BOARD OF DIRECTORS (OPEN)
Meeting Date: 14th November 2018

Open BoD 14.11.18
Item 14

TITLE OF PAPER	Senior Information Risk Owner (SIRO) Annual Report
TO BE PRESENTED BY	Phillip Easthope, Executive Director of Finance, IMST, Performance & Facilities
ACTION REQUIRED	For information and Assurance

OUTCOME	To report progress and provide an overview and status of key areas covered during 2017/18, whilst identifying areas for improvement and strengthening for 2018/19.
TIMETABLE FOR DECISION	None required.
LINKS TO OTHER KEY REPORTS / DECISIONS	• NHS Digital & England Guidance • Data Security & Protection Toolkit • Cyber-Security Best Practices • Information Technology Service Management • General Data Protection Regulation • Caldicott Principles • Data & Information Quality Management • ISO27001 Information Security Management Systems
STRATEGIC AIM STRATEGIC OBJECTIVE BAF RISK NUMBER & DESCRIPTION	Strategic Aim: Value for Money Strategic Objective: A401 We will improve the productivity and efficiency of our services, maximising time spent with service users. BAF Risk Number: A401ii BAF Risk Description: Trust governance systems are not sufficiently embedded,
LINKS TO NHS CONSTITUTION & OTHER RELEVANT FRAMEWORKS, RISK, OUTCOMES ETC	As above
IMPLICATIONS FOR SERVICE DELIVERY AND FINANCIAL IMPACT	

CONSIDERATION OF LEGAL ISSUES	None required

Author of Report	John Wolstenholme
Designation	Data Protection Officer
Date of Report	October 2018

BOARD OF DIRECTORS OPEN

Item Ref: 14

Date: **14 November 2018**

Subject : **Senior Information Risk Owner (SIRO) Annual Report**

Presented by: **Phillip Easthope, Executive Director of Finance, IMST, Performance & Facilities**

Author: **John Wolstenholme, Data Protection Officer**

---

1. Purpose

For Approval	*For a collective decision*	*To report progress*	*To seek input from*	*For information*	*Other (please state below)*
				X	

2. Summary

The following report was received and approved at Finance, Information & Performance Committee on the 22nd October 2018.

The committee noted the positive assurance, and the improvement to overall information governance assurance obtained now that the committee receives this information following the change to its terms of reference

Previously the report had been reviewed and approved at Digital Information Governance Board on 25th September 2018 and the Executive Directors' Group on 27th September 2018.

Senior Information Risk Owner (SIRO) 2017/18 annual summary position on the Trust's last 12 months' data and information governance challenges, risks, progress and focused commitment towards continuous data, information and system security and protection in accordance to:

- NHS Digital & England Guidance
- Data Security & Protection Toolkit
- Cyber-Security Best Practices
- Information Technology Service Management
- General Data Protection Regulation
- Caldicott Principles
- Data & Information Quality Management
- ISO27001 Information Security Management Systems

The report provides an overview & status for key areas covered during 2017/18, whilst identifying areas for improvement and strengthening for 2018/19.

