Health and Social Care Information Centre

Board Meeting

Public Session

Title of Paper:	The Role of the Information Governance & Standards Assurance Directorate Post-IGAR
Board meeting date:	5 March 2014
Agenda Item No:	HSCIC 13 14 04 (b)
Paper presented by:	Rob Shaw, Director of Operations and Technical Services
Paper prepared by:	Christina Munns, IG Policy Manager
Paper approved by (Sponsor Director)	Richard Wild, Director of Information Governance and Standards Assurance
Purpose of the paper:	To: a. Articulate some of the key issues encountered by the Information Governance and Standards Assurance (IGSA) function and b. Propose the role of the internal IGSA Directorate post–IGAR (Informatics Governance Assurance Review).
Patient/Public Interest:	Proposes a way to openly and transparently manage and assure the decisions of HSCIC on information governance, confidentiality and data protection issues.
Actions required by the Board:	Endorsement of the approach

The Role of the Information Governance & Standards Assurance Directorate Post-IGAR

Rob Shaw

25 February 2014

Contents

Introduction

Purpose & Summary

1. A briefing from the Director of Operations and Technical Services to:

    c. articulate some of the key issues encountered by the Information Governance and Standards Assurance (IGSA) function and

    d. propose the role of the internal IGSA Directorate post–IGAR (Informatics Governance Assurance Review).

2. This briefing emphasises the role of incident management (including near misses), audit, independent assurance and customer feedback as both preventative and corrective, stressing the importance of embedding lessons learnt into business as usual (BAU).

3. The proposed operating model mirrors the post-IGAR model for cross-organisational IG issues (Annex A) and aims to apply control and governance to the IGSA function, facilitate upwards reporting and gather intelligence for a root and branch review of IGSA.

Background

4. The IGAR reviewed existing arrangements relating to informatics programmes and made recommendations for change or improvement.

5. The recommendations have implications system-wide but also create a clear distinction between internal and external issues, with an accepted model for managing cross-organisational IG issues (see Annex A).

6. This proposition suggests how the internal IGSA Directorate should align itself to the IGAR findings and embed processes such as incident management, into the BAU framework.

The Issues

7. In adopting a model which fits with the IGAR findings, the IGSA Directorate aims to improve its structure, processes and performance by addressing the following issues:

i. ***Governance, escalation/reporting and incident management***: Need for a comprehensive governance structure with transparent decision making and escalation/reporting points, particularly for incident management, cyber threat management and complaints handling.

ii. ***Roles and responsibilities***: Need for clearly documented roles and responsibilities, particulary in realtion to risk ownership.

iii. ***Commissioned expert services***: Expert advice must be considered as a commissioned service for programmes within HSCIC to factor in at project set-up.

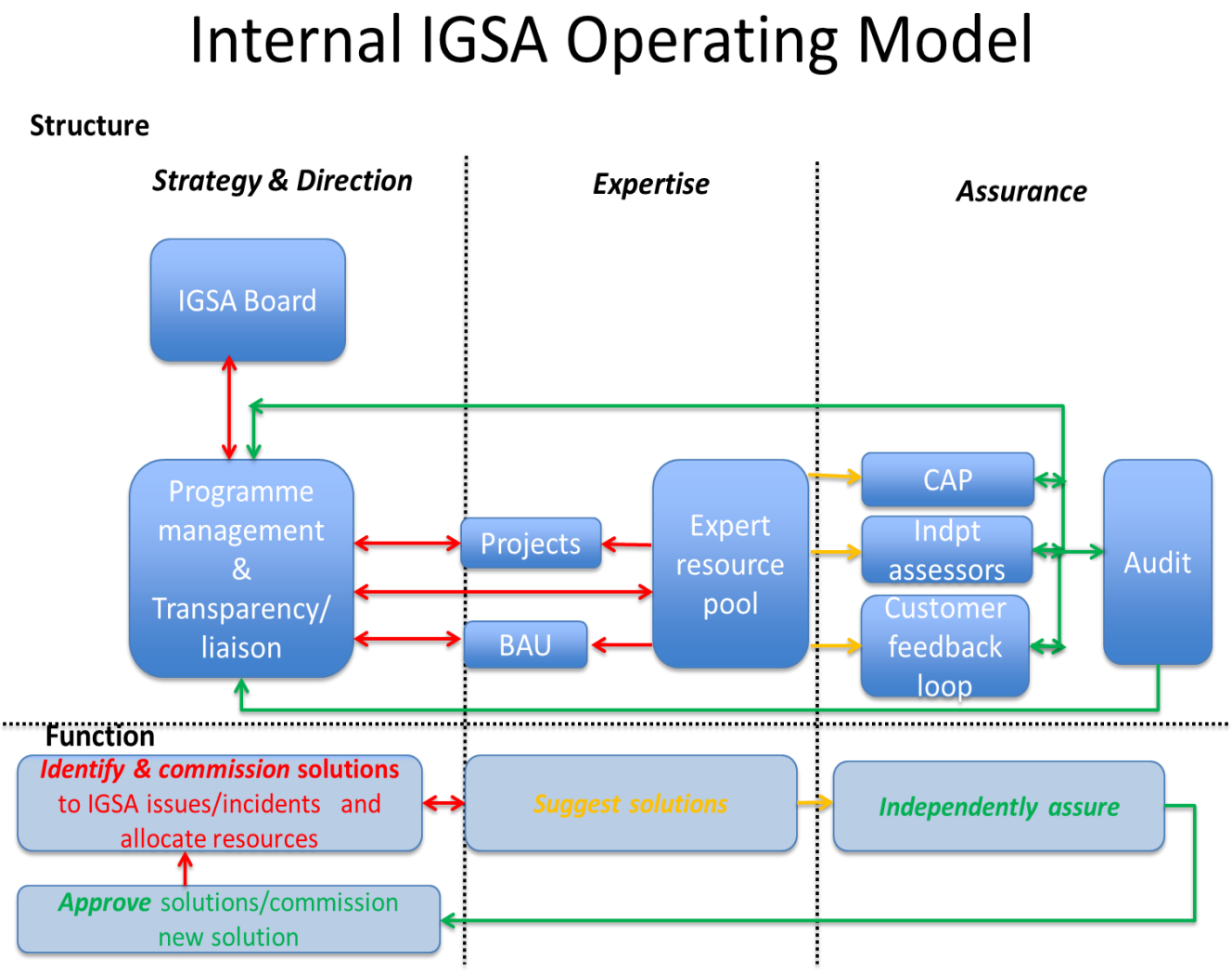
iv. ***Assurance***: Need for transparent solutions assurance and customer feedback mechanisms.

