Agenda item 15
Attachment 12

NHS
Surrey Downs
Clinical Commissioning Group

Title of paper:	**Governing Body Assurance Framework and Risk Register**
Meeting:	Governing Body, 231st January 2014
Author:	Justin Dix, Governing Body Secretary
email:	justin.dix@surreydownsccg.nhs.uk
Exec Lead:	Karen Parsons, Chief Operating Officer

Purpose	To Agree	
	To Advise	✓
	To Note	

Development

Description of the risk register and assurance framework

The Governing Body Assurance Framework and Risk Register are produced in conjunction with Heads of Service and other managers and reviewed by the Executive Committee.

The Assurance Framework enables the Governing Body to understand the risks to the principal objectives of the organisation and direct the Executive accordingly.

The risk register is closely aligned to the Assurance Framework but sets out a range of more operational risks within the organisation.

Local projects or service areas may have their own risk registers. At the moment the only risk register at this level is for Continuing Health Care, however a risk register for the Out of Hospital Programme is planned.

Review

The Audit Committee reviews both the Assurance Framework and the Risk Register in order to give the Governing Body assurance that they meet the requirements for the Annual Governance Statement and the system of internal control generally.

The Assurance Framework was reviewed by the Audit Committee on the 10th January, however the risk register had not been updated at this point. It has since been updated with heads of service.

At the Audit Committee it was agreed to use the 4 Ts standard to describe risk appetite in future. The Assurance Framework and Risk Register have both been updated to this effect:

- Treat - treat or mitigate is in practice the most common response, achieved by taking action to reduce the probability of the risk occurring or by reducing the impact. This enables the orgainsation to continue with the activity/objective but with controls and actions in place to maintain the risk at an acceptable level.

- Transfer - this option is normally taken to transfer a financial risk or pass the risk to an insurer. However, there is also the opportunity to agree to transfer risks to a partner organisation in a joint project, but it is important that all parties are clear to the exact extent of each partner's liability and responsibility for the risk.

- Tolerate - it may be appropriate to tolerate the risk without any further action for example due to either a limited ability to mitigate the risk or the cost of mitigation may be disproportionate to the benefit gained. The decision to tolerate would ideally be supported by a contingency plan in the event that the risk escalated.

- Terminate - some risks can only be contained at an acceptable level by terminating the activity. The capacity to address risks in the NHS in this way is limited, although it may apply to some projects that are no longer considered viable due to the resources required to manage the risks being disproportionate to the potential outcomes or benefits. The decision to terminate may mean that other more manageable or strategically acceptable risks have to then be described. An example would be terminating a contract that is unsafe or unsustainable. Terminating it may eliminate the risk but may mean that other risks have to be described and managed in the short term.

Changes to risk designation and management

As both the risk register and assurance framework have grown, they have become less manageable. The risk register has now been broken down into separate sections for different functions within the CCG and the designation of risks has been changed accordingly. However there is no variation in the structure and treatment of risk.

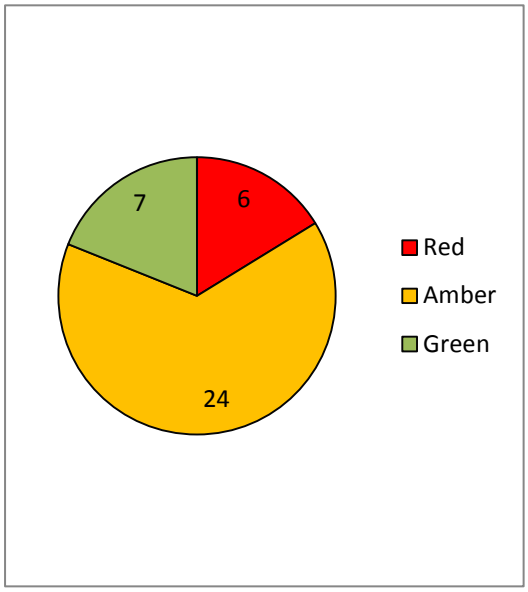
Executive Summary and Key Issues

Assurance Framework

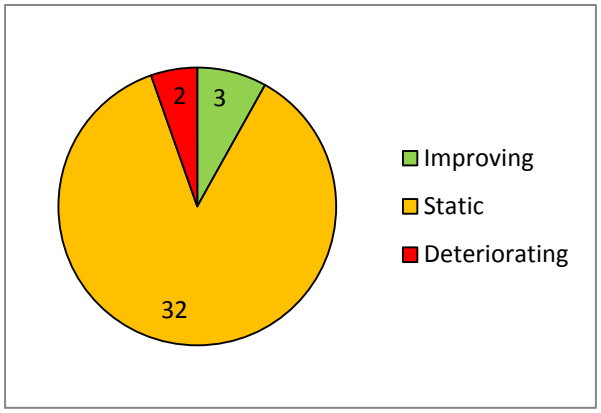
Movement within the Assurance Framework remains developmental. The key status

is as follows:

Balance of Red Amber Greens:



Improving, Static or Deteriorating:



Risk Register

Risks have been renumbered according to the team dealing with them.