2018/17 SIRO Summary Position

Area	Risk	Response	RAG
Policies	Policies maintained, reviewed and updated within agreed timescale.	All Data & Information polices reviewed and in date. Future review staggered to reduce further risk.	G
GDPR/DP	Maintain compliance, security and protection levels to GDPR requirement.	Further strengthening and transition required across the Trust. Plan in place to support positive progress in this area.	A
Incidents	Report and manage IG incidents to Trust policy and regulatory guidelines.	Systems & processes in place to deal with incidents and protect against threats. Tested and satisfied.	G
IG Toolkit	Maintain and provide evidence needed for DSPT compliance.	The DSPT imposes a new set of requirements which will require action from different areas across the Trust. A plan is in place which identifies responsibilities and this will evolve further throughout the year. Being this is a new and evolving area, some risk is carried due to change and transition.	A
Data & Information Assets	Identification and management of all Trust data & Information assets to ensure appropriate protections, controls and ownership in place.	Foundation register for data, information, systems and flows in place. Further work continues to strengthen this area further.	A
New Processing	New processing assessed, protected and controlled to Trust policy and regulatory requirements	IG considerations incorporated at the design stage. Evidenced with recent examples using Data Protection Impact Assessments and supported discussion through DPO, services and relevant boards.	G
Training & Awareness	Trust maintains training and awareness to support Trust wide compliance and understanding.	Required compliance level is 95%, and requires focused attention to ensure target trajectory.	A
Risk Analysis	Ensure incidents & risks are reported, escalated and managed according policy and response guidelines.	Appropriate policies and processes in place to ensure incidents are logged via and managed through corporate incident and risk register.	G
IG Audits	Maintain audit action and compliance within agreed timescales.	Rating relates to the audit process and does not attempt to anticipate the findings of the audits	G
CQC	Manage, maintain and implemented quality IG services to Trust and CQC expectations and targets.	No issues raised at this time.	G
SIRO Group	Maintain regional SIRO engagement and discussion	SIRO has attended regional meeting (meeting now under review)	G
Priorities	Maintain and implement agreed,	Raised as amber due to resource	A

	statutory and mandatory IG commitments and continuous improvement programmes.	capacity and associated work required to deliver and additional responsibilities required for GDPR, DSPT & DPO. Risk should to be reduced through automation, increased trust wide responsibility and transfer of some tasks to other IG staff.	

