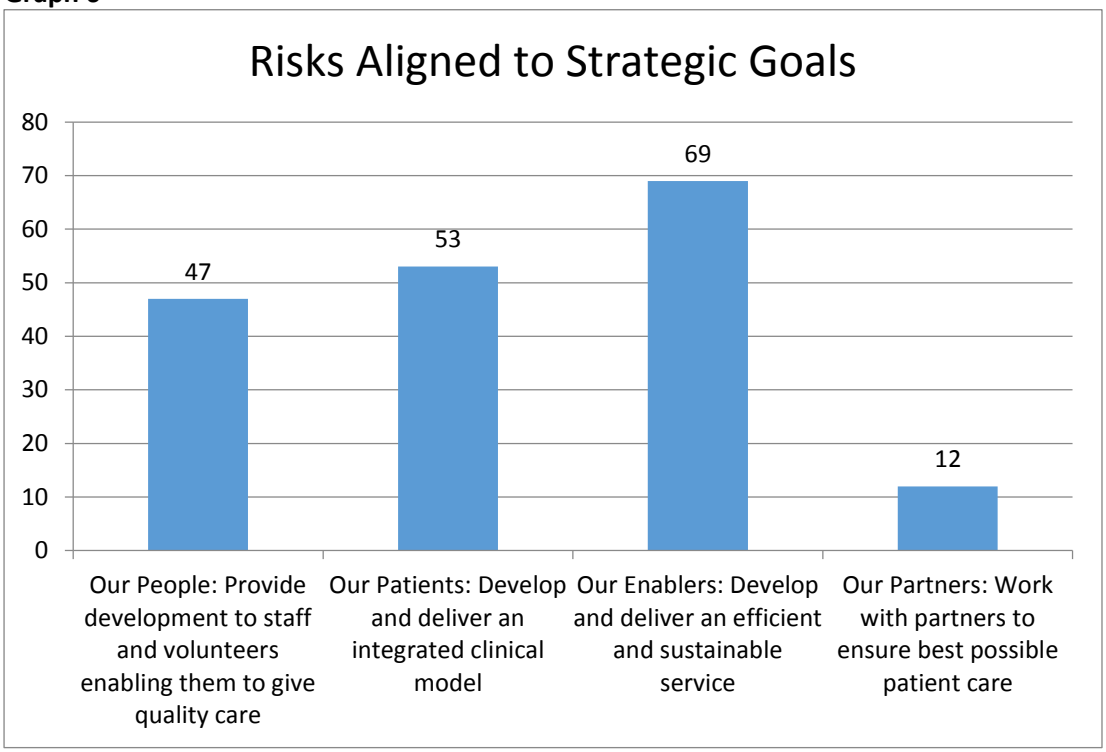
Graph 5 shows the distribution of risks across each of the Board Committees which enables oversight by each committee.

Graph 5



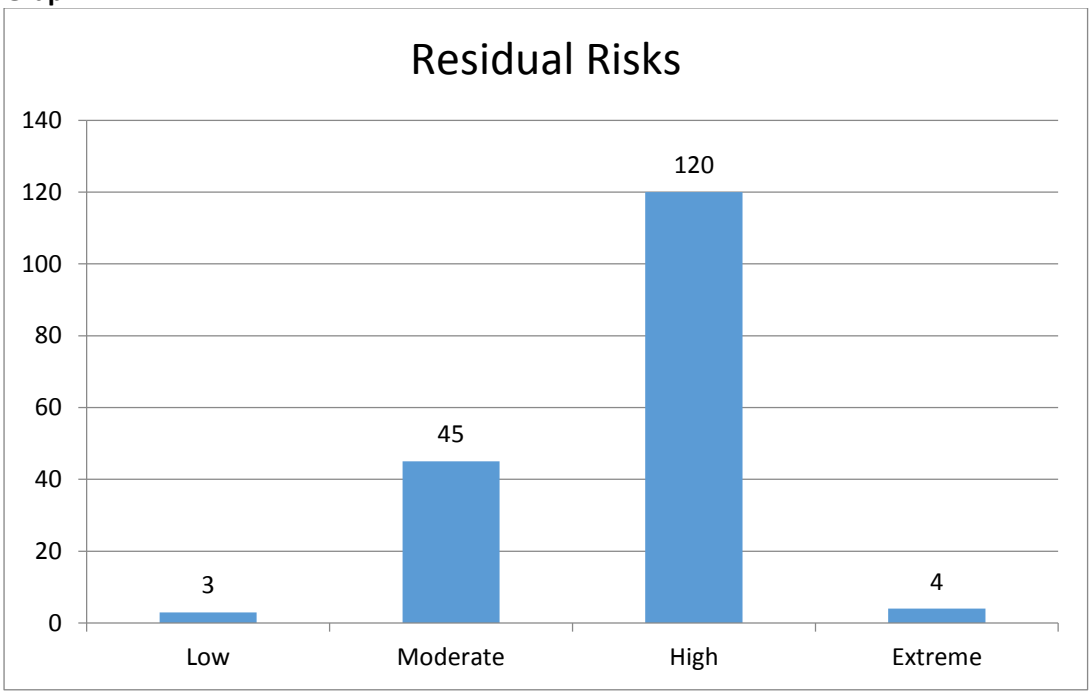
Graph 6 shows distribution of risks across the organisations strategic goals and this data can be further broken down by risk grade to support the Board Assurance Framework.

Graph 6



Analysis of the risk register revealed an inconsistent approach to how risks were graded. All residual risks with an extreme grading (scored 15 and above) have recently been reviewed and moderated and graph 7 below now shows the current distribution of residual risks.

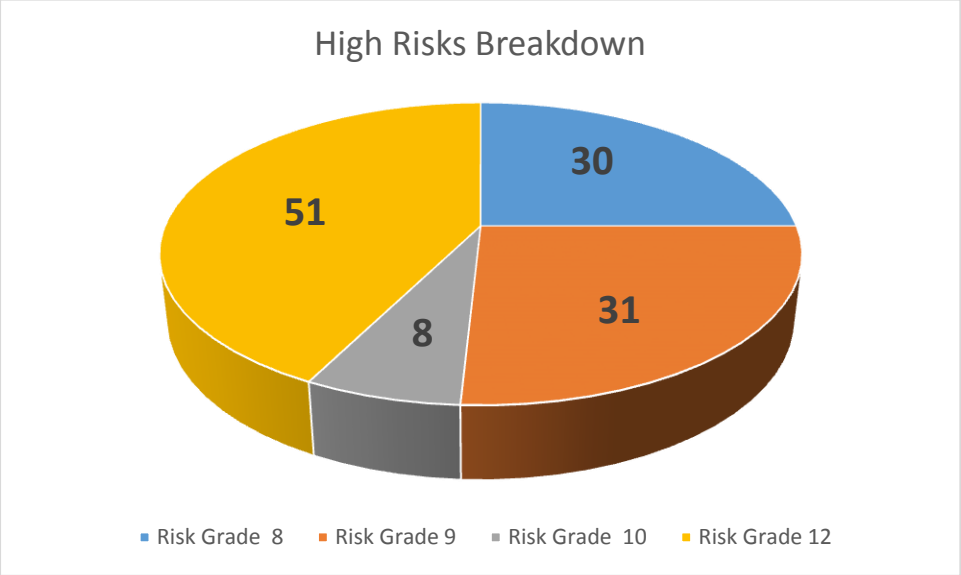
Graph 7



For context, a breakdown of the 120 high risks shown in Graph 6 above have been detailed in Pie Chart 1 below.

This Pie Chart shows the distribution of the risks graded as high (risks graded as high will have a score of; 8, 9, 10 and 12) and work is now underway to further review and moderate these risks.

Pie Chart 1



NEXT STEPS

1. Risk Management Strategy incorporated into SECAmb's Governance Strategy from June 2018.

2. Feedback, evaluation and approval of revised Risk Management Policy (v10.0) from May 2018.

3. Feedback, evaluation and approval of revised Risk Management Procedure (v6.0) from May 2018.

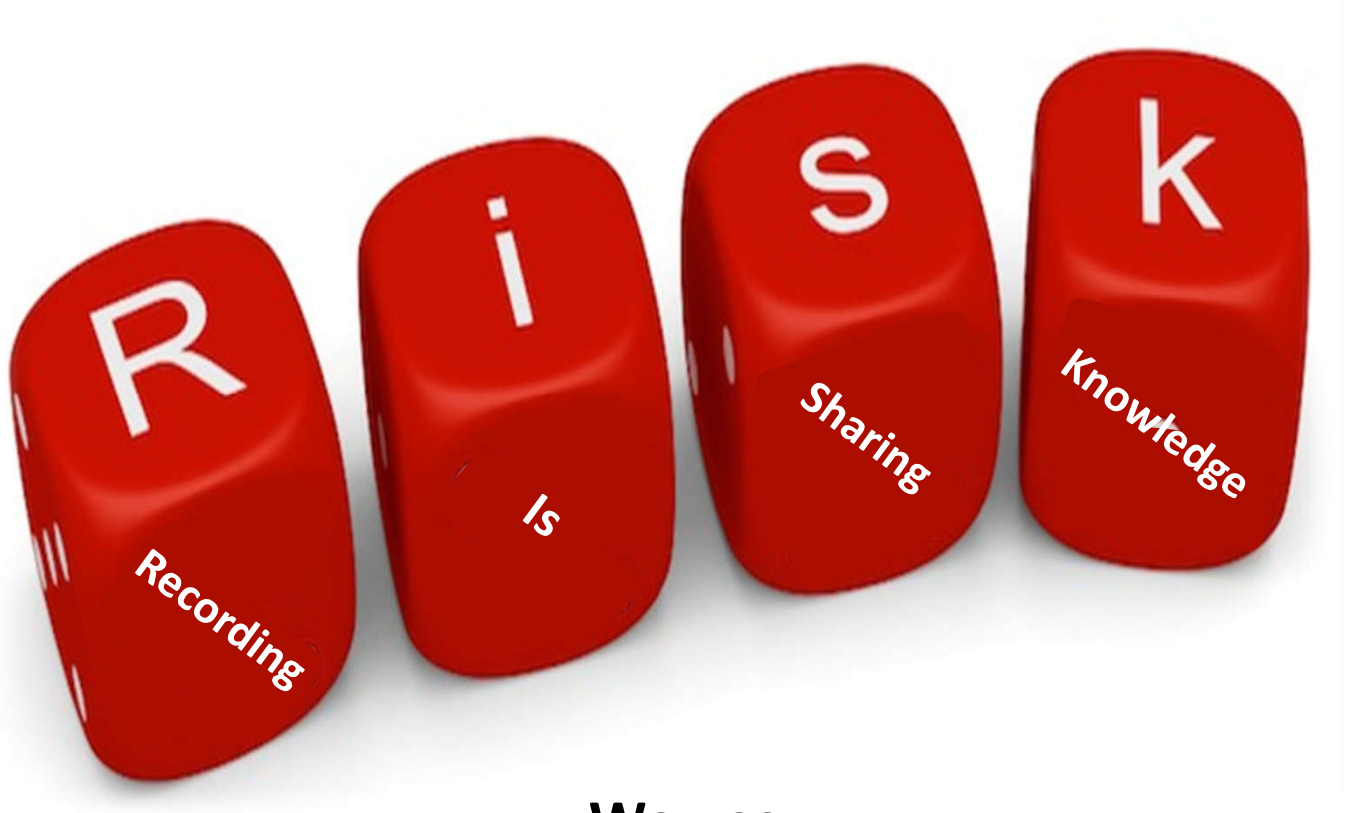
4. Roll out of the education and awareness programme from May 2018

5. Continue to develop risk management across Groups, Committees and Boards, ensuring robust data will help inform decision making and support a safe culture, including:

- Attend Groups, Committee and Boards to ensure risk management is embedded
- Audit Groups, Committee and Boards for assurance and/or to identify gaps.
- Analyse data from Datix and provide reports to Groups, Committee and Boards as required and in accordance with their ToR.
- Ask Groups, Committee and Boards what information from Datix they require going forward.

6. Continue to support strengthening the Board Assurance Framework

NHS
South East Coast Ambulance Service
NHS Foundation Trust



We use

Datix®

not only to record incidents (IWR1s) but also to record our risks.

