Report on Architectural Risk 2012 - Summary

12/3/2012

Introduction

1. The 2011 Corporate Technology Risk identified our solution architecture as being one of the contributors to the High risk rating. In recent years a strong focus on delivery has resulted in an under investment in architecture. This will eventually have an impact on our ability to deliver.

2. The December board meeting were concerned that investment decisions being made in the 2012/13 portfolio build could be non-optimal if architecture considerations were not taken into account and asked the following question:

   "Given our changes in mission and changes in the external environment (Cyber defence, offensive cyber, increased partnering, increased data volumes, etc) which parts of our architecture are under most strain and so carry the most risk to this year's investment "

3. Part of the new DCTO role is to define a technology vision and then champion improvements to the solution architecture at portfolio build time. However, it will take time to construct that vision. Therefore in the interim a broad brush approach has been taken in order to allow some immediate advice to be given to the portfolio.

4. We have a defined a number of high level change drivers on the architecture (Annex 1). These are changes in either our mission, ways of doing business or external technology which are relatively recent and were not taken into account when our current solution architecture was built. We have also represented our current solution architecture as a number of high level elements. We then assessed each change driver against the current solution architecture and identified those architectural elements most stressed by the drivers (Annex 3 and Annex 4).

5. This has been done in a short period of time with only limited amounts of effort. There are therefore a number of caveats that need to be made:

   - This is a broad brush, high level analysis.
   - Whilst we have consulted as widely as possible, we have inevitably not managed to consult everyone we would have liked to have involved
   - We have restricted ourselves to the infrastructure and application layers (and so not explicitly considered the business layer)
   - We are not attempting to define the "to-be" solution architecture. Instead we have concentrated on identifying risks with the current architecture

Recommendations

6. This high-level architectural analysis has highlighted parts of the solution architecture which needs immediate attention. There are currently line items in the unconstrained portfolio build which will help address the three main concerns. It is recommended that these line items are prioritised in the filter and twist phase.

    - Big Data. We need to develop an end-end big data strategy which covers expected data growth, tradecraft, QFD architecture, cloud architecture, Black Hole, the role of streaming analytics and the proposed new data centre. A series of experiments should be carried out between TA, TDB innovation, ICTR and SD to de-risk some of the possible solutions.
    - Integrated Analytics Framework. We need to converge to a small number of analytics frameworks for use across our multiple missions which support the rapid deployment of experimental analytics tools and provide the APIs required for fused analytics.
    - Security Services. We need to provide an end to end and cohesive uplift to the capabilities used to support assured information sharing within and across our enterprise boundaries, with support to the Information Assurance agenda, ensuring the appropriate accessibility, releasibility and traceability.
    - Vision and Strategy. The coherence we need in order to deliver against the drivers needs investment into the development of end to end technical vision and supporting technology strategies, supporting the business needs. The current "redness" in Annex 3 demonstrates that there are some fundamental changes required to the architecture. Whilst the first three recommendations will address some of the more urgent symptoms we need to also invest in addressing the underlying causes.