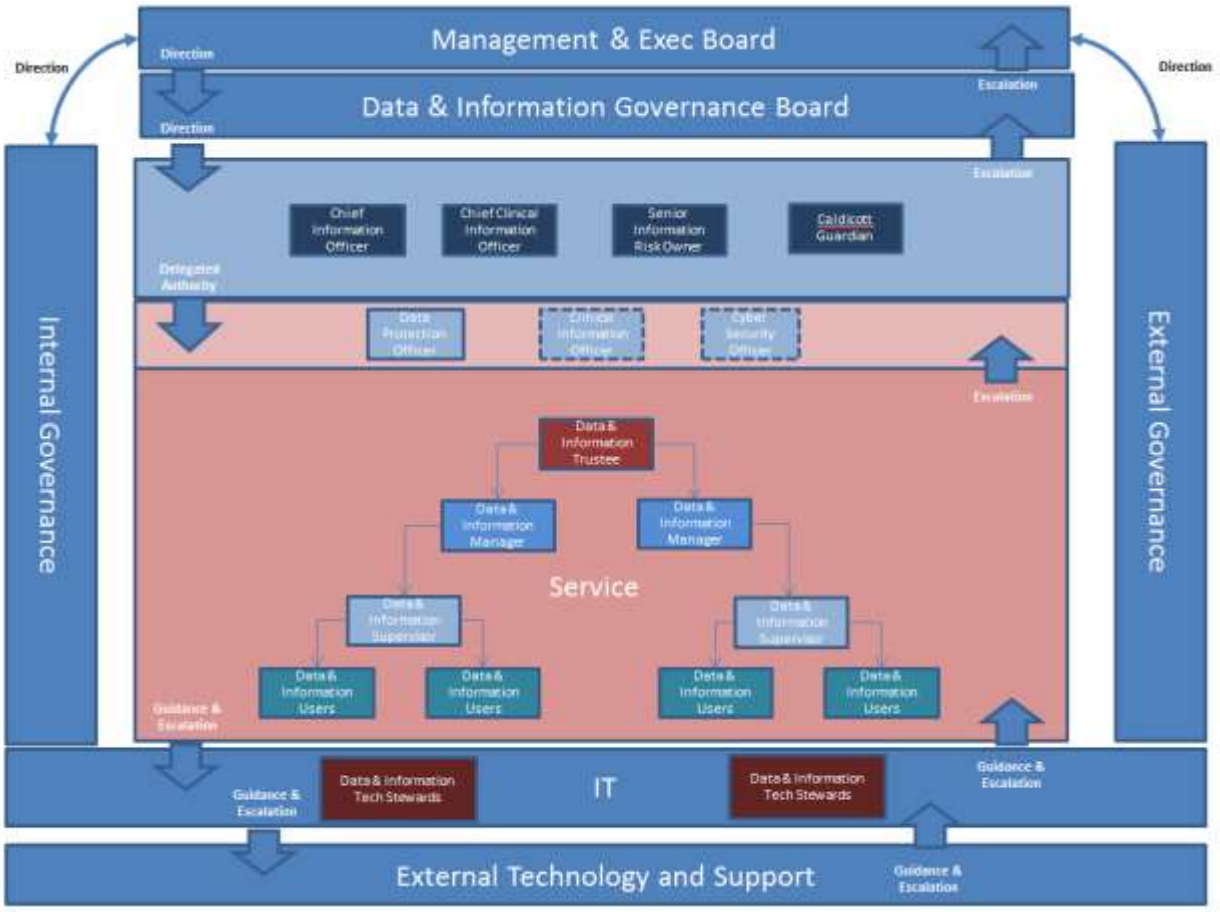
Role of the SIRO

The Senior Information Risk Owner (SIRO) is responsible for the management of information risks within the organisation and for holding Directors and other Data & Information Asset Owners (DIAOs) to account for the management of information assets and related risks and issues within their areas of responsibility. The SIRO ensures that Information Governance, information and cyber security are dealt with at the highest level of management.

Within SHSC the SIRO is the Executive Director of Finance. The SIRO is a member of the Data & Information Governance Board (DIGB) and the Executive Directors Group (EDG).

The framework for the management of data and information within the Trust is set out in the Data and Information Governance Policy – this specifies the relationship between the SIRO, other senior information governance roles (including the Caldicott Guardian, the Chief Information Officer and the Chief Clinical Information Officer) and Data & Information Asset Owners. The network of DIAOs and reporting processes to the SIRO will be further developed during 2018/19

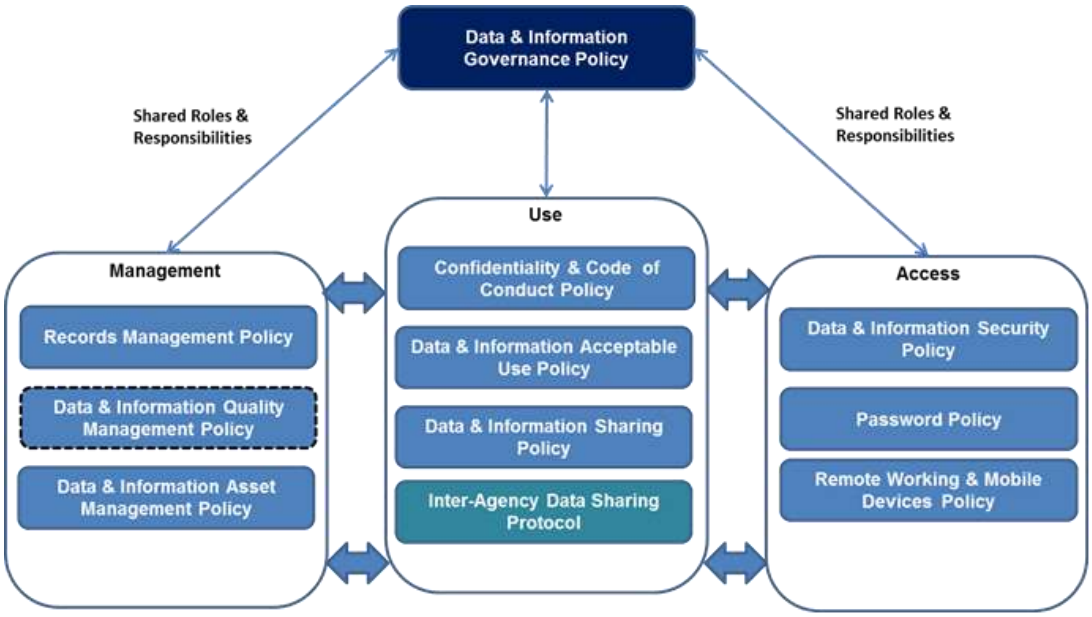
Data & Information Governance Structure



IG Policies

Area	Risk	Response	RAG
Policies	Policies maintained, reviewed and updated within agreed timescale.	All Data & Information polices reviewed and in date. Future review staggered to reduce further risk.	G