Risk Management training and awareness is being rolled out across SECAmb during 2018, but until then, we still need to hear from you.

If you think you may have identified a risk, please email your line manager or email the Risk Team: risk@secamb.nhs.uk
Please continue to report incidents via the IWR1.

Risk is everyone's business

South East Coast Ambulance Service NHS
NHS Foundation Trust

Agenda No	08/18

Name of meeting	Trust Board
Date	26 April 2018
Name of paper	Board Assurance Framework
Responsible Executive	Executive Team
Author	Peter Lee, Company Secretary
Synopsis	This BAF sets out the risks identified in the risk register that the most threaten the ability of the Trust to achieve its strategic goals. Its aim is to ensure the Board is sighted on these risks and how they are being managed.
Recommendations, decisions or actions sought	The Board is asked to; 1. agree the risks to be included in this version of the BAF 2. consider the mitigation and actions to manage each risk; and 3. note the extreme risks not included in the BAF. The Board is also asked to note that it will by June receive for approval the governance and assurance enabling strategy, which will set out the overarching assurance framework, which this BAF will form part of.

Does this paper, or the subject of this paper, require an equality impact analysis ('EIA')? (EIAs are required for all strategies, policies, procedures, guidelines, plans and business cases).	**No**

Board Assurance Framework

1. Background

In June 2017, the Trust Board approved the trust's five-year strategic goals and the related two-year objectives (Appendix 1). The Board Assurance Framework (BAF) established in light of the new strategy was a 'top-down' view of the executive, of the principal risk to each objective.

In February 2018, the executive reviewed its approach to the BAF, in response to both the feedback from the Trust Board, and the work being progressed on the risk register as part of the risk management improvement plan. The executive agreed that the BAF needed to be a more 'bottom up' view, in order to link more closely to the risks identified in the risk register.

This new version of the BAF, therefore, includes the risks from the risk register that the executive recommend to the Board for inclusion, on the basis that they are the key risks. The BAF will come to every meeting of the Trust Board.

2. Assurance Framework

This BAF is effectively a risk report. It forms one part of an overarching assurance framework, which includes the multiple sources of assurance relied on by the Board. This overarching framework is being set out in the governance and assurance strategy, which is one the enabling strategies in the Delivery Plan. The aim is to complete this for approval by the Board in June 2018.

3. The Board Assurance Framework – process and purpose

Each identified risk recorded in the (Datix) risk register is linked to one of the Trust's four strategic goals. The relevant forum is responsible for scrutinising the risk; ensuring robust management.

1. Our People	2. Our Patients	3. Our Enablers	4. Our Partners
We will respect, listen to and work with our staff and volunteers to provide development and support that enables them to provide consistent, quality care to our patients	We will develop and deliver an integrated clinical model that meets the needs of our communities whilst ensuring we provide consistent care which achieves our quality and performance standards	We will develop and deliver an efficient and sustainable service underpinning by fit for purpose technology, fleet and estate	We will work with our partners in STPs and blue light services to ensure that our patients receive the best possible care, in the right place, delivered by the right people

Figure 1 Strategic Goals

The executive reviews the risk register, deciding which risks should escalate to the BAF. The BAF should be dynamic, and the Board will be asked to approve the inclusion of any new risk, and the removal of an existing risk, as recommended by the executive.

The BAF should therefore include risks identified in the risk register that most threaten the ability of the Trust to achieve its strategic goals. It is intended to ensure the Board is properly sighted on the risks, and provide assurances in relation to how they are being managed. The BAF should also inform the Trust Board agenda.

Risks are quantified in accordance with a 5x5 risk score matrix used across the NHS, assessing the consequence should the risk materialise and the likelihood of it materialising.

	1-3	Low risk
	4-6	Moderate risk
	8-12	High risk
	15-25	Extreme risk

4. Risk Register - Extreme Risks

In addition to the three extreme-rated risks included in the BAF, there are two other risks within the risk register rated extreme. Details of these are summarised below.

ID	Risk	I	R	T	Next Review
174	Capacity and capability of the PMO and Project teams across the Trust is likely to be an issue with multiple agendas and many projects launched simultaneously which presents a risk to the overall delivery of the programme	20	20	8	28.04.18
367	(links to BAF risk 281) When searching for personnel files in SharePoint it is not bringing back accurate search results. It is at times bringing back nothing or the wrong information.	16	16	4	23.04.18

5. Current status – BAF version 1.0

Version 1.0 of the BAF includes 12 risks, as outlined in the dashboard. The risk radar illustrates how each risk is rated post controls.

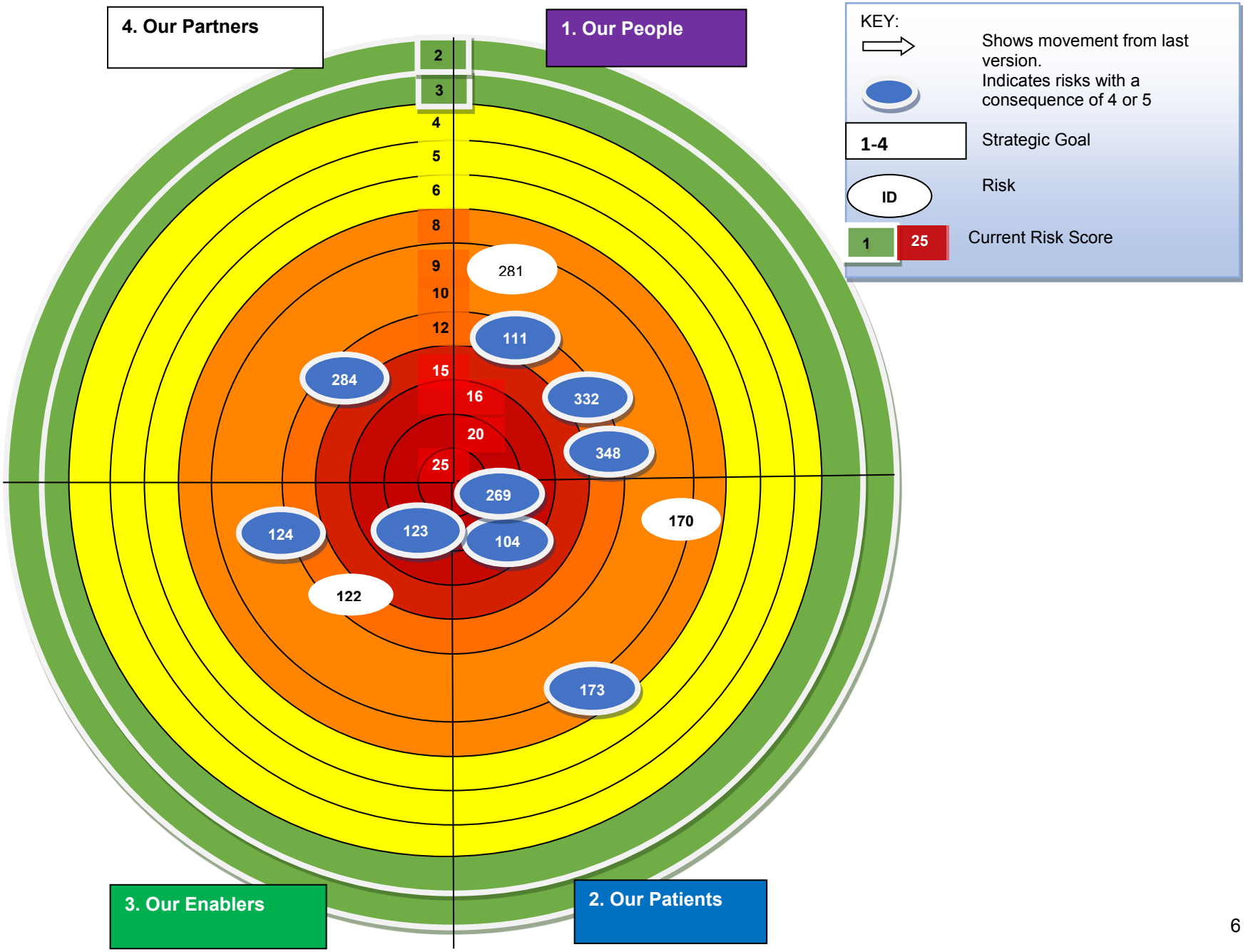
The Board will scrutinise the steps being taken to manage BAF risks 332, 111 and 269 as part of the Delivery Plan deep dives, on the Trust Board agenda.

The Board is asked to agree the risks included in this version of the BAF; consider the assurances set out; and note the other extreme risks listed. Any potential gaps in the BAF identified by the Board will be considered by the executive for inclusion in the next version.

The Board is also asked to note that work will continue as part of the risk management improvement plan to develop the risk register, ensuring improved risk descriptions and inclusion of all the controls, gaps, assurances and actions.

Links to objectives	BAF Dashboard	Inherent Score	Residual Score	Target Score	Committee
1, 2, 3 & 4	Risk ID 332: Lack of awareness and engagement in the Culture Change Programme. This links to risk 340 & 333, which describes the risks of a negative / sceptical response to the culture programme and / or resistance.	16	12	8	WWC
2 & 4	Risk ID 111: Risk to the continuity of service delivery and resilience due to unfilled vacancies. This may lead to increased costs on overtime (bank/agency spend) and low morale / wellbeing issues amongst substantive staff. This may also lead to increased sickness due to the increased pressure and stress within teams.	16	12	4	WWC
2 & 4	Risk ID 348: Lack of compliance with H&S legislation	16	12	4	WWC
2	Risk ID 281: Inability to produce staff records and meet the IG requirements for safe storage. This links to Risk ID 367 relating to SharePoint searches not bringing back accurate search results and, at times, nothing or the wrong information.	12	12	3	WWC
5, 7 & 8	Risk ID 104: Turnaround delays at hospitals has an adverse impact on patient care and the Trust's ability to achieve national performance standards.	20	16	4	QPS
5, 6, 7 & 8	Risk ID 170: Delivery plan fails to provide the impact needed to achieve the organisations strategic objectives, including correcting the issues identified by the CQC as 'Must Dos'.	16	12	4	AuC
7	Risk ID 173: Lack of alignment between the strategic goals / objectives, BAF, Delivery Plan, project KPI measures and the integrated performance report. This may lead to lack of consistency and misunderstanding / error in reporting and mitigating risks	16	12	4	AuC
5, 6, 7 & 8	Risk ID 269: Failure to achieve national performance standards for call answer (within 5 seconds 95% of the time) increases the risk of delay in providing timely advice and treatment to patients.	25	20	5	QPS
9 & 10	Risk ID 122: Data Quality	15	12	3	AuC
9, 11 & 12	Risk ID 123: Failure to achieve national performance targets, ensuring timely advice and	20	20	4	FiC

	treatment to patients.					
9 & 10	Risk ID 124: IT Infrastructure Resilience		15	10	5	FiC
13	Risk ID 284: Fragmentation of services with the 111 planned re-procurement		16	12	4	FIC


4. Our Partners
1. Our People
3. Our Enablers
2. Our Patients
2
3
4
5
6
8
9
10
12
15
16
20
25
281
111
284
332
348
269
170
124
123
104
122
173
KEY:
Shows movement from last version.
Indicates risks with a consequence of 4 or 5
1-4
Strategic Goal
ID
Risk
1
25
Current Risk Score

BAF Risks

Goal 1 Our People	**Risk ID 332:** Lack of awareness and engagement in the Culture Change Programme. This links to risk **340** & **333**, which describes the risks of a negative / sceptical response to the culture programme and / or resistance.	**Date risk opened: 17/10/2017**

Underlying Cause / Source of Risk: A lack of awareness and engagement in the Culture Change Programme could negatively affect staff perception of what is happening and their commitment to support delivery.	**Accountable Director**	Director of HR & OD
	Scrutinising Forum	HR Working Group
	Inherent Risk Score	**16** (Consequence 4 x Likelihood 4)
	Residual Risk Score	**12** (Consequence 4 x Likelihood 3)
	Risk Treatment (tolerate, treat, transfer, terminate)	**Treat**
	Target Risk Score	**08** (Consequence 4 x Likelihood 2)

