INFORMATION SECURITY ARRANGEMENTS WITHIN THE CARE QUALITY COMMISSION

FOLLOW UP EXTERNAL REVIEW REPORT

FOR THE CHIEF EXECUTIVE OF THE CARE QUALITY COMMISSION

30 SEPTEMBER 2017

CONTENTS Page

This review was conducted by Chris Hurran during August and September 2017 with the helpful assistance of a number of members of CQC.

Executive Summary

The aim of this follow up external review is to report on the progress of implementation of the 6 recommendations of the 2016 review of information security arrangements within CQC.

The review was carried out by consulting CQC staff, reviewing CQC documentation, and by conducting a scenario exercise.

The review notes that CQC has delivered an impressive programme of work to make very significant progress in implementing the recommendations of the 2016 external review. It concludes that recommendations 2 (security and audit aspects of contracts with third party suppliers), 3 (exercise testing the crisis management plan), 4 (risk management of visitors) and 5 (supply chain risk management) have been fully met and require no further work. Recommendation 1 (information risk management in projects) was fully met but changed working arrangements mean that further work will now be needed. Finally, excellent progress has been made on recommendation 6 (culture change) which was always recognised to be the most challenging recommendation but there is more work to be done. Sound governance has underpinned the successful delivery of the whole programme of work.

This follow up external review makes four new recommendations. Two relate to the ongoing work on culture change, one relates to the changed arrangements for project management and one relates to continuing overall programme governance.

Introduction, Purpose and Terms of Reference

In July 2016 a serious data loss took place in the margins of CQC office refurbishment works in Newcastle. A subsequent external review was carried out in August 2016 to establish relevant facts and causative factors with regard to the data loss incident, to review the incident response, to examine relevant information security policies and procedures and to make recommendations. The completed review made 6 recommendations

At its Board Meeting of 22 September 2016, CQC accepted the review's findings and recommendations and the Board decided that there should be a further external review after 12 months to review the progress of implementation of the 6 recommendations.

The aim of this follow up external review is to report on the progress of implementation of the 6 recommendations of the 2016 review. The full terms of reference are attached at Annex A.

Methodology

Information to meet the requirement was obtained by:

- Reviewing internal CQC documentation (including those references listed at Annex C),
- Obtaining evidence from CQC staff (face to face and/or by telephone and/or by e-mail exchange). Those consulted are listed at Annex B.
- Conducting a scenario exercise in connection with 2016 Recommendation 2.

Overall Programme and its Governance

The Information Governance Policy Statement and associated Work Plan were reviewed together with the detailed Project Plan. They represent an impressive and well-focussed programme of work and the long term, medium term and short term objectives are all sound and appropriately ambitious. The review's only concerns relate to the deliverables on culture which, although all commendable in their own right, fall short of the ambition that CQC needs to achieve to deliver on 2016 Recommendation 6. This is addressed more fully below.

At the CQC Board Meeting of 22 September 2016 it was decided that the implementation of recommendations from the 2016 external review would be overseen by the Audit and Corporate Governance Committee (ACGC). ACGC first considered progress at its meeting on 25 January 2017. Detailed references to the progress to that date are included below against the relevant 2016 recommendations. The following is an extract from the minutes of that meeting:

> Following the data security breach involving the loss of DBS certificates in July 2016, an external review of the incident had been commissioned. The Committee noted the recommendations of the external review, alongside the actions carried out to complete them and an overview of the wider programme of work on security improvements as set out in the meeting report. Five out of the six recommendations had now been completed and work to complete the final one - a programme of security culture change so that CQC could become an exemplary information security organisation in the context of "Safe Data, Safe Care" – was scheduled. The Committee suggested that it would be helpful for internal audit to review progress in 2017/18.

ACGC reported accordingly to the Board on 22 February 2017. On 5 April 2017 ACGC approved the 2017/18 Internal Audit programme which includes a planned audit on "Data protection, EUGDPR and actions following loss of DBS records". ACGC will now continue oversight as part of their regular scrutiny of progress on the annual audit plan.

This review is satisfied that the overall programme of governance of the implementation of recommendations from the 2016 external review is currently appropriate. However, in view of the change in status of 2016 Recommendation 1 (project management - see below) since the 25 January 2017 ACGC meeting and the potential timeframe required to implement 2016 Recommendation 6 (security culture – see below), this review recommends that the monitoring of progress of this programme of work should remain a standing item in Internal Audit programmes for the foreseeable future and not just in 2017/18.