During the 2017/18 year the suite of Information Governance policies have been revised and updated. These are:



GDPR/Data Protection Act 2018

Area	Risk	Response	RAG
GDPR/DP	Maintain compliance, security and protection levels to GDPR requirement.	Further strengthening and transition required across the Trust. Plan in place to support positive progress in this area.	A

In May 2018 the Data Protection Act 1998 was replaced by the General Data Protection Regulation/Data Protection Act 2018. Building on the previous legislation, this imposes new requirements on data processors, strengthens the rights of data subjects and gives the regulator the power to impose higher fines when things go wrong.

The SIRO oversaw preparations for the implementation of the new regulations and has a significant role in ensuring the Trust complies with legal requirements.

Basic requirements for compliance are in place and a work programme has been developed to strengthen performance & position during 2018/19.

IG Incidents

Area	Risk	Response	RAG
Incidents	Report and manage IG incidents to Trust policy and regulatory guidelines.	Systems & processes in place to deal with incidents and protect against threats. Tested and satisfied.	G

Information Governance incidents and risks are reported internally with other incidents via the Trust incident monitoring system. Those with an IG element are graded in terms of seriousness and any which reach a specified level are reported externally to the ICO.

Prior to the introduction of GDPR, serious incidents were required to be reported via the Information Governance Toolkit (IGT). The IG Toolkit has now been replaced by the Data Security & Protection Toolkit (DSPT) which includes a revised incident reporting tool.

GDPR/DPA 2018 require serious incidents to be reported within 72 hours, so our internal reporting processes have been revised to allow us to identify and grade incidents quickly and report them externally if necessary. The SIRO is involved in the assessment of potentially serious incidents and has the final decision on whether to report externally.

During 2017/18 the Trust did not report any IG incidents of level 2 or above via the IG Toolkit reporting system.

Information governance incidents are reported to the DIGB as a standing agenda item.

Notification of Cyber security risks from CareCERT are received and acted upon by the IT Department.

IG Toolkit/Data Security & Protection Toolkit (DSPT)

Area	Risk	Response	RAG
IG Toolkit	Maintain and provide evidence needed for DSPT compliance.	The DSPT imposes a new set of requirements which will require action from different areas across the Trust. A plan is in place which identifies responsibilities and this will evolve further throughout the year. Being this is a new and evolving area, some risk is carried due to change and transition.	A

The final submission of the IG Toolkit was made in March 2018. This involved a self-assessment of Trust performance on a specified list of requirements giving an overall score of 68% which is graded as “Satisfactory” (all requirements at level 2 or above). The SIRO receives reports and evidence on a number of requirements and is involved in signing off the final IGT submission.

For the 2018/19 year the IG Toolkit is replaced by the DSPT. The Trust is required to make a baseline submission in October 2018 and a final submission in March 2019 but NHS Improvement requested a status report for the Trust on the areas covered by the DPST in May 2018.

An initial plan for completion of the DSPT has been submitted to the DIGB

Data & Information Assets and Flows

Area	Risk	Response	RAG
Data & Information Assets	Identification and management of all Trust data & Information assets to ensure appropriate protections, controls and ownership in place.	Foundation register for data, information, systems and flows in place. Further work continues to strengthen this area further.	A

GDPR and the Data Security & Protection Toolkit require the Trust to maintain a register of information assets and flows of personal data. These have been established and will be further enhanced during 2018/19.