Controls in place (what are we doing currently to manage the risk)
The communication plan has helped ensure clarify on the case for change and planned approach. The Barometer group will also provide an insight and will trigger any intervention activity needed. Training requirements have been established First executive coaching session completed The first of 4 training modules for the board and senior management has taken place

Gaps in Control
Completion of the 4 training modules for the board and senior managers Agreement on roll out to staff below ?team leader-level

Assurance: Positive (+) or Negative (-)	**Gaps in assurance**

Mitigating actions planned / underway	**Progress against actions (including dates, notes on slippage or controls/ assurance failing.**

Last update	13.03.2018	**Last considered by the Board**	

Goal 1 Our People	**Risk ID 111:** Risk to the continuity of service delivery and resilience due to unfilled vacancies. This may lead to increased costs on overtime (bank/agency spend) and low morale / wellbeing issues amongst substantive staff. This may also lead to increased sickness due to the increased pressure and stress within teams.	**Date risk opened: 14/04/2016**

Underlying Cause / Source of Risk:		
Workforce data highlights recruitment and retention challenges including; - limited Recruitment capacity - high turnover and sickness in some areas - stress and burn out	**Accountable Director**	Director of HR & OD
	Scrutinising Forum	HR Working Group
	Inherent Risk Score	**16** (Consequence 4 x Likelihood 4)
	Residual Risk Score	**12** (Consequence 4 x Likelihood 3)
	Risk Treatment (tolerate, treat, transfer, terminate)	**Treat**
	Target Risk Score	**04** (Consequence 4 x Likelihood 1)

Controls in place (what are we doing currently to manage the risk)
Monthly resourcing summit between HR, Finance and Operations Managers (Chaired by Resourcing Lead). Bi-weekly task and finish groups are monitoring the unfilled staff posts with further actions being agreed. The numbers are being updated and discussed at every meeting. The recruitment team has been doing job fairs, paid for internet job sites and networking sites to bring in additional candidates. Plus approached all failed band 3 EMA's to come back as band 2 call comforters and they will then be re-tested to pull further people into the band 3 EMA role. The Trust is working with Universities and there is a healthy pipeline of graduates coming through on assessment days.

Gaps in Control
Review of internal HR processes

Assurance: Positive (+) or Negative (-)	**Gaps in assurance**
(-) workforce data	

Mitigating actions planned / underway	**Progress against actions (including dates, notes on slippage or controls/ assurance failing.**
1. Development of comprehensive workforce plan for 2017/18 2. Continue to utilise resourcing pipelines 3. Review of internal HR processes	

Last update	01.02.2018	**Last considered by the Board**	

Goal 1 Our People	**Risk ID 348**: Lack of compliance with H&S legislation	**Date risk opened: 27.11.2017**

Underlying Cause / Source of Risk:	**Accountable Director**	Director of Nursing & Quality
Limited evidence and assurance is available that the Trust has effective systems and processes to ensure it is discharging all its duties under H&S legislation. Some improvements have been made and an independent review was commissioned (due to report in Q1) to help establish the current gaps and priorities.	**Scrutinising Forum**	Central H&S Group
	Inherent Risk Score	**16** (Consequence 4 x Likelihood 4)
	Residual Risk Score	**12** (Consequence 4 x Likelihood 3)
	Risk Treatment (tolerate, treat, transfer, terminate)	**Treat**
	Target Risk Score	**04** (Consequence 4 x Likelihood 1)

Controls in place (what are we doing currently to manage the risk)
Management has agreed an enhanced H&S team A number of specific H&S risks have been identified (on the risk register) with related mitigating actions, for example in contractor controls assurance; fleet ergonomic assessments; incidents of violence and aggression; MSK and manual handling injuries; fire safety; and working from heights. A H&S dashboard for the H&S working group has been developed to ensure focus in the right areas The H&S Group has gone from quarterly to monthly meetings and reports directly to the executive management board Introduced a range of H&S metrics into the Integrated Performance Report Some Board members have completed IOSH training The Board receives a Q report – first one in Q4 of 2018/19.

Gaps in Control
Recruitment to the H&S team Completion of IOSH training for Board members

Assurance: Positive (+) or Negative (-)	**Gaps in assurance**
(+) HSE inspection visit in February 2018 focussing on Muscular Skeletal Disorders (+) violence and aggression to staff showing a slow downward trend. (-) manual handling incidents high (+) increase in H&S reporting – showing greater awareness – and decrease in RIDDOR reports.	Outcome of the independent external H&S review

Mitigating actions planned / underway	**Progress against actions (including dates, notes on slippage or controls/ assurance failing.**
Improvement plan being developed Recruitment to the H&S Team Independent H&S review to be completed Invite all members of the Trust Board to undertake IOSH training.	

Last Update	12.04.2018	**Last considered by the Board**	

Goal 1 Our People	**Risk ID 281:** Inability to produce staff records and meet the IG requirements for safe storage. This links to **Risk ID 367** relating to SharePoint searches not bringing back accurate search results and, at times, nothing or the wrong information.	**Date risk opened: 27.11.2017**

Underlying Cause / Source of Risk:	**Accountable Director**	Director of HR & OD
In 2017, a project was undertaken with the help of an external organisation to scan all staff records so that they were available on SharePoint. This project did not conclude and the risk identified was that some records were not scanned, remaining in boxes at various sites. In addition, when searching SharePoint it became clear that there were quality issues with the scanning, with some records illegible. Internal Audit was asked to undertake a review of the electronic files to help determine the size of the issue. The IA final report was issued on 6 April, along with the management response.	**Scrutinising Forum**	HR Working Group
	Inherent Risk Score	**12** (Consequence 3 x Likelihood 4)
	Residual Risk Score	**12** (Consequence 3 x Likelihood 3)
	Risk Treatment (tolerate, treat, transfer, terminate)	**Treat**
	Target Risk Score	**03** (Consequence 3 x Likelihood 1)

Controls in place (what are we doing currently to manage the risk)

HR documents have been moved from Coxheath to Crawley for sorting and work is underway to locate files across the different ambulance stations. Banstead files have been reviewed and an inventory recorded.
An internal audit was instructed on the electronic personnel files. The audit report has been issued and management responses pulled into a project mandate. Once the project mandate and business case has been approved it will be decided if this is a standalone project or part of a wider IG project.

Gaps in Control

No process and policy for electronic documents
Full inventory of paper documentation
SharePoint permissions to be set up
A project mandate to be agreed

Assurance: Positive (+) or Negative (-)	**Gaps in assurance**
+ HR were aware of the issues and reported to WWC. The gaps internal audit found replicated the issues already highlighted by HR	- Extent of the issue is yet to be fully established, although from reviews undertaken to-date and from the outcome of the internal audit, the issue is likely to relate to a minority of files.

Mitigating actions planned / underway	**Progress against actions (including dates, notes on slippage or controls/ assurance failing.**
1. A project plan / mandate is being developed with the objectives being to ensure we are not in breach of DPA and ensure all staff files are accessible in one central location by the relevant people.	

Last Update	12.04.2018	**Last considered by the Board**	

Goal 2 Our Patients	**Risk ID 104:** Turnaround delays at hospitals has an adverse impact on patient care and the Trust's ability to achieve national performance standards	**Date risk opened: 21.10.2010**

Underlying Cause / Source of Risk: Lost hours due to turnaround delays at hospital has been a long-standing, national and system-wide issue.		
	Accountable Director	Chief Executive
	Scrutinising Forum	Executive Management Board
	Inherent Risk Score	**20** (Consequence 4 x Likelihood 5)
	Residual Risk Score	**16** (Consequence 4 x Likelihood 4)
	Risk Treatment (tolerate, treat, transfer, terminate)	**Treat**
	Target Risk Score	**04** (Consequence 4 x Likelihood 1)

Controls in place (what are we doing currently to manage the risk)

Daily review of metrics for total time spent at hospital and regular reports on progress including clarity of targets and performance. No diverts, unless agreed at whole health system level in exceptional circumstances. HALOs (duty CTLs/Bronze managers) deployed to hospital sites in response to emerging handover delays. Implementation of Immediate Handover as instructed by Silver and authorised by Gold. A system wide Task & Finish Group is established. Handover and escalation policy is agreed with acute hospitals. NHSI & NHSE are working with system leaders to find a whole system approach to handover delays.
Project lead is in touch with the London region to share learning from the winter and identify actions, which can be put in place for future periods of pressure.
Crews take to action to manage individual risks e.g. observation monitoring during handover wait and escalating to nurse or consultant in charge at ED as required.

Gaps in Control

Implement the Conveyance and Transfer of Care procedure

Assurance: Positive (+) or Negative (-)	**Gaps in assurance**
(- & +) Handover data is still showing a significant number of lost hours but the summary for March demonstrates an improving trend. Overall, there was a 17% decrease in hours lost compared to the same period last year. Total hours lost at Sussex hospitals have decreased by 23%. Total hours lost at Kent hospitals have decreased by 14%. Total hours lost at Surrey hospitals have decreased by 12% (-) CQC inspection 2017 identified this as a 'should do'.	None

Mitigating actions planned / underway	**Progress against actions (including dates, notes on slippage or controls/ assurance failing.**
1. Conveyance and Transfer of Care procedure 2. Handover flow chart produced and approved by commissioners. 3. Determine best practice and build into new policy agreement signed up by commissioners and external stakeholders.	1. developed but not yet implemented

Last update	11.04.2018	Last considered by the Board	

Goal 2 Our Patients	**Risk ID 170:** Delivery plan fails to provide the impact needed to achieve the organisations strategic objectives, including correcting the issues identified by the CQC as 'Must Dos'.	**Date risk opened: 26.10.2016**

Underlying Cause / Source of Risk:
The Trust had in place a unified improvement plan primarily to address the issues identified by the CQC inspection in 2016. When the CQC returned in 2017, it found that little progress had been made. The main causes of this included a lack of capacity; lack of engagement; and issues with the culture.

In July 2017 the Trust established a new strategy, and the Delivery Plan sets out the priorities for the first two years (2017-19), including the specific areas of improvement to be achieved during 2018.

Accountable Director	Chief Executive
Scrutinising Forum	Executive Management Board
Inherent Risk Score	**16** (Consequence 4 x Likelihood 4)
Residual Risk Score	**12** (Consequence 4 x Likelihood 3)
Risk Treatment (tolerate, treat, transfer, terminate)	**Treat**
Target Risk Score	**04** (Consequence 4 x Likelihood 1)

Controls in place (what are we doing currently to manage the risk)

Recruitment to key posts (head of risk, clinical audit etc.)
Change in leadership approach; establishing through engagement a new values and behaviours framework
Better accountability through more regular supervision and improved management information
More robust improvement plans
Task and Finish Groups and Compliance Groups.
Robust Project Management Office (PMO) support.
Steering Groups established
Weekly monitoring via Turnaround Executive
Board oversight through monthly board reports
Board Committee scrutiny
A review has been undertaken of all projects across the Trust and decisions made about which should be paused / stop, to ensure focus on the priorities set out in the deliver plan.

Gaps in Control

Assurance: Positive (+) or Negative (-)	Gaps in assurance
Improvement Plans / Task & Finish / Steering Groups Delivery Plan Quality & Performance Reports CQC Deep Dives	Report updating on progress against each objective.

Mitigating actions planned / underway	Progress against actions (including dates, notes on slippage or controls/ assurance failing.
1. Continue to review and assure there are sufficient resources available to continue with improvement programme in a timely way.	1. Ongoing

Last update	12.04.2018	Last considered by the Board	

Goal 2 Our Patients	**Risk ID 173:** Lack of alignment between the strategic goals / objectives, BAF, Delivery Plan, project KPI measures and the integrated performance report. This may lead to lack of consistency and misunderstanding / error in reporting and mitigating risks	**Date risk opened: 24.08.2017**

Underlying Cause / Source of Risk:
A review undertaken by the Executive during Q4 of 2017/18 identified a lack of alignment with the various reports to the Board, making it difficult to judge the progress being made and key risks.

