hscic Health & Social Care Information Centre

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:

    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).

2. This paper emphasises the role of incident management (including near misses), audit, independent assurance and customer feedback as both preventative and corrective, emphasising 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***: Lack of a robust governance structure with transparent decision making and escalation/reporting points, particularly incident management, cyber threat management and complaints handling.

ii. ***Roles & responsibility***: Duplication of effort both within and outside of the IGSA directorate, stemming from a lack of clear processes, roles and responsibilities. For example, there is a lack of clarity re. risk ownership between programmes and IGSA.

iii. ***Commissioned expert services***: Expert advice considered as an ‘add on’ or afterthought, rather than a commissioned service to factor in at project set-up.

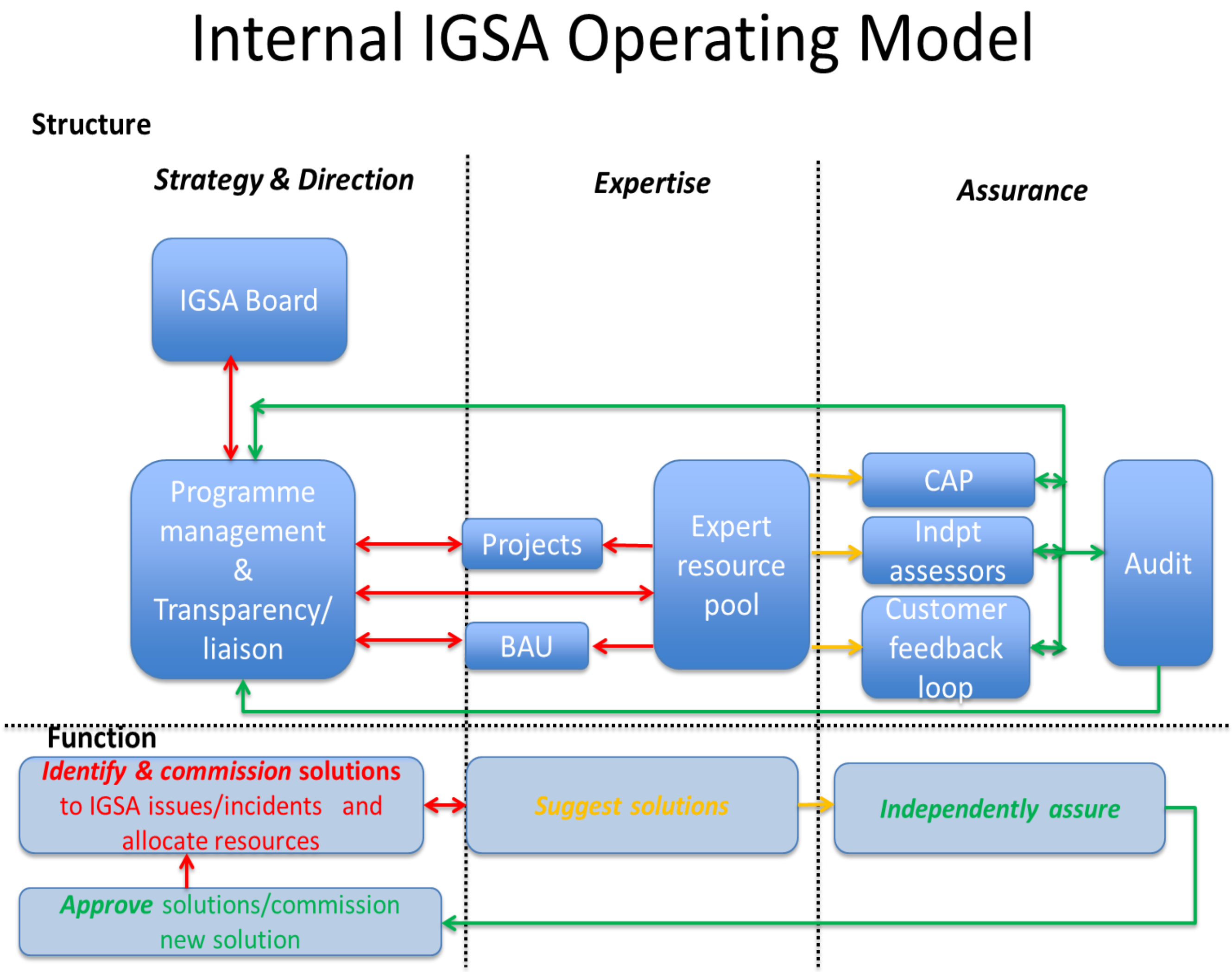
iv. ***Assurance*** : Lack of solutions assurance and customer feedback.

v. ***Transparency & swift data access***: The decision making process for access to data takes too long and customers are unaware of the process due to lack of transparency.

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).


Internal IGSA Operating Model
Structure
Strategy & Direction
Expertise
Assurance
IGSA Board
Programme management & Transparency/ liaison
Projects
BAU
Expert resource pool
CAP
Indpt assessors
Customer feedback loop
Audit
Function
Identify & commission solutions to IGSA issues/incidents and allocate resources
Suggest solutions
Independently assure
Approve solutions/commission new solution

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 & 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. **An IG Alliance Centre of Excellence** will be led by the HSCIC. Resources from across the health and social care system will be drawn to together to suggest an answer for system-wide IG issues. This will be independently assured and when agreed by the appropriate governance structure will be published to establish a single point of truth. They will provide an escalation route for internal issues.