v. ***Transparency and swift data access***: The decision making process for access to data must be transparent and as timely as possible.

The Proposed Solution

The Operating Model

8. A scaled down “3 pillar model” (1. Strategy and direction, 2. Expertise and 3.Assurance) reflective of the IGAR model (see Annex A) is proposed. Each pillar will interface with its counterpart in the system-wide model as appropriate/necessary (e.g. as an escalation route).



N.B. CAP = The Common Assurance Process. A generic, end-to-end process for assuring the development and delivery of high quality and clinically-safe IT systems. This would be one assurance mechanism for expert advice commissioned by the programmes.

The Proposition

9. The table below summarises the proposed function and benefits of the work streams.

10. There is work underway on some elements of the proposition, including:
    a. **A cyber security programme** is now being implemented within HSCIC which includes proposals for active protective monitoring, independent assurance services and an improved governance model for cyber security management.
    b. **Incident management and reporting** will be managed centrally by the National Service Desk (NSD) from 1 April 2014. A security operations team will work closely with the NSD. The processes will mirror those already established for Service and Safety incidents, and will ensure consistency re. incident reporting, severity rating and escalation.
    c. **The IG Alliance Centre of Excellence (IGACE)** will be led by the HSCIC. Expert resources from across health and care will be drawn together to suggest answers for system-wide IG issues. Suggestions will be assured by a transparent, public-facing function and if agreed by the appropriate governance structure, published to establish a single point of truth. This group will be an accessible point of expertise for internal issues.

Workstream	Function	Key benefits/characteristics
Direction & Strategy - including interface with the system-wide operating model counterpart	IGSA Board	• ***Escalation*** and approval route, chaired by the SIRO (Senior Information Risk Owner). • Feeds into the cross-organisational IMB ***governance structure***.
	Programme/ portfolio management	• Matrix management of skills, maintaining the 'go to' expert list. • Develops SIAM (Service Integration and Management)-based offerings for ***commissioned expert advice*** embedded within delivery framework planning with agreed funding, ***roles, responsibility*** and ***risk ownership***. • Streamlines BAU based on customer feedback and analysis. • Overview of portfolio and risks and issues to report to SIRO • Business planning, budget planning and monitoring plan. • Sets ***reporting*** structure and receives progress updates.
	Transparency / liaison and 'front door'	• Fulfilling legal obligations (publishing info. flows etc), ensuring SLAs are set and managed for ***swift data access decisions***. • Primary interface (e.g. corporate governance, NSD, portfolio) • Stakeholder management and escalation to Board/SIRO. • Oversees complaints/incidents/process improvement/FAQs.
Expertise - including interface with the system-wide operating model counterpart	Projects	• Expertise used flexibly to develop outputs. Includes an interface with the system-wide **IGACE**, where necessary. • ***Large-scale cyber security initiatives***, gathering organisation-wide input, and smaller-scale projects establishing BAU.
	BAU (tools/ services)	• Reactive (e.g. ***incident management***) and • Proactive (e.g. ***cyber threat monitoring***). • Through a combination of the above and active management of the Key Performance Indicators (KPIs) for IG incidents it is expected that incidents would be minimised and reduced.
Assurance - including interface with the system-wide operating model counterpart	Customer feedback	• BAU solutions delivered directly, with a feedback loop to Direction and Strategy for continuous improvement.
	CAP	• Feeds into HSCIC-wide assurance process for IT programme advice, at the correct time of the product lifecycle.
	Independent assessors	• Standards and ***assurance*** of accreditation against standards (e.g. IGT) receive independent scrutiny.
	Audit	• Increased audit re. compliance of recipients of data.