New Processing

Area	Risk	Response	RAG
New Processing	New processing assessed, protected and controlled to Trust policy and regulatory requirements	IG considerations incorporated at the design stage. Evidenced with recent examples using Data Protection Impact Assessments and supported discussion through DPO, services and relevant boards.	G

Any new processing of personal information or any significant changes to existing processing require the completion of a Data Protection Impact Assessment which helps to identify any potential risks and how they may be mitigated.

The use of new technology such as Cloud storage will raise risks which will need to be assessed and appropriate safeguards implemented.

Major projects and processes are governed by the Digital Transformation Strategy.

Training and Awareness

Area	Risk	Response	RAG
Training & Awareness	Trust maintains training and awareness to support Trust wide compliance and understanding.	Required compliance level is 95%, and requires focused attention to ensure target trajectory.	A

The SIRO has completed specific, relevant training in support of his role.

All staff are required to complete the mandatory national information governance training on an annual basis. Compliance is monitored and reported by the Mandatory Training Steering Group.

There will be further staff awareness on GDPR and the DSPT provided during 2018/19.

A Data & Information Governance & GDPR SharePoint page has been established to support collaborative working and shared knowledge in this area

Risk Analysis

Area	Risk	Response	RAG
Risk Analysis	Ensure incidents & risks are reported, escalated and managed according policy and response guidelines.	Appropriate policies and processes in place to ensure incidents are logged via and managed through corporate incident and risk register.	G

Information Governance risks including cyber security risk are reported to the DIGB. Sufficiently serious risks are included in the Corporate Risk Register.

DIAOs are responsible for assessing information risks attached to the systems/assets they are responsible for and providing reports to the SIRO. Further strengthening and awareness in this area to continue as part of 2018/19 schedule.

IG Related Audits

Area	Risk	Response	RAG
IG Audits	Maintain audit action and compliance within agreed timescales.	Rating relates to the audit process and does not attempt to anticipate the findings of the audits	G

The SIRO oversees the audit programme for the Trust. During 2017/18 the following IG-related audit reports were received:

IG Toolkit Self-Assessment	- Significant Assurance
GDPR Preparedness (Sep 2017)	- Limited Assurance
Cyber Security Governance	- Significant Assurance
Remote Access Follow-Up	- Significant Assurance

The new audit programme for the 2018/19 year has been agreed including:

Data Security Standards
Patient Safety
Governance
Risk management

CQC Inspection

Area	Risk	Response	RAG
CQC	Manage, maintain and implemented quality IG services to Trust and CQC expectations and targets.	No issues raised at this time.	G

The SIRO and CIO were key contacts for the CQC inspection of the Trust in July 2018. No significant IG-related issued were identified.

South Yorkshire SIRO Group

Area	Risk	Response	RAG
SIRO Group	Maintain regional SIRO engagement and discussion	SIRO attending regional meeting	G

The SIRO has attended the South Yorkshire SIRO group but the future of this meeting is currently under review.

Priorities for 2018/19

Area	Context	Response	RAG
Priorities	Maintain and implement agreed, statutory and mandatory IG commitments and continuous improvement programmes.	Raised as amber due to resource capacity and associated work required to deliver and additional responsibilities required for GDPR, DSPT & DPO. Risk should to be reduced through automation,	A

		increased trust wide responsibility and transfer of some tasks to other IG staff.	

- Review the Information Governance Framework to account for organisational and external change and guidance.
- Work to strengthen GDPR arrangements, awareness and processes.
- Implementation of a work programme to meet the requirements of the DSPT.
- Data and Cyber Security incident planning and testing
- Audit action
- Data Protection duties and support.

3. Next Steps

NA

4. Actions

This is the first iteration of this report, to note for assurance and information, acknowledging that it relates to 2017/18.

5. Monitoring Arrangements

Through Nicola Haywood-Alexander, CIO, Director of IMST and PMO, and David Hush, Head of Informatics and Information Systems.

6. Contact Details

John Wolstenholme, Data Protection Officer