Recommendation 1: CQC should continue to monitor this programme of work through Internal Audit for the foreseeable future.

2016 Recommendation 1

"CQC should consider information risk to be by default an integral element of all projects which are subject to formal project management. If a decision is made by the SRO that the circumstances of a particular project makes information risk irrelevant then that decision should always be documented and endorsed by the SIRO."

On 25 January 2017 the Information Governance Working Group (IGWG) reported to the ACGC as follows:

> The Information Security and Governance Teams have worked with the CQC Design Authority (DA) to ensure that all projects are required to consider information risk. The teams are now represented at the DA meetings and have a complete list of all projects and any proposed changes to check that any information risk is being appropriately addressed. Decision gateways 0 and 2 at the DA for projects and changes are being used to provide triggers for risk and privacy assessments by project teams with assistance, where necessary, from the information security and governance teams. This will ensure that decisions made by the project teams can be reviewed and challenged as necessary.
>
> A final gateway check is provided at Investment Committee meetings via a requirement to confirm to the committee that any requests for capital or revenue funding have appropriately considered information risk, addressed that and had sign off from the information security and governance teams.
>
> Any projects or changes which require security exceptions will be flagged, discussed and brought to the attention of the SIRO for approval if required.

On the face of it, this 2016 Recommendation would appear to have been satisfactorily implemented. This review sought to confirm that fact by, for example, engaging with the CQC Design Authority (DA) but was informed that, following the appointment of a new Chief Digital Officer, the DA was "in

abeyance/on hold". There was anticipation that the roll out of a replacement process was likely to be "less formally structured" as part of introducing agile product development methodology but there was recognition that CQC "must not lose sight of this issue in the new process as it develops".

Whilst the review was clear that CQC has no deliberate intention to weaken information security governance of projects (both digital and those with no obvious digital component – such as the office refurbishment project that led to the DBS data loss of 2016), there remains a possibility (all too often seen in other public sector bodies) that security could slip in priority in comparison with other policy imperatives (efficiency, speed of working, driving down costs, etc) as memories of the DBS data loss fade. That could prove a costly error under GDPR. This review therefore recommends that these new processes, whatever they are, are closely scrutinised by IGWG as they develop. IGWG in turn should be monitored through the Information Governance Group (IGG), as well as the annual work programme of Internal Audit.

Recommendation 2: IGG should be required to approve information security aspects of new project management processes as they develop and Internal Audit should continue to monitor these developments as part of their annual programme of work.

2016 Recommendation 2

"Existing contracts with third party suppliers should be reviewed to ensure that they provide for the provision of audit information in real time for the purpose of managing incidents or investigating wrong doing. Future contracts should include this provision by default."

On 25 January 2017 the Information Governance Working Group (IGWG) reported to the ACGC as follows:

> We have worked closely with the CQC contracts and commercial team to address this recommendation. The CQC uses the Crown Commercial Services (CCS) framework wherever possible, and that framework contract includes comprehensive security clauses and refers suppliers to the need to comply with our internal security and governance policy. The content of the security clauses have been closely examined to ensure that they are appropriate and detail our right to audit and test contract delivery against them.
>
> We also use 2 separate internal framework contracts for engagement with suppliers in circumstances where the CCS template is not available or suitable. These framework contracts have also been examined and amended where necessary to also provide assurance that they contain appropriate information security and governance clauses.
>
> We have also carried out a review of all existing contracts with suppliers and given each contract a risk status based on the following criteria:
>
> - Red – The services provided under the contract necessitate one or more third party contractors having direct and authorised access to CQC data.

- Amber – The services provided under the contract do not give the third party contractor any authorised access to CQC data but the provision of the contracted services may put them in a position where they have access to CQC premises or locations where data is stored or processed.
- Green – The services or goods provided under the contract do not give any third party access to any CQC premises, data storage or processing areas.

All future contracts will be categorised using the above criteria and have the confirmed, comprehensive security clauses applied at the time of contracting.

Following on from this piece of work we will develop and carry out spot checks with our suppliers to confirm our right to audit and to test compliance with our contracted information security requirements. This will be conducted in conjunction with the contracts and commercial team in accordance with the contract management process.