Accountable Director	Director of Strategy
Scrutinising Forum	Executive Management Board
Inherent Risk Score	**16** (Consequence 4 x Likelihood 4)
Residual Risk Score	**12** (Consequence 4 x Likelihood 2)
Risk Treatment (tolerate, treat, transfer, terminate)	**Treat**
Target Risk Score	**04** (Consequence 4 x Likelihood 1)

Controls in place (what are we doing currently to manage the risk)

Development has been undertaken on the risks to strategic objectives (BAF), Delivery Plan and IPR and the risk register.
Delivery Plan and IPR has been reviewed and will continue to be developed
Approach to the BAF has been reviewed by the Executive Management Board; it is now more bottom up to reflect the risks as identified in the risk register.

Gaps in Control

Need to link the BAF risks with the metrics in the IPR
New approach to the BAF to be approved by the Board

Assurance: Positive (+) or Negative (-)	Gaps in assurance
(+) feedback from the Board re IPR and Delivery Plan narrative	

Mitigating actions planned / underway	Progress against actions (including dates, notes on slippage or controls/ assurance failing.
1. Review the metrics in the IPR and draw a clear link with the BAF risks and Delivery Plan 2. Exceptional Audit Committee to consider the revised risk policy and approach to the BAF 3. Board in April to receive the new approach to the BAF risk report.	

Last update	12.04.2018	Last considered by the Board	

Goal 2 Our Patients	**Risk ID 269:** Failure to achieve national performance standards for call answer (within 5 seconds 95% of the time) increases the risk of delay in providing timely advice and treatment to patients.	**Date risk opened: 24.10.2017**

Underlying Cause / Source of Risk: Increase in average length of 999 call; a shortfall in EMA recruitment; staff turnover and EMA sickness; increased call volume; limited capacity in training to ensure staff have completed pathways training.	**Accountable Director**	Director of Operations
	Scrutinising Forum	Regional Operations (EOC) Meeting
	Inherent Risk Score	**25** (Consequence 5 x Likelihood 5)
	Residual Risk Score	**20** (Consequence 5 x Likelihood 4)
	Risk Treatment (tolerate, treat, transfer, terminate)	**Treat**
	Target Risk Score	**05** (Consequence 5 x Likelihood 1)

Controls in place (what are we doing currently to manage the risk)

EOC improvement plan
Weekly task & finish group has been established to drive the recovery.
EMA retention plan approved and being rolled out.
Diamond pods for new staff have worked well providing additional support.
EOC Leadership approves all scheduling to improve resourcing.
Designated HR resource commenced to support the leadership team in managing performance issues / supporting staff wellbeing.
Approval for two development OUM's for a 6-month period.
Introduction of an analyst role to report on the call answer process and identify improvements.
Regular conference calls and quality improvement huddle with the team leaders.
AACE peer review of processes in the EOC

Gaps in Control

Assurance: Positive (+) or Negative (-)	**Gaps in assurance**
(+) Recruitment has increased with targets to bring in more staff into the trust being achieved (-) It has been identified that 1 in 5 calls are duplicate calls (ETA calls) as we do not have enough resources to send, which is being considered as part of the demand and capacity review. (-) Performance data still showing less than 80% pick up within 5 seconds (-) Improvement Plan is RAG-rated Red.	

Mitigating actions planned / underway			Progress against actions (including dates, notes on slippage or controls/ assurance failing.
1. EOC improvement plan has a range of actions			1. Plan remains at Red due to the continued challenges with recruiting necessary EMA staff, audit levels not meeting the national requirements and failure to meet call answer trajectory. The expectation is that this project will move to Amber by end of June 2018 following the realisation of Clinical Retention Plan, the introduction of the EOC Clinical Framework and CDSS, with a continued push towards meeting audit requirements. The aim then is to move to RAG green by end of August 2018 following the development of HR recruitment and progression strategies for clinical recruitment and the EMA Retention framework (including EMATL evaluation) as part of career progression scheme.
Last update	12.04.2018	**Last considered by the Board**	

Goal 3 Our Enablers	**Risk ID 122:** Data Quality	Date risk opened: 17.03.2017

Underlying Cause / Source of Risk: Lack of confidence in data interpretation and sharing because of poor database design and the requirement for manual intervention in generating reporting. This leads to a risk of data reliability; clinical and corporate.	**Accountable Director**	Director of Strategy
	Scrutinising Forum	Information Governance Group
	Inherent Risk Score	**15** (Consequence 3 x Likelihood 5)
	Residual Risk Score	**12** (Consequence 3 x Likelihood 4)
	Risk Treatment **(tolerate, treat, transfer, terminate)**	**Treat**
	Target Risk Score	**03** (Consequence 3 x Likelihood 1)

Controls in place (what are we doing currently to manage the risk)
AQI guidance and interpretation approved by the Finance & Investment Committee Data validation procedure and both automated and manual data validation processes are in place. Regular data review by operational teams, contract team and commissioners. Existing opportunities within the national data submission processes to update data as part of on-going validation and clarification The new CAD system provides cleaner and more accurate data Since the new implementation of the AQIs, another interpretation paper has been developed, with the logic applied in an SSRS report to enable the informatics team to quickly and consistently produce the necessary reports. Review of workforce data
Gaps in Control
The new data warehouse is currently in place but not fully operational. Work is currently being done to ensure this progresses at pace and will be able to reduce this risk to a safe level.

Assurance: Positive (+) or Negative (-)	**Gaps in assurance**
Operational and information team reviews of highlighted issues.	The Trust has sought independent review, which is underway as of 3 April and is to report by the end of May. A review of all ambulance trusts reporting procedures for the AQIs is soon to be undertaken by the National Ambulance Information Group, ensuring that all Trusts have the correct technical information and supporting governance

Mitigating actions planned / underway	**Progress against actions (including dates, notes on slippage or controls/ assurance failing.**
1. Development of a new data warehouse to ensure logic is captured at the time of the incident, ensuring consistency and accuracy with the data and the historical reporting.	

Last update	24.01.2018	**Last considered by the Board**	

Goal 3 Our Enablers	**Risk ID 123:** Failure to achieve national performance targets, ensuring timely advice and treatment to patients.	**Date risk opened: 13.04.2017**

Underlying Cause / Source of Risk:	**Accountable Director**	Director of Operations
It is an accepted position with commissioners that the Trust does not have the right resource / configuration to meet the new Ambulance Response Programme (ARP) targets for each category of patient. The underlying cause pre-dates ARP .	**Scrutinising Forum**	Executive Management Board
	Inherent Risk Score	**20** (Consequence 4 x Likelihood 5)
	Residual Risk Score	**20** (Consequence 4 x Likelihood 5)
	Risk Treatment (tolerate, treat, transfer, terminate)	**Treat**
	Target Risk Score	**04** (Consequence 4 x Likelihood 1)

Controls in place (what are we doing currently to manage the risk)

A joint review has been commissioned to clearly establish the capacity and resource required to meet ARP targets and, therefore, the level of investment and resource profile. In the meantime, some additional investment has been secured and commissioners have agreed to pay the contract to plan for year-end, which facilitates additional and targeted hours of operation to circa 9000 hours per day. There is daily monitoring of Cat 1 and 2 performance. Daily operational calls to manage risk and coverage issues in real time, and weekly calls to review performance and consider mitigation beyond increased and targeted additional hours in EOC and with crews.
There is weekly progress updates to the executive team and monthly reports to the Executive Management Board and Trust Board.
An external review through AACE has been completed of EOC practice & process.
AQI and Performance Task & Finish Group working on performance solutions
Surge Management Plan implementation
Implementation and continuation of hand over delay project - implemented Command Hubs reviewing Hospital delays, CCPs, HEMS and HART.
Processes to maintain safety e.g. safety huddles, clinical safety navigator, welfare call backs.

Gaps in Control

Demand and Capacity Review to be finalised.

Assurance: Positive (+) or Negative (-)	**Gaps in assurance**
(+ / -) Performance Reports showing improvement in comparison to other ambulance Trusts, in Cat 1 and 2, but concerns with response times for Cat 3 and 4	

Mitigating actions planned / underway	**Progress against actions (including dates, notes on slippage or controls/ assurance failing.**
1. Implementation of ARP Phase 3 Project to take into account the findings of the Demand and Capacity Review (phase 2 completed) 2. Hear and Treat Project 3. Develop and implement new recruitment plan including increased paramedics and Associate practitioner numbers 4. Working towards a modified 30:70 SRV to DCA split 5. Transact findings of the Demand and Capacity review	

Last update	12.02.2018	Last considered by the Board	

Goal 3 Our Enablers	**Risk ID 124:** IT Infrastructure Resilience	Date risk opened: 02.09.2014

Underlying Cause / Source of Risk: Catastrophic failure of IT systems caused by software, hardware or communications failure may result in business continuity / invoking manual processes. This is expected to be an ongoing risk due to the critical nature of IT systems in deploying resources to patients.	**Accountable Director**	Director of Finance & Corp. Services
	Scrutinising Forum	IT Group
	Inherent Risk Score	**15** (Consequence 5 x Likelihood 3)
	Residual Risk Score	**10** (Consequence 5 x Likelihood 2)
	Risk Treatment (tolerate, treat, transfer, terminate)	**Treat**
	Target Risk Score	**05** (Consequence 5 x Likelihood 1)

Controls in place (what are we doing currently to manage the risk)

1. Data is backed up to tape and kept in data safes
2. Servers and key infrastructure items are covered by maintenance/warranty
3. Servers are protected by UPS battery systems
4. Adoption of Cloud First approach for new systems and potential migration of existing systems against IM&T Cloud Services Adoption template.
5. Transfer data to a SAN environment with replication to another site to prevent data loss in the event of a failure.
6. Resilience improvements designed into the arrangements for new HQ.
7. Infrastructure being moved into purpose built data centre in Crawley with high resilience on power and cooling
8. New WAN links installed to Coxheath and Crawley with diverse routing through different BT exchanges.
9. Banstead decommissioned and relocated to Crawley and Crawley made primary site.
10. Testing on failover between sites complete December 2017
11. Network configuration upgraded and complexity reduced in Coxheath December 2017
12. Review of power requirements ongoing Coxheath and Crawley

Gaps in Control

Head of Contingency Planning & Resilience to ensure Departments should have robust business continuity plans.
Ensure each control centre can operate stand alone

Assurance: Positive (+) or Negative (-)	Gaps in assurance
(+) Regularly testing failover	Continuing minor failures occurring identifying further areas to resolve

Mitigating actions planned / underway	Progress against actions (including dates, notes on slippage or controls/ assurance failing.

1. Development of a lessons learnt document 2. Review of arrangements at senior managers meeting 3. Updating senior managers objectives to reflect requirements			
Last update	12.04.2018	**Last considered by the Board**	

Goal 4 Our Partners	**Risk ID 284:** Fragmentation of services with the 111 planned re-procurement	**Date risk opened: 30.11.2017**

Underlying Cause / Source of Risk: Kent, Surrey and Sussex Commissioners are procuring, separately, 111 and urgent care services, to be in place by April 2019. The scope of procurement risks fragmentation of service continuity depending on results of the tender.	**Accountable Director**	Director of Strategy
	Scrutinising Forum	Executive Management Board
	Inherent Risk Score	**16** (Consequence 4 x Likelihood 4)
	Residual Risk Score	**12** (Consequence 4 x Likelihood 2)
	Risk Treatment **(tolerate, treat, transfer, terminate)**	**Treat**
	Target Risk Score	**04** (Consequence 4 x Likelihood 1)

Controls in place (what are we doing currently to manage the risk)
Attendance at soft marketing procurement events Internal meeting held on 20/11/17 Resourcing and partnership approach agreed Resource of a Programme director, manager and finance officer in place Bids submitted for Sussex and in development for Kent and Surrey
Gaps in Control

Assurance: Positive (+) or Negative (-)	**Gaps in assurance**

Mitigating actions planned / underway	**Progress against actions (including dates, notes on slippage or controls/ assurance failing.**

Further actions to be identified as the process progresses			
Last update	18.04.2018	**Last considered by the Board**	