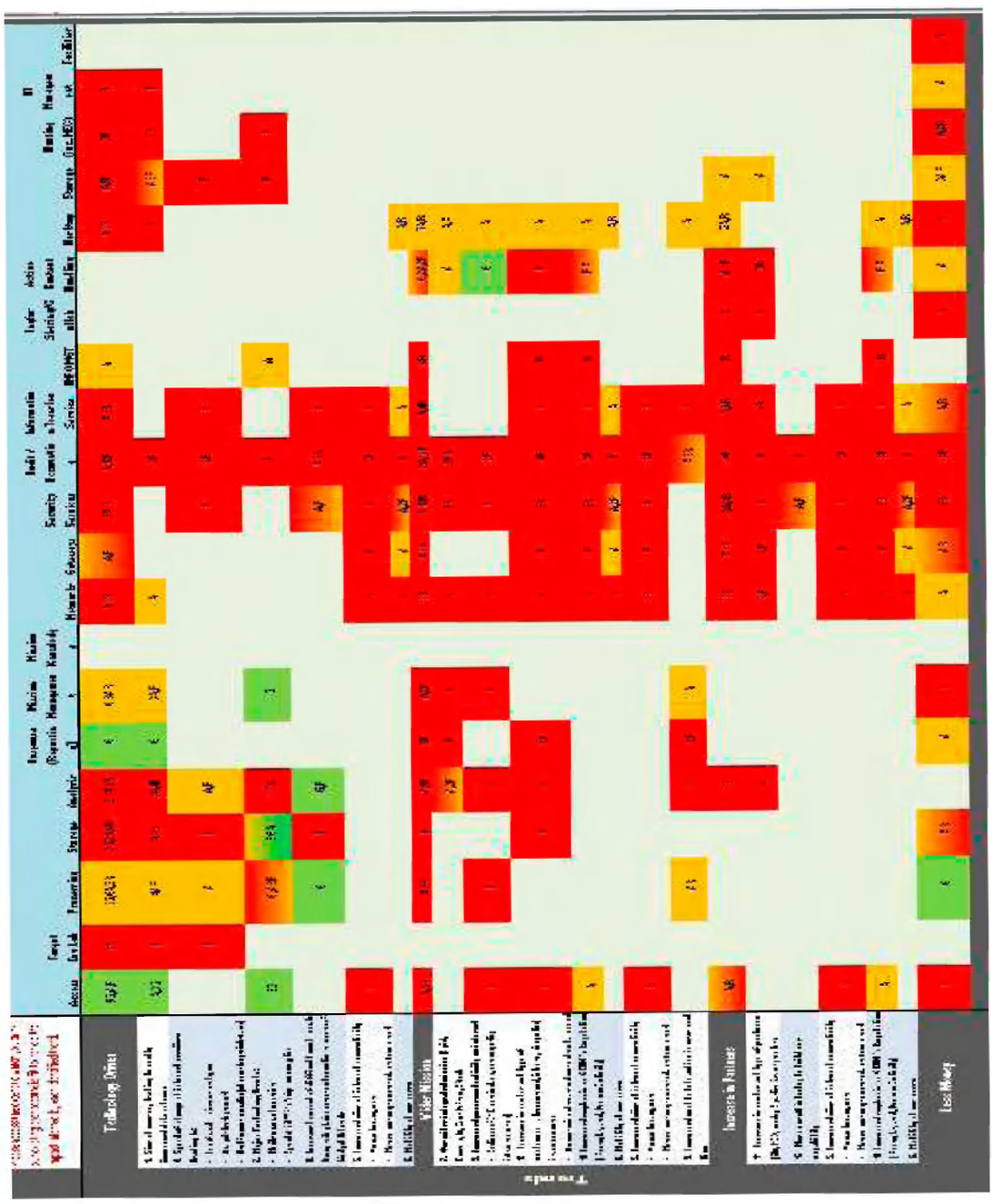
7. NSA are already some way down the path of instantiating their new architecture. Their "2017 Vision: the Future of NSA IT" has a small number of principles: smart data; virtualization and mobility. As we construct our equivalent vision we need, as a minimum, to be interoperable with NSA's new architecture. We should also look to take as much advantage as makes sense of NSA's specific implementations.

8. Finally, please note this report was created over a short period of time with only limited amounts of effort. There is a need to establish an appropriate framework that allows a more considered view to be presented as input to future portfolio builds.

Annex 1: Change Drivers

1. Size of access => vastly increased data volumes
2. Increase in number and type of customers (wider government, industry, third parties) i.e. our consumers
   - And more points where are customers interact with us (not just EP)
3. Increase in number and type of partners (SIA, MOD, industry, 3rd parties) i.e. our providers
4. NSA/US IT efficiencies
   - Rationalisation of systems
   - More integrated US intelligence community
5. Increased size of internet connectivity
   - One way, two way, covert
   - More reliance on open source obtained from internet
6. Increased presence/activity on internet
   - Scaling up of CNE (more implants, more supporting infrastructure etc)
7. Speed of change of internet services leading to:
   - Lots of capability in experiment space
   - Analyst task becomes harder
   - Analyst – developer model
   - More types of data
   - Need for more innovation (which needs open interfaces)
8. Our wider integrated mission (Sigint, Domestic, IA, Cyber Defence, Effects)
9. Increased need to take action in near real time
10. Increased emphasis on GCHQ's Reputation (IA exemplar, Legal, Business Continuity)
11. Major Technology trends:
    - Mobile broadband and devices
    - Spread of SSL/VPNs/ubiquitous encryption
12. Mobility of our users
13. Less money (Finite/shrinking resources)
    - To build systems
    - Support systems (power, space, cooling)
14. More use of industry to build our capability
15. Increased amount of difficult work (in scale & complexity) placing more demand on our limited numbers of highly skilled people
16. Volatility of target networks

Annex 3: Mapping of Drivers to Architecture Elements



Annex 4: Summary of RAG Status of each Architectural Element