

The group may have moved beyond its original role. Of the key original areas where it focused all except C&M have moved on significantly.

JH's role is to deliver the piece of plastic – group's role is more about assuring the whole value proposition is delivered. Tricky, as NIS business case lacks some key elements. But a Q for JH – is the card a 'step 1' in a larger delivery plan? If so, then this may slot into the group's vision of their role – and this view is supported by recent strengthening of IH's team. But unsure whether to go as far as saying JH is lined up with DN on x-Gov't IDM delivery.

The group suggested JH had three things to do: (A) Deliver the card, (B) encourage card use across Gov't, and (C) deliver benefits proposition for customers and service partners – there's some catching up to do on (B) and (C).

What's the group for?

1. Where does group sit? Common view was that it should be "at the top of the tree" of assurance functions, above assurance functions in programmes, taking a 'big picture' view. It should ensure assurance is done – currently lots of assurance happens in silos, but no one makes sure it's all joined up and that no holes are left.
2. It should report – in the future more proactively and in a timely way, through its minutes.
3. It should be JH's "voice of conscience"
4. It should sit at an overview level in terms of x-Gov't IDM and NIS (note that this is at odds with SM's paper). There ought to be nothing JH is responsible for outside group's remit.
5. It should address hard issues which aren't owned elsewhere – e.g.:
 - a. Where are we in terms of programmes' time/ cost/ performance trade-off?
 - b. How are we striking a balance between data governance and privacy/public acceptance?
 - c. What are the inter departmental conflicts?
 - d. To whom are we delivering and why?
 - e. Will the public/media accept this scheme?
 - f. We can control the security of the technology, but with so many players and interests, can we achieve this?
 - g. Will it be sidelined by commercial developments?

JH's view was that

1. We have "reached the end of the beginning" – this is where things can go wrong – and we are moving into a more formally regulated place, with the Commissioner, etc.
2. The HS has agreed that public panels are the future for oversight and reporting, but that these are limited and will need expert advice and so will be supported by experts (with the risk that these experts will bring their own agendas).

3. These panels will take on much of the current BAG/ISAP role and the process for recruiting panels and experts is being finalised.
4. So, what do we do with the group? Three options:
 - a. Members transition to experts group
 - b. Group remains as a private advice group for JH
 - c. Disband, after suitable time (e.g. end of '09)
5. Lots of uncertainties (political and otherwise) ahead – and complicated by the progress of 2ndary leg.
6. On (B), above, the x-Gov initiative “Safeguarding Identity” (ACTION: distribute) is ready for publication after a long process of agreeing consensus. This agrees common processes for IDM and a single sign-on through Gov GW. It’s important that it separates NIS from the general problems of managing identity.
7. Individual members have given excellent assistance – e.g. XX helping IH. In the future more help along the lines of the ‘deep dives’ is likely to be needed. A distinct group of people with a public reporting role is probably not what we need – rather we need a ‘Rolodex’ of talent to call on.
8. If asked whether we’re disbanding the group before it’s had a chance to face the real hard problems, we’d say we’re transitioning to new assurance arrangements and taking on the Commissioner – who will be served by the new experts group.
9. Four key things stand out from list of groups priorities:
 - a. Integration,
 - b. Establishment of the Commissioner (who the group ought to brief, re their journey), the expert group and the panels,
 - c. The Target Operating Model
 - d. The counter-fraud arrangements
 - e. And also (suggested by AH), “Safeguarding Identity” (ACTION: ask for update to group on this)
10. GW reviews, Panels and Expert groups won’t be able to do certain types of advice/assurance – e.g. fix a broken contract – and won’t be able to do ‘deep dives’, etc.
11. Experts group will support Public Panels and feedback will go to the HS
12. Alongside other changes, there will be a refresh of the NEDs on the board
13. There is a need for some assurance to maintain objectivity, relevance and currency (this is at the opposite end of the spectrum to GW reviewers)

So, JH and group are concerned with the delivery and assurance of delivery of infrastructure, but are hampered by the lack of market/clients for services and benefits which causes inadequate information to feed back into the design. Neither the experts supporting panels or the NEDs are a substitute for the current group role. The group has

not had time to assess IPS's 'execution' capability – although note CWIC. Lots of faith is being placed in Commissioner's abilities. JH does not appear to believe he needs the group – so group should put on record that they think something's missing in his thesis that isn't met by the new arrangements.

So there are some things the group would like to feed back:

1. The requirements are not properly informing the design work because of slow benefits realisation
2. There's an omission in JH's approach – public panels etc. are good, but not a substitute for impartial advice to SRO
3. x-Gov't IDM is good too, but this doesn't have assurance either
4. Lack of alignment between comms and market, ID services and cardholders
5. Continuity (i.e. using the group) is needed between this year and next
6. We suggest enhancing internal assurance, not relying on consultants "marking their own or each others' homework"
7. IPS and x-Gov't IDM need strong NEDs
8. The SMB, MB and IDSG need to be better defined and differentiated
9. Whilst there are new senior execs and new civil servants, IT delivery hasn't been problem-free recently – there's still a way to go.
10. Lessons on assurance arrangements to be learnt from DWP? In any case, clear internal assurance structures are needed.
11. Service Delivery needs to be better able to manage change