The review scrutinised the models of contracts used by CQC (described above) and also the spreadsheet on which the risk status of existing contracts has been assessed. The process of assessment for existing contracts seems comprehensive and the categorisation appears sound. The review did not scrutinise individual contracts but the assessment of those categorised Red (25 at the time of the review) looked appropriate. The model contracts address security and audit in different ways which are appropriate for their use:

- CQC Long Form Contract: The relevant provisions in the Long Form (contained in clauses D5, E1, E2, E9 and Schedule 8) are very comprehensive and fully meet the requirements of this recommendation.
- CQC Short Form Contract: The security requirements in the Short Form are not as comprehensive as the Long Form because this contract is predominately use for low value/low risk services. References to different aspects of security appear in various sections but principally paragraphs 7 (staff vetting) and 13 (data protection). There is no specific reference to audit rights although there are relevant processes in place (eg paragraph 7.2.2 (provision of data about staff) and paragraph 10.2 (retention of and access to records)). In view of the use made of these contracts these provisions meet the requirements of this recommendation.
- Crown Commercial Services Framework Agreement and Call Off Contract: The relevant provisions in the Framework Agreement are contained in Section 7 and in clauses 14, 15, 17 and 20. As an example the review saw the Digital Outcomes and Specialists Framework Agreement and the relevant provisions are very comprehensive and fully meet the requirements of this recommendation. More generally, CQC as a buyer would also be able to request that a supplier complies with its own security policy and incorporate such a requirement into the Order Form.

Consideration was given to the review "dip testing" selected contracts in order to scrutinise them in depth to ensure that they fully met the requirements of this recommendation in practice. After discussion it was agreed that a more useful means of verifying this would be by the use of a scenario

exercise. The exercise used was a data leak scenario exercise in connection with CQC Supply Chain Contracts. Responses required access to a wide range of data from a range of suppliers. Overall the responses were highly satisfactory with regard to obtaining audit logs and billing data from suppliers and access control and CCTV coverage from office facilities providers. Other difficulties exposed by the exercise are very typical of most public sector organisations and not specifically relevant to this recommendation. CQC IGG may wish to reflect on wider issues raised by this exercise in due course.

Overall the review is of the opinion that CQC has responded in full to this recommendation and therefore makes no further recommendations in this respect.

2016 Recommendation 3

"Once the new Crisis Management Plan has been formally approved it should be exercised (perhaps with a complex data loss incident scenario involving electronic data)."

On 25 January 2017 the Information Governance Working Group (IGWG) reported to the ACGC as follows:

> We agreed with CQCs business continuity management team for the schedule of testing to include a data loss scenario as one of the first tests to be carried out this year.
>
> That initial test was carried out on 8th November 2016 to exercise the scenario with the Executive Team. Follow up exercises are planned to expand on the Crisis Management Plan and to develop associated processes, procedures and actions. As an initial step, emergency planning cards are being issued to all staff along with information relating to the CQC reaction in the event of an incident or emergency.

The review saw the report from the 9 May 2017 Executive Team Gold Command Exercise and the scenario (cyber-attack) and report from the 15 August 2017 Executive Team Gold Command Exercise. Both reports showed that incident response processes in CQC are fundamentally sound.

The review is of the opinion that CQC has responded in full to this recommendation and therefore makes no further recommendations in this respect.

2016 Recommendations 4 and 5

"The IGG risk register Risk 25 mitigating actions should be expanded to include the normal requirement for non-CQC visitors to CQC premises to be appropriately supervised."

"The IGG risk register should have an additional risk fully addressing information security risks in the CQC supply chain. "

On 25 January 2017 the Information Governance Working Group (IGWG) reported to the ACGC as follows (in respect of 4):

We have amended this risk and are confirming with the estates and facilities team that all visitors and contractors to be appropriately escorted whilst in CQC offices.

The action to update the risk register has been completed. Follow on actions with the estates and facilities team are to be carried out to confirm that procedures are being adhered to. We are also carrying out spot checks of visitor logs and procedures in conjunction with our regular office security reviews.

and (in respect of 5):

We have included a new risk in the IGG risk register covering contract and supply chain management. This action is being followed up further, in conjunction with the work carried out to address recommendation 2 above, to ensure that the information risks in the CQC supply chain are being comprehensively addressed.