Appendix 1
Strategic Goals & Objectives

Our Themes	Our People	Our Patients	Our Enablers	Our Partners
Our five year goals	We will respect, listen to and work with our staff and volunteers to provide development and support that enables them to provide consistent, quality care to our patients	We will develop and deliver an integrated clinical model that meets the needs of our communities whilst ensuring we provide consistent care which achieves our quality and performance standards	We will develop and deliver an efficient and sustainable service underpinning by fit for purpose technology, fleet and estate	We will work with our partners in STPs and blue light services to ensure that our patients receive the best possible care, in the right place, delivered by the right people
Our two year objectives	With the support and engagement of staff and volunteers, refresh the Trust values and behaviours	Develop and deliver a clinically led process to prioritise patient need at the point of call, increasing referral to alternative services where clinically appropriate	Ensure our services are efficient and sustainable and that they are supported by appropriate levels of funding	Work with STPs to achieve the best care for our patients through emerging local out of hospital care systems
	Develop effective leadership and management at all levels, through our new selection, assessment and development processes	Further integrate and share best practice between NHS 111 and 999 services, striving for Integrated Urgent Care service where this is considered viable	Develop and deliver a digital plan which supports integration with the health system and enables the clinical model and our approach to continuous improvement	Work with STPs to design and deliver generalist and specialist care pathways for patients requiring an acute hospital attendance
	Ensure all staff and volunteers have clear objectives, and a plan for their	Further improve and embed governance and quality systems across the	Ensure that our fleet is fit for purpose and supports the clinical model	Work with education and STP partners to develop career pathways that support our

	development, set through regular appraisal	organisation, building capacity and capability for continuous improvement		staff to make effective clinical decision making
	Improve staff and volunteer health and wellbeing	Improve clinical outcomes and operational performance, with a particular focus on life threatening emergencies	Ensure that our estate is fit for purpose and supports the clinical model	Work with blue light partners to ensure collaboration supports patient outcomes and efficient service delivery

Agenda No	13/18

Name of meeting	Trust Board
Date	26.04.2018
Name of paper	IG Annual Report
Responsible Executive	Bethan Haskins, Director of Quality & Safety
Author	Caroline Smart Information Governance Lead
Synopsis	Information Governance is an enabler for Confidentiality, Information Security and appropriate Information Sharing and predominately covers the following criteria: • Information Governance Management • Confidentiality & Data Protection Assurance • Information Security Assurance • Clinical Information Assurance • Corporate Information Assurance This annual update report provides the Board with a high-level summary documenting the progress and current IG Framework status within SECAmb during 2017 / 2018. It also highlights specific concerns and actions required by the organisation.
Recommendations, decisions or actions sought	The board is asked to review this annual update report and accept the current position within the organisation

Does this paper, or the subject of this paper, require an equality impact analysis ('EIA')? (EIAs are required for all strategies, policies, procedures, guidelines, plans and business cases).	**Yes/No** NO

Information Governance Annual Report 2017-2018

INTRODUCTION

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services, resources and performance. It is therefore paramount that SECAmb has an appropriately robust Information Governance Framework in place. This acts as an enabler to ensure that all confidential information is processed legally, securely, efficiently and effectively, in order to deliver the best possible care to our patients and employees.

Information Governance stipulates / sets out the way in which NHS organisation should handle information, particularly personal / sensitive data. This refers to personal information about identifiable individuals, whether alive or deceased, for whom there is a duty to maintain confidentiality, and includes patients, and employees. The definition also incorporates sensitive data, such as race, political opinion, religion, trade union membership, physical or mental health, sexual life and criminal conviction.

All employees of the Trust, regardless of grade or profession, must adhere to an Information Governance Framework. This also includes any Local Authority employees, medical employees, directly employed, bank, agency, contractors and locum employees working in Trust services. Plus, non-medical employees and internal appointments, seconded staff volunteers and any other iteration of personnel considered staff.

Executive Directors, Directors, Managers, Supervisors and Team Leads all have a responsibility for promoting and enabling good IG practices within the work environments they manage. Each service in the Trust must ensure that a member of staff within the service has been tasked with departmental responsibilities for leading Information Governance.

This includes, but is not limited to ensuring that national and local Information Governance standards are upheld within their department(s), ensuring that ALL staff complete their mandatory IG training on an annual basis, and advising staff of their information security, confidentiality and data quality responsibilities. They also have a responsibility to contact the Trust Information Governance Lead where necessary regarding issue and/or incidents of concern.

KEY ACHIEVEMENTS 2017

- IG Framework now in place
- Successful IGT submission 2017
- Positive internal audit with RSM
- Engagement with outside regulators – Information Commissioners Office
- Membership of the NAIGG (National Ambulance Information Governance Group)
- Terms of Reference approved - IG Working Group
- Operational IG Working Group with organisation wide membership
- Trust IG training reviewed and updated
- Corporate induction training now in place

- Internal trust wide engagement now in place and developing
- IG policies reviewed
- Implementation of Privacy Impact Assessments
- Information Asset Register and appointed IAO/IAA's in situ
- IG Lead working in collaboration with external stakeholders / organisations
- Streamlined FOI process with new procedures

KEY ACTIONS 2018:

- Implement the new Data Protection Legislation – May 2018
- Attain Cyber Essentials accreditation
- Adopt a streamlined process for recording IG training completion.
- Allocation of time for mandatory IG training
- Build a robust Data Privacy Impact Assessment (DPIA) process Trust wide
- Trust review of Information Sharing Agreements & process
- Continue development of the Information Asset Register
- Create and implement a Trust wide model for Registration Authority process
- Adequately resource the Information Governance portfolio
- Undertake an organisation wide records review. Create a centralised repository for records management, standard operating procedures and look to utilise scanning solutions for historic and current records.
- Implement and resource a robust process for investigating IG related IRW-1's

BACKGROUND

The Trust appointed an Information Governance Lead in January 2017 who inherited a very challenging position. At this time, the Trust was unable to demonstrate any internal assurance, there were no operational groups representing information governance, IG policies were out of date and the Information Governance Toolkit (IGT) contained historic information some of which dated back to 2010. In addition to this, the IGT had not been audited for around 5 years, this was clearly unacceptable.

This lack of framework placed the Trust at significant risk both at an internal and external level. In addition to this Trust was not able to demonstrate that it was compliant with its legislation responsibilities.

Staff awareness of information governance was extremely 'patchy'; there was no process in place for the legal sharing of information with partner organisations some of which had taken place over a significant period of time. Privacy Impact Assessments were not completed and the Trust IG training was outdated and required a total review and update.

INFORMATION GOVERNANCE - CURRENT TRUST POSITION

GENERAL DATA PROTECTION REGULATION (GDPR) – See Appendix 2 for information

The General Data Protection Regulation (GDPR) is a significant piece of legislation, which comes into force on the 25 May 2018. This will effectively 'replace' the current Data Protection Act (DPA) 1998 although in general terms it is a 'strengthening' of what is already in place.

This new legislation incorporates the underlying principles of the existing DPA but whereas there are eight principles currently in place, GDPR will have six.

However, the legislation is still awaiting 'Royal Assent' and the current assumption is that this will take place around April 2018 although it is still not clear whether this will be known as 'GDPR' or the Data Protection Act 2018.

Summary of deviations / changes:

- Consent
- Contracts must be GDPR compliant
- Increase in penalties
- Privacy Impact Assessments / Data Protection Impact Assessments
- Privacy Notices / Information Sharing leaflets
- Data Processors / Contracts
- Subject Access Requests
- Data Protection Officer Role
- Reporting times for IG breaches

As an organisation, SECAmb must ensure it is 'ready' for the implementation of the new GDPR. Whilst information and guidance relating to the new legislation at a national level remains slow engagement at a locality level continues through swIGg (Sussex Wide Information Governance Group) with IG Leads working collaboratively throughout the locality.

In addition to this, the Information Governance Lead is now also a member of the National Ambulance Information Governance Group (NAIGG) and Surrey IG Group.

Whilst the ICO is providing organisations with information around GDPR this currently remains a 'work in progress' with formal guidelines only being published as and when the legislation develops.

GDPR remains a standing agenda item within the Trust IG Working Group. The Information Governance Lead is ensuring that all relevant groups / committees / directors are updated when information relating to this legislation is published. This engagement also includes the Trust SIRO and Caldicott Guardian.

Engagement within the organisation and via the IG Working Group is pivotal to the implementation and post implementation of GDPR.

Current key areas of concern:

- Organisation resource to manage GDPR implementation in addition to BAU activities
- Employee contracts
- Third party contracts
- Subject Access Requests
- Information Sharing Agreements
- Consent*
- Privacy Impact Assessments**

**The ICO are yet to publish final definitive guidance on the consent model. This is due for publication in February 2018.*
***The IGA (Information Governance Alliance) are due to publish guidance and new templates relating to DPIA's (Data Protection Impact Assessments) in March 2018*

Progress to date:

- A Trust wide action plan is in place to monitor progress.
- An organisation wide Privacy Notice is in place following collaboration with the swIGg group (Sussex Wide Information Governance Group) members.
- An Employee Privacy Notice is in place and available.
- The Information Governance Lead is working alongside the Sussex Wide Information Governance Group, Surrey IG Leads Group and National Ambulance Information Governance Leads Group to collaboratively address and review GDPR.
- NHS Employers have recently issued GDPR guidance in collaboration with Capsticks. Meetings have taken place with Human Resources to share information and confirm actions.
- Engagement with Procurement is in place. 'Third Party' suppliers have now been contacted to confirm that they are compliance with the new legislation.
- Meetings have taken place with Legal Team / Complaints Team / HR regarding Subject Access Requests.
- The Information Governance Lead continues to update the IG Working Group and Executive Team.
- GDPR implementation has added to the Corporate Risk Register.
- The Executive Board have been asked to accept GDPR as an ongoing risk.

Required actions:

- Information from NHS England regarding the format and content of NHS contracts.
- All IG related policies need to be updated in line with the new legislation
- Letters and forms relating to subject access requests need to be updated – meeting are arranged for 23 April 2018 during which time the updates will take place
- Staff engagement and communications regarding GDPR will take place mid-April 2018
- Complaints consent needs to be reviewed and processes documented*
- Records management needs to be robust and in line with new legislation – this is being built on through the Information Asset Owner registry and Records Management repository
- A central repository is needed detailing records management in line with Article 30 *see above
- Update IG training once new legislation is in situ
- Issue new Privacy Notices / Information Leaflets

ICO consent guidance currently remains in draft and we are awaiting final guidance

INFORMATION GOVERNANCE FRAMEWORK

Information Governance Working Group

The Trust now has a robust IG Working Group with defined and ratified Terms of Reference (ToR). The group commenced operation in June 2017 and meets on a bi-monthly basis.

There is now positive widespread group engagement, which has continued to increase since group's implementation. The agenda is robust with regular reports presented at each meeting. The group members have clear expectations of their roles and responsibilities as defined within the ToR and all meetings are thoroughly minuted with documented actions in place.

Information Governance Awareness

Fundamental to the success of delivering a robust Information Governance agenda across the organisation is the development of an IG-aware culture.

IG training is provided to all staff to promote this ethos and ensure that the \Trust meets its statutory requirements under the Information Governance Toolkit. The historic training material has now been updated in line with current legislation, cyber security initiatives and is now more robust. However, this will require a thorough review once the new data protection legislation comes into effect in May 2018.

Information Governance awareness now forms part of the Trust Corporate Induction training and is delivered by the Information Governance Lead. This training is designed to raise general awareness and a local level understanding of information governance which effectively 'dovetails' to the more specific IG training modules.

The SIRO, Caldicott Guardian and Information Governance Lead undertake practitioner-level training through completion of the relevant IGTT 'NHS and Social Care' modules, accessed via NHS Digital.
The Information Governance Lead also attends external training to develop and extend knowledge of national legislation and Trust requirements.

INFORMATION GOVERNANCE TRAINING

Current position

Since April 2017, IG training completion has been closely monitored with the L&D team providing regular IG training updates to the Information Governance Lead. However, it is evident that Trust wide there remains some disparity with the reporting of training completion figures although this is not solely related to IG training.

The Trust uses ESR as the 'gold standard' for reporting on training completion. However, the internal training systems (historic and current) used are not electronically integrated with ESR and training completion needs to be manually recorded. This 'workaround' is labour intensive, time consuming and can result in updates being delayed. There is also the increased possibility of dual recording and error occurring.

The Trust has achieved its 95% target figure relating to IG training with a figure of 95.39% obtained on the 26 March 2018.