A new risk has been added around failure to achieve compliance with the Information Governance Toolkit. The CCG is in the process of assigning the roles of Information Asset Owners and Data Custodians and has an Information Governance Action Plan in place, however failure to achieve toolkit requirements would have significant practical and reputational consequences for the CCG

A new risk has been added regarding achievement of the CCG's Equality Duty. A full report and action plan on Equality Duty has been provided to the 31st December

Agenda item 15
Attachment 12

Governing Body.

Risk re EDICs transfer of records: This can now be removed as the project is completed.

Reiteration of the difference between the Assurance Framework, Risk Register, and project risk registers

Assurance Framework	**Risk Register**	**Project Registers**
Risks to the organisation's principal objectives	**Broad range of operational risks**	**Risks specific to projects where change is being sought**
Key Focus for Governing Body with mitigation by the Executive	**Key focus for the Executive with mitigation by Heads of Service**	**Key focus for Heads of Service with mitigation by Project Leads**

Internal Review of Risk Maturity

A review of our risk management systems was undertaken by the Governing Body Secretary and the two lay members for Governance in December. This is attached and will require further development.

Recommendation(s):

The Governing Body is advised that the Assurance Framework and Risk Register provide positive assurance in most areas, however there are concerns about financial trends, partnerships and localities. See "Risk and Assurance" below for comments on the maturity of the system of internal controls in relation to risk.

Attachments / References:

- Risk maturity assessment (attached)
- Surrey Downs CCG Governing Body Assurance Framework Jan 2014 (under separate cover due to size and format of document)
- Surrey Downs CCG Risk Register Jan 2014 (under separate cover due to size and format of document)

Agenda item 15
Attachment 12

Implications for wider governance

Quality and patient safety: Quality and Patient safety risks will be reviewed by the Clinical Quality Committee in February.
Patient and Public Engagement: None specific
Equality Duty: There is a new risk on the risk register regarding achievement of the CCG's Equality Duty.
Finance and resources: Finance and resource are reviewed by the Executive Committee.
Communications Plan: This paper is available on the CCG web site.
Legal or compliance issues: The Assurance Framework and Risk Register are a part of the Annual Governance Statement and the overall system of internal controls. A number of individual risks relate to statutory duties.
Risk and Assurance: The CCG's approaches to risk management and risk tolerance are still maturing. There also remains a need to achieve a better understanding or risk throughout the organisation, with managers using risk assessment tools as part of everyday work rather than risk just being perceived as a compliance exercise.

Agenda item 15
Attachment 12

Measure	Failing	1	2	3	4	5	6	7	8	9	10	Exemplar
Development & understanding of risk across the organisation	*No clear understanding of risk in a consistent way across the CCG*					5						*Risk is owned and managed across every sector of the organisation*
Risk strategy	*No strategy in place or strategy not used*				4							*Risk strategy is fully owned and used operationally*
Risk appetite	*Risk appetite not defined or understood*					5						*Risk appetite is defined and measured, and implemented across the CCG*
Risk definition / classification	*No definition of risks or the context in which they operate*					5						*Risk definition fully defined in the context of the CCG as a distinct NHS body*
Risk organisation	*Risk management is at best advisory and roles are not defined*					5						*Risk roles and responsibilities fully defined an owned at every level and used in practice*

Agenda item 15
Attachment 12

Measure	Failing	1	2	3	4	5	6	7	8	9	10	Exemplar
Learning from / management of change	*The organisation serially fails to improve its risk management approach from experience*				4							*There is a culture and practice of learning from failure and developing the management of risk accordingly*
Data and information to support decision making on risk	*Risk decisions are not based on the use of empirical information or viable soft intelligence*			3								*The organisation runs on the use of high quality management information and this is reflected in risk management processes*
Management process and decision making	*No formalised management of risk and poor quality decision making*				4							*Formailsed risk management is embedded at every level of the organisation and part of the operational fabric*
Risk measurement	*There is no system of risk measurement in place*				4							*Risk measurement is standardised across the organisation and is used as an operational control process*
Risk measurement as an integral part of business continuity management	*There are no links between risk management and business continuity / disaster recovery*			3			6					*Risk and recovery are fully integrated and support preparation for a business continuity episode or major incident*

Agenda item 15
Attachment 12

Measure	Failing	1	2	3	4	5	6	7	8	9	10	Exemplar
Skills and resources	*There are few risk management skills and or these are held centrally*			3								*All staff in management roles have appropriate levels of risk management expertise and regular training*
Culture and values	*The organisation does not recognise risk within the culture and values of the organisation*			3			6					*The culture of the organisation is open to honest discussion of risks and their management*
Performance management	*Performance measures are not aligned to risk management*			3	4							*Performance and risk are fully integrated at all levels, including personal objective setting*