The review scrutinised the Information Risk Register and noted that not only had these two recommendations been acted on but there have also been a number of risks added to the register since the 2016 review. This risk register is now extremely comprehensive.

The review is of the opinion that CQC has responded in full to these recommendations and therefore makes no further recommendations in this respect.

2016 Recommendation 6

"CQC should embark on a programme of security culture change so that they can become an exemplary information security organisation in the context of "Safe Data, Safe Care"."

On 25 January 2017 the Information Governance Working Group (IGWG) reported to the ACGC as follows:

This action is acknowledged within the report as being the most challenging recommendation to address.

A project team has been established, chaired by the Head of Stakeholder Resolution, Rights and Reviews and reporting into the IG Group, to address a range of security and governance work items. The IG Group and this wider programme of work are chaired by the Executive Director of Strategy and Intelligence and CQC SIRO. A range of work streams are included in the wider information security and governance project which is due to be implemented throughout 2017 with a number of items due for completion by 1st April 2017, the remainder are scheduled to be completed during the rest of the calendar year. Initial work on this project is progressing well through engagement with the Academy team to implement new, tailored training packages for all staff groups, which will be delivered via ED.

The project is also working with the Engagement Team to deliver a programme of clear communications to all staff, highlighting the need to consider security as an integral part of all work that we carry out. The emphasis of the programme will be that security matters are part of 'everyone's responsibilities', it has been agreed that the communications programme will be branded as 'CQC Values Information'. The engagement team is working on producing a detailed plan to commence in 2017which will include messages to all staff via the intranet, tailored emails and Lync sessions where they will receive short briefings and have the opportunity to address any related concerns they may have.

We are also collaborating with other organisations to identify good practice and effective ways to engage staff as part of wider work taking place with the DH, NHS Digital and NHS Improvement to implement new data security standards throughout Health and Social Care.

This programme of work is being jointly supported by the Information Security, Information Rights and Knowledge and Information Management teams, overseen and assisted by the Information Governance Group. It is the subject of the wider information security and governance work plan which has already commenced and is scheduled for completion by the end of 2017/18.

The review was impressed by the very significant effort committed to addressing this recommendation. The review accessed a number of relevant documents but in particular the culture-related strands of the Information Governance Work Plan, the detailed Project Plan and the IGWG Dashboard and Roadmap. From these documents and others it is clear that the ambition to become an exemplary information security organisation is very strong and that CQC is investing significantly to achieve that.

The highlight of the work carried out in the last year was "CQC Values Information" month in April 2017. The infographic and reach data attached at Annex D illustrate the imaginative range of activities undertaken but also highlight the patchy take up by CQC employees. The review saw many of the materials used and also the presentation given in advance to the Strategic Leadership Team on 15 March 2017, as well as the results of the staff survey carried out subsequently (180 respondents from a headcount of approximately 3200 employees).

The review is aware from the plan that this is ongoing work and in particular that there is recognition across CQC that this is a change programme that will go on for ever. The review is also aware that CQC has some unique advantages in delivering this change (eg the strong existing culture of information and records management and the network of KIM champions) and some very challenging disadvantages (eg roughly two thirds of employees work from home and a complicated mix of paper and digital records). At this point of the implementation of this recommendation, the review believes that CQC needs to take two important steps to control this programme of work – defining what success looks like and measuring progress towards it. In more detail:

- Defining success: The 2016 review was careful not to define what "an exemplary information security culture" would look like for CQC. It is always best for organisations to

try to answer this question themselves, albeit with help if needed. But it is fundamental that the Board should own this definition. The definition may be expressed in terms appropriate to the organisation but some public sector and national infrastructure organisations choose to do so across the following 8 dimensions of security culture (further details are attached at Annex E):

- Results or process orientated
- Innovative or cautious
- Information sharing or information restricting
- Collective or individualistic
- Deadline orientated or detail conscious
- Indirect or direct control
- Questioning or accepting
- Participative or authoritative

Of course other definitions are available. But what is important is that the CQC Board should own whatever definition they choose. At present there is no evidence that this is the case.