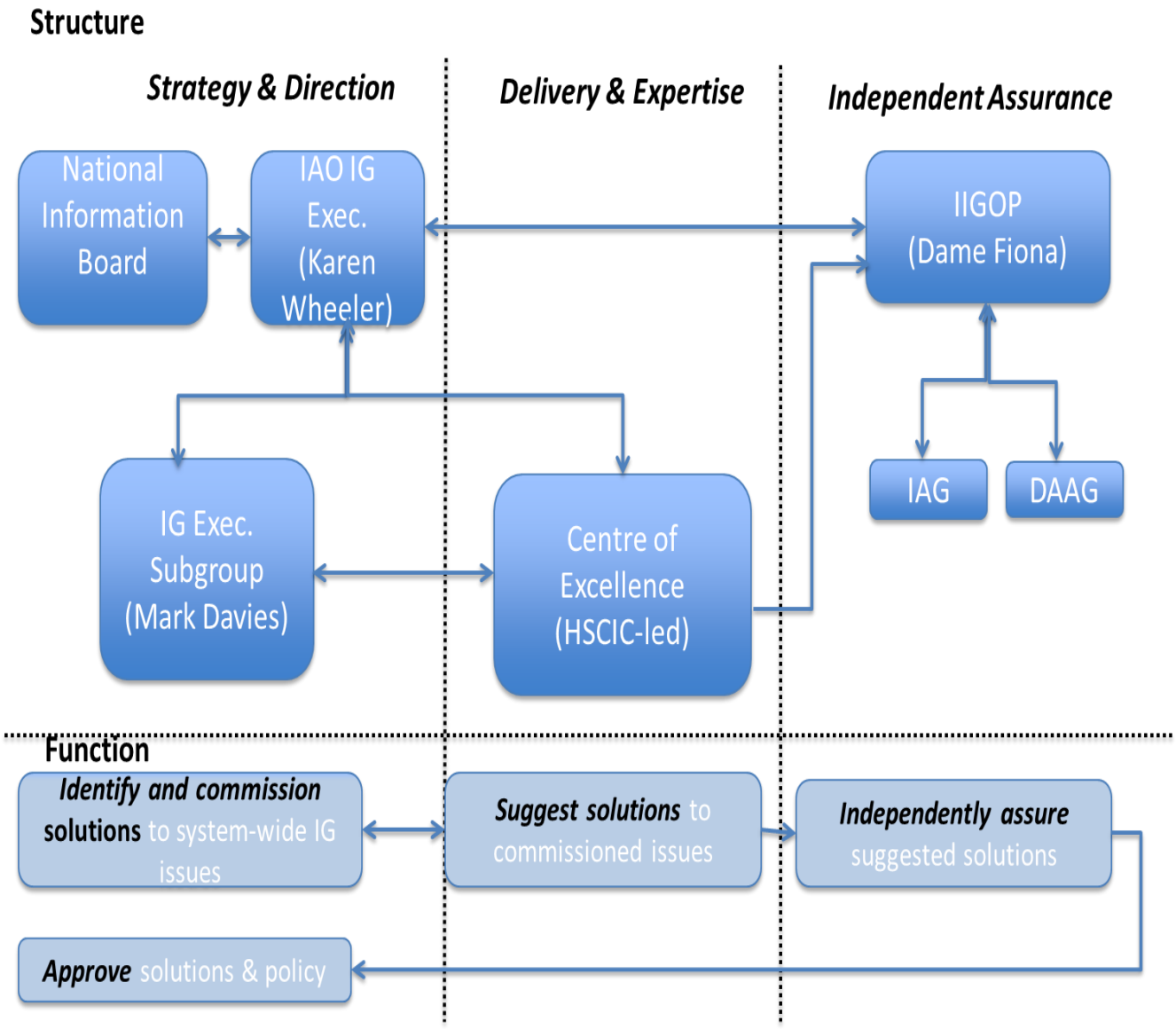
Next Steps

11. Resources are allocated to the Direction and Strategy work stream, so that detailed planning can commence.

Actions Required of The Board

12. For endorsement.

Annex A – External IG Operating Model Post – IGAR



N.B. IIGOP = Independent IG Oversight Panel

IAG = Independent Advisory Group

DAAG = Data Access Advisory Group