The Information Governance Lead has continued throughout the year to utilise locally available 'tools' to promote the completion of IG training these include:

- Email signature panels
- Use of SECAmb Twitter
- Use of SECAmb Facebook Groups
- Weekly Bulletin
- CEO message(s) to highlight completion
- Emails to OUM's highlighting IG training completion

However, SECAmb has a significant volume of employees, is geographically challenged with a vast number of sites / silos. Therefore, the Trust must consider / review how Discover and ESR can be integrated or alternatively provide an electronic streamlined solution for recording training completion.

It is accepted and acknowledged that the Trust statutory and mandatory training can be time consuming. However, this is mandatory and the Trust must ensure that staff have the opportunity and time to complete this during the year.

Action: Adopt a streamlined process for recording IG training completion.

CYBER SECURITY

During May 2017, the NHS experienced a national 'cyber-attack' of its systems, which infiltrated a significant amount of Trusts within the UK. This was known as the 'WannaCry' malware attack and affected around 45 NHS organisations although SECAmb was not affected.

As part of a national directive, there has been an increased focus on cyber security. This element is now incorporated into IG Corporate Induction and the Trust mandatory training; the IG Working Group also has active membership from the Trust IT Department.

With the implementation of the new General Data Protection Regulation on the 25 May 2018 and the release of the new Data Protection and Security Toolkit the Trust must now work towards attaining a 'Cyber Essentials' accreditation.

Action: Attain Cyber Essentials Accreditation

INFORMATION GOVERNANCE TOOLKIT (IGT)

The Trust's Information Governance compliance is measured through the completion of a mandatory self-assessment process of specific standards. This is known as the Information Governance Toolkit (IGT), which all NHS organisations and providers of services to the NHS must complete on an annual basis.

Following the implementation of the NHS Operating Framework for 2010/11, all organisations are required to achieve Level 2 (of 3) performance against all requirements identified in the IGT. As an

Ambulance Trust SECAmb has 35 requirements and must demonstrate a minimum Level 2 across ALL 35 requirements in order to achieve an overall Level 2.
As part of its IGT submission, the Trust re-affirms its IG Assurance Statement. This is the terms and conditions for all organisations wishing to access and use NHS systems and services, including the N3 network

2017 Results

The IGT has three annual reporting deadlines:

- Baseline assessment on or before 31 July
- Performance update on or before 31 October
- Final submission on or before 31 March

The final performance assessment submitted to NHS Digital on the 31 March 2017 was 66%, Level 2 across all 35 requirements.

2018 Results

The Trust published its Information Governance Toolkit results on the 28th March 2018. An overall satisfactory Level 2 was obtained with a significant improvement percentage on the previous year.

The final performance assessment figure was 73% with 7 out of 35 requirements reaching a Level 3 (20%) of the overall toolkit. These positive results were due to the Trust having a sound IG Framework in place around Information Governance and Freedom of Information requests. In addition to this, a Level 3 was attained for the Clinical Audit requirement. This is due to the Trust now having a robust audit / reporting framework in place and significant work is continuing within this function.

INFORMATION GOVERNANCE TOOLKIT – RSM Internal Audit

To provide internal and external assurance the IGT is audited on an annual basis. This audit effectively 'dovetails' to NHS contracts which stipulate that organisations must attain a Level 2 IGT and demonstrate assurance. Failure to achieve this score would affect the Trusts ability to bid for future contracts and place us in breach of our existing contract requirements.

Prior to 2017, an internal audit had not taken place for a considerable number of years. This was a significant failing in terms of assurance and the monitoring of compliance.

RSM conducted an internal audit of the IGT in mid-April 2017 following the 31st March 2017 submission. An audit of 10 out of the 35 requirements, all of which were predetermined took place, this also included IG Training. With the exception of IG training, all requirements were found to be sufficient / adequate at a Level 2.

Whilst the target figure for completion of IG training is, 95% SECAmb submitted a training figure of 90.2% as at 31 March 2017. Despite our submission figure, the final audit report issued by RSM illustrated that the Trust had achieved an adequate Level 2 against the 10 requirements it was audited on. The auditors were assured that the high-level papers and forward plan previously presented to the Quality & Safety Group / Senior Management Team provided enough internal assurance for this submission.

This year's internal audit will take place on 9th April 2018 following the Trusts final submission. RSM will be auditing 10 requirements and a full audit report will be provided to the IG Working Group during May 2018.

RECORDS MANAGEMENT

The IGA Records Management Code of Practice for Health and Social Care 2016 sets out the requirements, which NHS organisations in England must comply with to manage records correctly. This document is based on current legal requirements, professional best practice and was published on 20 July 2016 by the Information Governance Alliance (IGA).

It also holds an Appendix, which contains retention schedules. These schedules set out how long records should be retained, either due to their ongoing administrative value or because of statutory requirements.

General Information

Records of NHS organisations are public records in accordance with Schedule 1 of the Public Records Act 1958. This includes records controlled by NHS organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. This applies regardless of the records format.

The Public Records Act 1958 requires that all public bodies have effective management systems in place to deliver their functions. For health and social care, the primary reason for managing information and records is for the provision of high quality care.

The Secretary of State for Health and all NHS organisations have a duty under this Act to arrange for the safekeeping and eventual disposal of all types of records. This is carried out under the overall guidance and supervision of the Keeper of Public Records, who is answerable to Parliament.

The NHS Standard Contract notes a contractual requirement to manage records for those health and social care records in organisations that are not bound by the Public Records Act 1958 or the Local Government Act 1972.

Currently the Data Protection Act 1998 (DPA) is the principal legislation governing how care records are managed. This will change once GDPR is implemented although the new legislation should follow the same principles in practice.

It sets in law how personal and sensitive personal information may be processed.
Records managers are expected to adhere to a code of practice 21 issued under Section 51(4).

The current DPA principles are:

1. Personal information must be fairly and lawfully processed
2. Personal information must be processed for limited purposes
3. Personal information must be adequate, relevant and not excessive
4. Personal information must be accurate and up to date
5. Personal information must not be kept for longer than is necessary

6. Personal information must be processed in line with the data subjects' rights
7. Personal information must be secure
8. Personal information must not be transferred to other countries without adequate protection

Policy and Strategy

Each organisation should have an overall policy statement on how it manages all of its records, including electronic records. The statement should be endorsed by the management team, board (or equivalent) and made available to all staff at induction and through regular updates and training.

The policy statement should provide a mandate for the performance of all records and information management functions. In particular, it should set out an organisation's commitment to create, keep and manage records and document its principal activities in this respect.

The policy should also:

- Outline the role of records management within the organisation and its relationship to the organisation's overall strategy
- Define roles and responsibilities within the organisation, including the responsibility of individuals to document their actions and decisions in the organisation's records and to dispose of records appropriately when they are no longer required
- Provide a framework for supporting standards, procedures and guidelines and regulatory requirements (such as CQC and the HSCIC hosted DH Information Governance Toolkit)
- Indicate the way in which compliance with the policy and its supporting standards, procedures and guidelines will be monitored and maintained
- Provide the mandate for final disposition of all information by naming the committee or group that oversees the processes and procedures
- Provide instruction on meeting the records management requirements of the FOIA, the DPA and the Environmental Information Regulations 2004.

The policy statement must be reviewed at regular intervals (at least once every two years) and if appropriate should be amended to maintain its relevance. It is also an important component of the organisation's information governance arrangements and should be referenced in the organisation's Information Governance Management Framework

Current Trust Position

KEY ISSUES:

- There is NO organisational awareness of what records are held and where
- Records are not recorded on a central database
- There is 'Dual' recording in place. Paper and electronic versions of records
- Multiple Trust silos / sites which hold information
- No audits have taken place for a significant number of years
- Retention periods not widely known
- Historic records have been transferred to purely 'shift the burden'
- Directorates need to be accountable for their own records
- Goddard inquiry implications
- Secure storage facility – capacity and contract timeframes

SECAmb became operational in 2008 following the merger of 3-indivudal ambulance Trusts, Surrey, Sussex and Kent. Each of which had independent practices and procedures coupled with a vast array of records.

It is accepted that the Trust is of a significant size, geographically challenged with a large number of sites / silos spread across three counties all of which have the potential to hold information.
However, at this time, the Trust cannot accurately determine what records it has in place.
In addition to this, it does not have a framework in place for the audit and control of its records.
This is a significant shortfall and is potentially a breach of legislation.

The move into the new Trust HQ from Lewes and Banstead further highlighted the inherent risk around records management.

Whilst the move into Crawley has been successful with the Trust now benefiting from having a central location with collaborative working, it has significantly highlighted that there are no controls in place around records management.

On review, the Trust should have scoped out its records management position at the project onset and placed a higher emphasis on reviewing the records retained within the project mandate / remit.

To date the Trust still has a significant volume of records remaining within Banstead and Coxheath. These records need to be catalogued, recorded on a central database, retention periods agreed and the decision taken whether to archive of destroy those records.

There is minimal storage available within the Trust HQ and whilst the Trust does have a records storage facility nearby the capacity will undoubtedly need to be increased. From a contractual view, there will be an increase in costs and without reviewing; the facility may have space implications.

From an information governance perspective a review of the facility needs to be undertaken to confirm what confidentiality clauses are in place with the contracted organisation (relevant under GDPR) and to also ascertain how records are recorded, kept securely and signed out / in when required.
Action: The Trust has approved an overarching records management review with the project mandate recently completed. However, this is a significant piece of work, which will need to be adequately resourced with a phased completion.

Goddard Inquiry

There is also the added implication of the Goddard Inquiry to take into consideration with any organisation wide records review. As part of the review, all NHS CEO's were contacted in June 2015 and requested to hold the records of children:

EXTRACT……
I would be grateful if you could ensure a thorough search of all your paper files, all digital records and all other information – however held – to ensure that everything of potential relevance to the Inquiry is retained.
END……..

This inquiry has implications for all organisations, which hold records relating to children.

To summarise ALL organisations must ensure that these records for the time being are held indefinitely.

Policies

The Trust Patient Data & Health Records Policy now includes the following extract, which relates to the code of practice and Goddard Inquiry, which significantly affects the destruction of health records.

EXTRACT…….

2.5. As detailed in the Records Management Code of Practice for Health and Social Care 2016, a Health Record may be destroyed 10 years after conclusion of treatment or death for an adult and 25 years for a child although this is subject to restrictions, as stated in the Goddard Inquiry (IICSA).

END……..

Records Management Policy

There is a Records Management Policy in place, which provides information around records management; the Information Governance Lead has recently reviewed and updated this policy.

Trust awareness

It is acknowledged that record retention times within the Trust are not widely known and currently there is limited information available to hand. In view of this, the Director Quality & Safety has requested that workshops be facilitated to discuss records management within the Trust and to create local procedures.

An initial workshop took place on the 1st February 2018. This was well attended by senior members of staff across all directorates and for assurance was formally minuted. It is widely accepted that there is limited awareness around records management and steps have now been taken to address this.

It is clear that a Standard Operating Procedure document is needed within the Trust. This will provide local information regarding record retention times, which are not widely known.

In addition to this and to provide audit and assurance a separate repository is to be created directorate wide to demonstrate records management. Each directorate will 'own' and catalogue those records held, this information will then feed into a Trust wide 'master' database. This repository will 'dove tail' to the Trust Information Asset Register, which holds details around information flows.

Under Article 30 of the new GDPR, organisations need to evidence 'Records of their processing activities. This specifically would apply to Information Asset Registers, Data Flow Mapping and Records Management repositories.

Actions: Produce a Trust wide Standard Operating Procedure for records management
Undertake a full Trust wide records management review
Record all records within the Trust on an overarching database
Review contract periods with external records storage suppliers

Ensure that directorates are aware of and comply with their records management responsibilities

INFORMATION GOVERNANCE POLICIES

Definition – A policy documents guidance, standards, roles and responsibilities in order for organisations to remain compliant with the NHS Operating Framework and national statutory legislation such as the Data Protection Act 1998.

Organisation wide policies apply to all relevant staff and are a 'must do' requirement. A policy document is a formal document that is regarded as a legally binding document and therefore its purpose, definitions and the responsibilities outlined within its content must be upheld in order that it may be used to support an individual or the Trust during legal action.