- Measuring progress towards success: Despite the unique difficulty of its distributed workforce, the CQC Board needs aggregated metrics in order to see what progress is being made towards the achievement of the desired security culture through the actual behaviours of employees throughout the organisation. The current programme has no process in place to achieve this. Whilst recognising that this is never easy, the review noted that CQC already has at least one mechanism which might be adjusted in order to harvest this data – the "CQC values" objective in the appraisal system. Included in those values presumably is information security. The IGWG could easily furnish reporting officers at all levels with appropriate language to use when completing appraisals. Not only would this raise awareness of this vital work across the whole of CQC but it would also provide the board with the metrics it needs. Of course other methods of measuring progress are available but it is important that the CQC Board should decide what they will use.

In summary, although the review is impressed with the progress made to date on this recommendation, it makes 2 recommendations in order to take better control of the information security culture change programme and its outcomes:

Recommendation 3: The CQC Board should define its desired information security culture.

Recommendation 4: CQC should put in place procedures to obtain metrics in order to monitor progress towards the desired information security culture.

Conclusions and Recommendations

CQC has delivered an impressive programme of work to implement the recommendations of the 2016 external review of information security arrangements. Four of the recommendations have been fully met and require no further work. One was fully met but changed working arrangements mean that further work will be needed. Finally, excellent progress has been made on the culture change recommendation which was always recognised to be the most challenging. Sound governance has underpinned the successful delivery of the whole programme of work.

This follow up external review makes four new recommendations summarised below:

Recommendation 1: CQC should continue to monitor this programme of work through Internal Audit for the foreseeable future.

Recommendation 2: IGG should be required to approve information security aspects of new project management processes as they develop and Internal Audit should continue to monitor these developments as part of their annual programme of work.

Recommendation 3: The CQC Board should define its desired information security culture.

Recommendation 4: CQC should put in place procedures to obtain metrics in order to monitor progress towards the desired information security culture.

Annex A

Review Terms of Reference

Terms of Reference for the follow up external review of information security arrangements within CQC.

1st August 2017

Background

Following a serious data security incident reported internally on 11th July 2016, the Chief Executive requested that an independent, external review of CQC security and data handling arrangements is carried out. That review was completed during August 2016 with a report and associated recommendations presented to the Executive team. It was requested that a follow up review take place during summer 2017 to check on the implementation of the recommendations.

This follow up review has been scheduled for 15th August to 30th September and has been commissioned by the Director of Governance and Legal Services on behalf of the Chief Executive, SIRO and Director of Customer and Corporate Services.

Incident Recap

A major programme of works to refurbish CQC offices in Newcastle and Leeds was carried out between 31st May and 24th July 2016. One phase of the refit to the office in Newcastle was carried out on 8th and 9th July. During that phase 4 lever arch files were lost, these files contained sensitive Disclosure and Barring Service (DBS) information relating to 500 individuals.

A significant amount of follow up work was carried out to investigate; report on and mitigate the loss of this information. That work concluded with an independent, external review of security arrangements in place at CQC both directly linked to this incident and more widely to the organisation wide security and governance controls.

Description of the review

The follow up review is intended to focus on the recommendations made as a result of the initial review in 2016, those recommendations are:

Recommendation 1: CQC should consider information risk to be by default an integral element of all projects which are subject to formal project management. If a decision is made by the SRO that the circumstances of a particular project makes information risk irrelevant then that decision should always be documented and endorsed by the SIRO.

Recommendation 2: Existing contracts with third party suppliers should be reviewed to ensure that they provide for the provision of audit information in real time for the

purpose of managing incidents or investigating wrong doing. Future contracts should include this provision by default.

Recommendation 3: Once the new Crisis Management Plan has been formally approved it should be exercised (perhaps with a complex data loss incident scenario involving electronic data).

Recommendation 4: The IGG risk register Risk 25 mitigating actions should be expanded to include the normal requirement for non-CQC visitors to CQC premises to be appropriately supervised.

Recommendation 5: The IGG risk register should have an additional risk fully addressing information security risks in the CQC supply chain.

Recommendation 6: CQC should embark on a programme of security culture change so that they can become an exemplary information security organisation in the context of "Safe Data, Safe Care".

The intention is to check that these recommendations have been implemented as fully as possible, the effectiveness of that implementation and to advise on whether or not there are other actions which CQC could carry out to further improve information security and governance arrangements.

The following elements should therefore be delivered within the scope of this review:

- A review of the IG and Security work plan which has been implemented as a result of the initial review and associated recommendations,
- Consideration of the effectiveness of the CQC wide engagement work which has been carried out and the extent to which this has enhanced the security culture across the organisation.
- Providing expert insight and guidance as to any further work items which CQC may be able to implement to further improve IG and Security arrangements.
- The production of a report which addresses the issues outlined above which can be shared with those impacted by the loss of data, stakeholders and the wider public as necessary.