Workstream	Function	Key benefits/characteristics
Direction & Strategy - including interface with the system-wide operating model counterpart	IGSA Board	• ***Escalation*** and sign-off route, chaired by SIRO. • Feeds into IMB ***governance structure***, as the interface with the external operating model.
	Programme/ portfolio management	• Matrix management of skills, maintaining 'go to' list for experts. • Develops SIAM based offerings for ***commissioned expert advice*** embedded in delivery framework planning with agreed funding, ***roles and responsibility*** and ***risk ownership***. • Streamlines BAU based on customer feedback and analysis. • Overview of portfolio and risks & 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**. • 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 and skills used flexibly to develop outputs. This will include an interface with the **Information Governance Alliance Centre of Excellence**, where necessary (part of the external structure for system-wide issues). • Projects include **large-scale cyber security initiatives**, gathering organisation-wide input, as well as smaller projects establishing BAU e.g. automating tasks etc.
	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 programme 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.

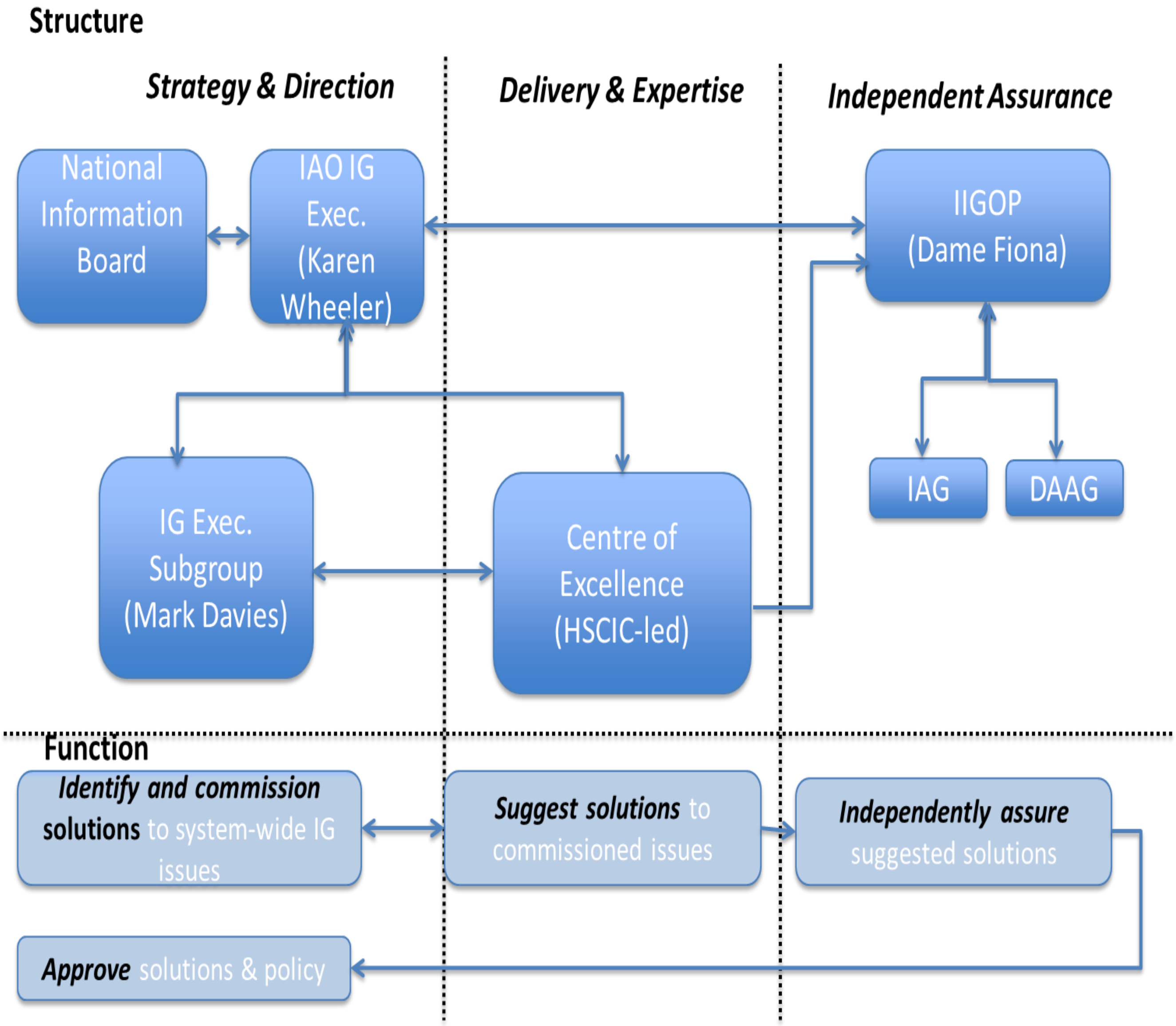
Next Steps

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


Structure
Strategy & Direction
Delivery & Expertise
Independent Assurance
National Information Board
IAO IG Exec. (Karen Wheeler)
IIGOP (Dame Fiona)
IAG
DAAG
IG Exec. Subgroup (Mark Davies)
Centre of Excellence (HSCIC-led)
Function
Identify and commission solutions to system-wide IG issues
Suggest solutions to commissioned issues
Independently assure suggested solutions
Approve solutions & policy