Policies provide a consistent logical framework for Trust action across different functions or directorates. All policies must be reviewed at least every 3 years or sooner if there is a significant change either on a local or national level such as new legislation. A good example of this is the implementation of the new GDPR in May 2018.

Following review by the JPF all policies are ratified by the Trust Senior Management Team, this ratification process is documented in the form of meeting minutes. For assurance the IG Working Group also review those polices which have been updated. Following agreement and sign off ratified polices are disseminated and made available for ALL staff through the intranet.

Current position

The Trust has a significant number of Information Governance polices which were out of date and had not been reviewed for a number of years. Again, this was a significant failing for the Trust. With the exception of two policies the suite of IG related polices have now been reviewed, ratified and published on the intranet. However, these will need to be reviewed and updated further once the final legislation for GDPR becomes law.

Action: Review and update all IG related polices in line with new Data Protection legislation.

PRIVACY IMPACT ASSESSMENTS – Data Protection Impact Assessments

Any new or significant changes to the Trust's processes or systems, which use personal / sensitive information, **must be** assessed through the completion of a PIA.

These are essentially a 'Risk Assessment tool', which are used to ensure that the Confidentiality, Integrity and Availability of personal / sensitive information is maintained. They also provide an action plan regarding perceived privacy risks.

PIA's will become a *legal requirement* under GDPR and their completion forms part of the Trust IGT requirements. The IGA (Information Governance Alliance) will be issuing a new template and national guidance in February 2018.

Current Position

Historically there was no local process or awareness within the Trust or an assurance framework in place to ensure that PIA's were incorporated within any proposed system or process changes.
A prime example of this shortfall is illustrated with the implementation of the new clinical system EPCR.

This project should have had a PIA completed within the initial 'scoping' or 'project initiation' stage.
A lack of a PIA presents a significant risk and lack of due diligence, this requirement and awareness is clearly lacking within the Trust.

The Information Governance Lead has now taken a proactive approach to ensure that departments are aware of this requirement. PIA's are a standing agenda item within the IG Working Group and the Trust SIRO who is responsible for the PMO has taken a proactive approach. There is now the assurance that any new projects include the completion of a PIA and IG engagement at the initial scoping stage / project initiation stage.

Miscellaneous information: Information Commissioners Office

The need to complete PIA's was further highlighted following a publication made by the The Information Commissioners Office in July 2017. The Royal Free London NHS Foundation Trust were found to have breached the Data Protection Act 1998 when it handed over the sensitive personal date of 1.6 million patients to Google DeepMind.

Although this Trust did complete a PIA this was only completed after Google DeepMind had already been provided within the information. As quoted by the ICO 'This is not how things should work'.

One of the key recommendations to come out of their publication was the need for organisations not to 'dive in too quickly' and ensure that PIA's are completed as soon as practical to whilst planning an innovation or trial. This will allow organisations to factor in their findings at an early stage helping them to meet legal obligations and public expectations.

Details of this breach and the subsequent publication materials were presented by the Information Governance Lead during the August 2017 IG Working Group.

Action: Develop and implement a 'Trust wide' process for the completion of PIA's including the creation of a new template in line with GDPR.
Create an internet page for advice and guidance.

INFORMATION SHARING AGREEMENTS (ISA)

Information Governance is not a 'blocker' for sharing information but as an organisation we must ensure that any information shared has a legal basis in accordance with Data Protection legislation.

It is accepted that the sharing of information between partner agencies is vital to the provision of co-ordinated and seamless provision of care services. The need for shared information standards and robust information security to support the implementation of joint working arrangements is widely recognised.

An ISA is good practice and can be a useful way of providing a transparent and level playing field for organisations that need to exchange information on a regular basis. They provide assurance in respect of the standards that each party to an agreement will adopt. This ensures that each organisation is aware of their obligations and adherence to Data Protection legislation and those legal and regulatory requirements are met. ISAs are not required where the sharing is for an ad hoc request for information.

However, **they do not** provide a lawful basis for sharing confidential information and therefore are not legally binding. Equally, the completion of an ISA is not a prerequisite for automatic data sharing and consent must always be sought unless there is a legal requirement to share information such as public interest / safety or it is in the patient's vital interest.

It is important to note that in addition to having an ISA in place organisations must ensure that when data is shared with outside organisations patients / employees are informed of this through Privacy Notices and Information Leaflets. This is paramount under the new Data Protection legislation, which stipulates that all organisations are open and transparent about the sharing of data.

ALL ISA's must be reviewed by the Information Governance Working Group, and signed off by the Trust Caldicott Guardian and SIRO. The Trust must develop and hold a centralised log (repository) for all current ISA's in place, which must be reviewed on an annual basis. This 'evidence' also constitutes part of the Trusts IGT requirements.
See Appendix 1, which provides details on information sharing.

Current position

Historically, there is very little information or records available relating to ISA's, or key governance in place around the ratification and sign off process. The Trust does not currently have a robust ISA process in place although one is being developed.

It is still unclear what information sharing takes place between SECAmb and outside partner agencies although details relating to previous information sharing is slowly becoming known but very much on an ad-hoc basis. There are considerable 'gaps' within the organisation and that an internal review within the Trust and our partner organisations needs to take place.

IBIS

A review of ISA's relating to the IBIS system is currently underway and a new central repository is now in place. The IBIS Manager has taken a proactive approach, is working closely with the Information Governance Lead, and is in the process of obtaining named IG contacts within each of our partner organisations who use IBIS.

This review process is divided into the following phases:

Phase 1

The Information Governance Lead and IBIS Manager will review all IBIS related ISA's and update the IG Working Group with progress. Once obtained the existing agreements will need to be reviewed and updated further in line with GDPR.

Phase 2

A full Trust wide review to ascertain the type of information, which the Trust shares with partner organisations, is urgently required. Current information around information sharing is very 'patchy' and the sharing of information has only becomes evident on a retrospective basis.

When questioned there is no evidence to ensure that any assurance or due diligence had previously taken place. This places the Trust at significant risk as there must be a legal basis for the sharing of information plus the assurance that this is conducted securely.

An internal review must take place. This is a significant piece of work, which will need involvement from several directorates within the Trust including the Informatics team, Research, Human Resources, Clinical Audit and IBIS.

Once this is established, contact will need to take place with our outside partner organisations. The Trust needs to ascertain what information is shared, the legitimate basis for sharing, how regularly this occurs and how this information is securely transferred.

Phase 3

Create a robust process for information requests from third party organisations i.e. CCG and Research organisations. This will ensure that there is a legal basis for sharing information.
New ISA's will need to be drawn up in line with new legislation and ratified by the IG Working Group.

Actions: Continue to develop the new repository for ISA's held within the Trust.
Conduct an internal review to ascertain Trust wide what information sharing is taking place.
Contact partner organisations and implement robust ISA's in line with new Data Protection legislation.

INFORMATION ASSET REGISTER (IAR)

ALL NHS organisations must have a fully functioning information asset register. This register acts as a repository for all the information assets held within the Trust. It also measures how information is 'flowed' within the Trust and who is responsible for access and use of this information.

The Trust SIRO (Serious Information Reporting Officer) has overall responsibility for the IAR. The Trust must also have appointed *Information Asset Owners (IAO's) and Information Asset Administrators (IAA's) within each directorate who are responsible for their respective information assets and the information they contain.

These roles are mandatory in line with IGT and NHS requirements.
**IAO's are usually Heads of Department and IAA's are Department Managers*

CURRENT POSITION

Whilst the Trust had an IAR in place this had not been reviewed for a significant number of years, was out of date and not fit for purpose. In addition to this, the Trust did not have any appointed IAO/IAA's in place. This again presents a significant shortfall and a lack of control / assurance around information sharing / collation within the Trust.

The information Governance Lead with the support of the former Trust SIRO has worked hard to produce a high-level information asset register and has facilitated several high level meetings to determine and agree *Information Asset Owners / Information Asset Administrators. These roles are mandatory in line with the IGT and NHS requirements.

**A 'Roles and Responsibilities' procedure document is now in place for IAO/IAA's. This clearly defines expectations, roles and responsibilities and will be uploaded to the IGT as evidence of the Trusts internal assurance process.*

This has involved a significant piece of work, which remains ongoing and forms an integral part of the Trusts overall IG Framework. It is also a 'must have' for the IGT and provides internal assurance that the Trust is able to demonstrate what information assets are in place and how data / information flows.

A new IAR has now been created in line with the new GDPR. This now incorporates retention periods and PIA information in addition to IAO/IAA's.

The IAR will also 'dovetail' to Data Flow Mapping. This exercise is a requirement under the IGT and defines / illustrates how information flows into, between and out of the organisation.
It forms part of the Trusts mandatory IGT requirements relating to **information security assurance** and evidence is required to confirm that this has taken place.

A data flow mapping exercise has now been completed across a variety of directorates. The Information Governance Lead will present a report for assurance to the March 2018 IG Working Group. This report will be uploaded to the IGT to support the exercise and will be presented to RSM to demonstrate assurance.
Action: The ISA is a work in progress and will continue to develop Trust wide.
Ensure half-yearly audits take place and that Data Flow mapping dovetails to these.

REGISTRATION AUTHORITY - SMARTCARDS

The NHS Spine allows information to be shared securely through national services such as the Electronic Prescription Service, Summary Care Record, Patient Demographic Service and ESR.
Smartcards are required to access NHS Spine information systems with Registration Authorities roles and responsibilities defined by NHS policy.

RA equipment (hardware and software) and consumables must meet current specifications, be adequately maintained, are made subject to business continuity and contingency planning needs, and are securely stored. NHS Digital develops and maintains the NHS Spine through the Digital Delivery Centre and adequate procedures are needed to ensure all NHS Smartcards and access profiles are issued appropriately.

Smartcards are similar to chip and PIN bank cards and enable healthcare professionals to access clinical and personal information appropriate to their role. A smartcard used in conjunction with a passcode, known only to the smartcard holder and gives secure and auditable access to national and local Spine enabled health record systems.

Registration Authorities are responsible for issuing smartcards to authorised staff with an approved level of access to patient information. This is essential to protect the security and confidentiality of every patient's / employees personal and healthcare information and to ensure that information is accessed with a legitimate basis.

It is essential that the Trust can evidence that it has robust controls and procedures in place as RA is reliant on having appropriate 'position based roles' assigned to users. There must be a legitimate reason for access and all new users must comply with e-GIF level 3 identity checks which is a government standard.

The RA Manager is ultimately responsible Trust wide for this process, and is responsible for monitoring / troubleshooting system access and overseeing those individuals appointed as RA agent's / RA super users / Sponsors who undertake key operational work requirements.

In addition to this, the Trust must audit access to the NHS spine on a regular basis. This auditing is undertaken by appointed Data Privacy Officers and is a mandatory process within the RA function.

Current position

From February 2018, responsibility for Registration Authority (RA) will sit within the Information Governance portfolio with the Information Governance Lead appointed as the Trust RA Manager.

Initial findings illustrate shortfalls within the process with no overarching 'business model' in place. At this time, the RA Manager is conducting an independent internal review of this process. Smartcards are integral to the operation of systems / services within the Trust such as KMSS 111, ESR and Clinical Audit with additional 'pockets' of clinicians who require access.

NHS recommendations are also that all Trusts have a **minimum of two RA Managers or more** (for contingency) although this is dependent on the size of the organisation.

At this time, there are two functioning Data Privacy Officers (located within the KMSS 111 service) in place who are responsible for monitoring access to the NHS Spine. They complete and evidence regular audits and report any anomalies direct to the Senior Clinical Manager. These audits are part of the overarching RA requirement for the IGT.

However, information to date demonstrates that the RA function within the Trust is 'patchy'. It is clear that a robust overarching organisational model is required. There is a lack of resource, equipment and support available to manage this process with no dedicated IT support in situ. This is a mandatory requirement as the use of smartcards, is dependent on access to a national IT system

The Trust must also ensure that, it has an adequate supply of printers to facilitate the issue of cards. Currently there is only one *fully functional* smartcard printer, which is located within the KMSS 111 service. This provides no resilience or contingency and places the organisation at a high risk considering this service and a selection within Human Resources are reliant on access to the NHS Spine.

The budget for RA also needs to be reviewed and agreed. This should not be allocated to one budget holder / directorate alone, as it relates to an overarching operational process, which is, used Trust side. The recommendation is that there is a centralised budget available as this relates to a national IT system.

In addition to this there is no internal assurance regarding access in place. An urgent review of the current access roles / positions allocated within the Trust is needed.

At this time, the Trust cannot definitively demonstrate that it is compliant around access control. Initial findings indicate that individuals who may have left the Trust or changed roles still have 'open positions' and access to the NHS spine. This is not acceptable and a clear breach of compliance. It also demonstrates that the leaver's process within the Trust is not robust or adequate.

The Trust will be looking to rollout the use of smartcards to both EOCs (Crawley and Coxheath).

This will enable clinicians (Phase 1) and call handers (Phase 2) to access the national 'patient demographic service' and 'summary care record' programmes held in the NHS Spine. Access to these systems will ensure NHS number capture.

This access will increase the NHS number usage within the Trust and forms part of our 2 year CQUIN from 2017-2019. However, this will involve a significant piece of work. The project will need to be fully scoped and 'outsourced' as the Trust does not have the capacity to internally manage the registration and issue of smartcards on such a significant scale.

Considerations will also need to be given to the management of the process with the recommendation that each EOC adopts its own RA model for contingency.

Actions: Appoint additional RA Managers to underpin the process.
Design a 'business operating model' for this service.
Allocate and agree IT support. Agree centralised budget.
Ensure that the Trust has robust business continuity plans in place
Review the Trust leaver's process to ensure that roles / positions are closed

IG INCIDENT REPORTING – IRW-1

The internal reporting of incidents is vital to all organisations. SECAmb is a substantially sized organisation, which manages a significant volume of sensitive information. The recording of Incidents demonstrates shortfalls, risks and in some cases highlights the need to improve or change processes.

Incident reporting is integral within the Trust for the following reasons:

- They illustrate that the Trust has an 'open and transparent' culture
- Provide excellent 'shared learning'
- Improve processes and reduce risk

The Trust uses an internal incident reporting system – Datix, a centrally held database used to record IG incidents. However, historically there is little evidence to illustrate how incidents were managed or what internal assurance measures were in place.

In order to demonstrate a sound IG Framework the Trust must have a robust internal reporting system in place for the recording of IG incidents. This reporting must follow clear, defined end-to-end processes, which must be followed through with clear findings / lessons learnt implemented.

CURRENT POSITION

Incident reporting is noticeably increasing and it is important that the Trust continue to recognise this positively. It is clear that historically the organisation was 'under reporting' and the increase in incidents is not necessarily due to increased errors.

There is still work to do but the Trust setting / environment is now stabilising and the key foundations are in place to develop a robust framework. This has had a positive impact within the organisation, which has been key, to the increase in reporting, which collectively is attributed to:

- Raised staff awareness around the importance of incident reporting
- Staff now being confident that the reporting of incidents is not a 'finger pointing' exercise
- An improved culture the Trust with it demonstrating that incidents will be acted upon

However, whilst increased incident reporting is a positive step there is a clear lack of resource to ensure that internal IG related incidents are reviewed and acted upon.

Conversely serious IG related incidents are correctly managed in line with national standards, i.e. graded in line with the HSCIC matrix, recorded within the Trust IG Toolkit and reported externally to our regulatory organisations. There is however a 'gap' for those incidents, which are internally reported and managed.

This 'gap' is largely due to a lack of resource, which means that the Trust cannot currently provide the internal assurance needed to support those incidents. There is a great opportunity for SECAmb as an organisation to learn and develop through incident reporting but this will only be achieved if the process is adequately resourced and there are clear processes in place.

Actions: Increase resource within the Information Governance portfolio to enable benefits realisation from internal incident reporting

FREEDOM OF INFORMATION REQUESTS (FOI'S)

The Freedom of Information Act 2000 provides public access to information held by public authorities.

The FOI Act does this in 2 ways:

• Public authorities are obliged to publish certain information about their activities; and

• Members of the public are entitled to request information from public authorities.

The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. Information held by Scottish public authorities is covered by Scotland's own Freedom of Information (Scotland) Act 2002. All requests received must be responded to within 20 days.

The Act does not give people access to their own personal data such as their employee / health records or credit reference file. If a member of the public or employee wishes to see information a public authority holds about them, they should make a subject access request under the Data Protection Act 1998.

Current position

The Trust had an experienced longstanding FOI co-ordinator in situ who resigned at the end of April 2017. Whilst this position was temporarily filled until the middle of May 2017 there was then a period

where the process was completely unattended due to lack of resource. For assurance and transparency, this at the time was recorded as a risk on the Corporate Risk register.

However, following a successful recruitment campaign the Information Governance Lead successfully appointed a substantive member of staff who joined the Trust on the 12 June 2017. The new FOI coordinator 'inherited' a significant backlog and has worked hard alongside the Information Governance Lead to manage the backlog, review and address breaches and streamline the process.

There have been two complaints received by the Information Commissioner's Office (ICO) in relation to the Trust breaching the 20-day statutory timeframe. In each instance, the Information Governance Lead has provided a full letter of explanation and apology to the requestor.

Open dialog has also taken place with the ICO and in the spirit of remaining 'open and transparent' a formal letter has been sent on behalf of the Trust by the FOI Lead. This notification confirmed the Trusts current position regarding the historic backlog whilst providing assurance that it has recently invested in additional resource to support this process.

The ICO have confirmed that they have noted the Trusts position and no further action has been taken.

The Trust is fully aware of its responsibilities to comply with this statutory process and to date *29 March 2018 there are approximately 53 requests outstanding with 24 breaches. An internal review of requests is completed on a regular basis and a weekly report is forwarded to the Trust SIRO – this process has been in place since September 2017.

The Trust now has a fully functional IG Working Group which meets bi-monthly, is chaired by the SIRO and attended by the Caldicott Guardian. FOI's are a standing agenda item for these meetings and an update report is presented within the meetings remit.

Conclusion

The last 12 months has been particularly challenging but significant progress has been made with the foundations now in place for a robust IG Framework. It is clear that a substantial volume of work is still needed which will continue to remain a work in progress and naturally evolve as the organisation becomes more established.

There are however considerable 'gaps' within the Trust which are noted within this annual review. Resource is key to providing a safe legal framework within the organisation and currently there is no resilience. The Trust is at risk as it is operating through a 'single point of failure'. This needs to be accepted and noted. Provisions must be made to ensure that there is contingency and the Information Governance Lead will be completing a business case during Quarter 1 2018 with a recommended business model.

The implementation of GDPR presents a risk to ALL organisations (public and private sector) and it is still not clear how this new legislation will affect organisations. However, the Information

Governance Lead will continue to proactively work in collaboration with partner organisations both pre and post implementation.

Internal processes and frameworks around Privacy Impact Assessments, Information Sharing Agreements and Records Management still need to be implemented. These are key information governance areas, which are of high risk to the organisation.

The organisation is becoming more 'IG Aware' and with this awareness, there is an increase in the volume of IG related questions and queries, which are being highlighted. Historic processes and agreements are now becoming known and these areas require significant review.

The formation of STP's require IG engagement, as does the implementation of new systems and processes. IG is pivotal to the success of the Trust.

Both patients and employees have the right and expect their information to be kept safe, secure and managed within the bounds of our legal obligations.

This can be ensured and evidenced through the creation and maintaining a strategic IG framework which is 'fit for purpose' within the organisation. The Information Governance Lead will continue to build on this, ensure Trust wide engagement takes place and provide regular updates through the Trust operational / executive groups.

Caroline Smart
Information Governance Lead
April 2018

Appendix 1

REQUESTS FOR INFORMATION RECEIVED FROM OTHER NHS ORGANISATIONS
The uses of clinical NHS data can be divided into two categories.

1. The first is Direct Care:

A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals including supporting an individuals' ability to function and improve their participation in life and society.

This includes the assurance of safe, high quality care and treatment *through local audit*, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care

2. The other use is Secondary Usage:

Any purpose which does not "directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided" to the individual.

Any requests for information from other organisations such as CCG's and research companies must be directed to the Information Governance Manager in the first instance. The requesting organisation must provide a 'legal basis' for requiring the information whilst stating what the requirement is for.

Section 251

Under Section 251 of the National Health Service Act 2006, the Secretary of State for Health is permitted to make regulations to set aside the Common Law Duty of Confidentiality for defined medical purposes. These are essential activities of the NHS, and important medical research, that require the use of PCD but because patient consent had not been obtained to use it for these other purposes, there was no secure basis in law.

Section 251 can be utilised when it is not possible to use anonymised information and where seeking consent is impractical, having regard to the cost and technology available.
It is administered by the NHS Health Research Authority, through a Confidentiality Advisory Group.

Appendix 2

General Data Protection Regulation

Changes to legislation

Much of the information organisations should supply is consistent with their current obligations under the DPA, but there is some further information, which they are explicitly required to provide.

The information supplied about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge

Consent

Extract from ICO 'Consent Guidance' issued March 2017

""*Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. Organisations must have an effective audit trail of how and when consent was given, in order to provide evidence if challenged."*

The recording of consent under GDPR needs to be robust, in general terms the recording of consent should not be a 'tick box' exercise. Consent to process is not required under GDPR for the provision of **Direct Care**. However, practitioners (both IG and clinical) must maintain an awareness.

However, **Secondary Care** still requires consent if patient information is to be given in full with key identifiers such as NHS numbers. Aggregated or pseudonymised information is still acceptable if it cannot be traced back to the individual.

Penalties / Fines

The current maximum penalty for data breaches stands at £500,000. Under GDPR, this significantly increases and there is the potential to find organisations who have data breaches up to:

- Tier 1 level, 20 million euros or 4% of their turnaround,
- Tier 2 level would be 10 million euros and 2%.

It is not clear how strict the ICO / Regulatory bodies will be under GDPR but the consensus at this time is that the Information Commissioners Office (ICO) may have the opportunity to 'cap' fines under GDPR. This may potentially apply to 'Public Body' organisations but clarification is still required.

It is thought that a percentage of fines would potentially apply to large 'global' organisations. However, NHS organisations have been fined historically for data breaches and are therefore not 'immune'.

Privacy Impact Assessments (PIA)

Data protection impact assessments (DPIAs) (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

Under GDPR, this now becomes a legal requirement, (privacy by design). If organisations do not complete a PIA, they could be fined.

Privacy Notices / Fair Processing Notices

These provide patients / public with information about how their information is shared. GDPR emphasises the need for transparency over how you use personal data.

The 'right to be informed' means that organisations must provide 'fair processing information', typically through a privacy notice. Privacy notices will play a greater role within GDPR and must be more robust with information to explain about 'consent' and sharing information. The Trust must also provide hard copies as a minimal legal requirement.

Data Processors

Data Processors Not Data Controllers become liable for breaches. Under the existing DPA 1998, they cannot be fined but under GDPR, this will change.

The recommendation is that NHS organisations also attain a cyber-essentials certification.

Subject Access Requests

GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63). These are similar to existing subject access rights under the DPA.

Under GDPR, organisations will not be able to charge a fee for completing subject access requests. The removal of the £10 subject access fee is a significant change from the existing rules under the DPA.

The Trust currently charges a nominal fee for this process, which cannot exceed £50, this higher amount usually, applies to third parties requesting information such as Coroners, Police and Solicitors. However, the Trust will be able to charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The statutory timeframe for subject access requests will also reduce from 40 days to 30 days under GDPR

Data Protection Officer

Under the GDPR, the Trust must appoint a data protection officer (DPO) under the following:

- The organisation is a public authority (except for courts acting in their judicial capacity)
- It carries out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- Undertakes large scale processing of special categories of data or data relating to criminal convictions and offences.

The DPO must remain 'impartial' so the consensus is that this role cannot fall to a board member as due to potential conflict of interest and the need to remain impartial.

It has been agreed, in principle, through IG Working Group engagement that SECAmb will appoint two DPO's. One will sit under a 'corporate' umbrella and the other as a 'clinical' lead. The recommendation is that these roles will sit with the IG Lead and Head of Compliance who is a senior clinician. Both roles fit within the same 'Directorate'.