The Commission will:

- Provide a contact person with whom an external reviewer can liaise and who can provide necessary assistance.

- Ensure that the reviewer is provided with all necessary information to allow them to complete their review.

- Provide names and contact details of all parties identified as being part of the review.

- Ensure that those people in the direct employ of the Commission are available for interview as part of the review and are appropriately aware of the nature and scope of the enquiry.

Timescales:

The commencement date of this investigation is the 15th August 2017. The reviewer should aim to complete this review and deliver a report to the Director of Governance and Legal Services on the areas identified by 30th September 2017.

A further piece of work may be carried out following the primary review, this will be dependent on the findings of the review. It may consider a more detailed examination of one or more particular aspects of any areas identified which merit closer investigation. This further piece of work, if carried out, will be completed within the existing, authorised funding envelope and will be reported on separately by no later than 30th October.

Should it become apparent that there is good reason to extend these timescales; the reviewer should communicate this to the Director of Governance and Legal Services.

Signed: ……. Date:……..

Annex B

CQC Staff providing evidence to the Review

Malte Gerhold

Martin Harrison

Ayo Owusuh

Simon Richardson

Brian Silk

Natalie Treadgold

Derek Wilkinson

Annex C

References:

1. 2016-10-03 INFORMATION GOVERNANCE WORK v1
2. 20170822 IG Project Plan v1
3. 20170125 ACGC - DBS Incident Actions Update (CH Review)
4. ACG041701 - Item 2 - Minutes ACG 25 January 2017 FINAL DBS extract
5. CM021709 Item 9 ACGC Report to the public Board
6. Copy of 20161115 Live Contracts (CH Review)
7. 2016-12-14 Contract for the Provision of Services Nov 2016 Final Clean
8. 2015-12-02 Short Form Contract (Services) Dec 2015 Final clean version
9. 2017-8-25 DOS 2 Framework Agreement
10. 2017-8-25 digital-outcomes-and-specialists-2-call-off-contract (1)
11. 20170516 Gold exercise de-brief (CH Review)
12. 20170801 Cyber Attack draftv5 Y Drive Edit FINAL
13. 20170821 Gold exercise de-brief points
14. Information Risk Register MASTER COPY
15. 20170615 - IGG Paper 2 - IG working group Dashboard and roadmap
16. 20170502 IG CQC Values Information Engagement plan v2.5
17. 2017-6-30 - CQC Values Information month engagement case study
18. 2017-3-15 CQC Values Information SLT presentation v2 DRAFT
19. Value Information Employee Survey
20. 20150611 Information Security Matters Jun 15
21. 20160415 Information Security Matters April 2016
22. 20161020 Information Security Matters November 2016
23. 20170401 All Staff Lync Session
24. 20170626 Cheshire and Wirral Briefing Pack (CH Review)
25. April is CQC Values Information Month
26. ICO to DC - letter dated 23 02 17
27. IG Project Group Meeting Agenda 20170411 V1
28. IG Project Group Meeting Agenda
29. Intranet Articles - CQC Values Information
30. The tables have turned on us
31. 2017-7-6 Management assurance definitions Final drafts
32. 2017-6-7 ET paper Management assurance review

Annex D: CQC Values Information month (April 2017)

Objectives

- To ensure all staff are aware of the importance of effective information governance and security, and their role within in
- To deliver a compelling narrative that explains the link between good information governance and security, CQC's purpose and our Strategy 2016-21, and how it relates to the individual's role and of their team
- To drive an improved culture in CQC around information governance and security so that it becomes a natural part of people's way of working.

Activities

27 March	'Next month is CQC values information month' teaser banner
31 March	David Behan weekly message (and exec directors)
3 April	'Launch' intranet news story
3 April	Start of Yammer conversation: What's the most valuable thing you've lost?
6-28 April	Three all-staff Skype sessions on various topics
20 April	Mid-campaign refresh, using Intranet news story: Video 'What's the most valuable thing you've lost?' and 'quick pack' for use at team meetings
27 April	Launch of survey on information security
2 May	Summary of the month and suggestion to continue

Quantitative data

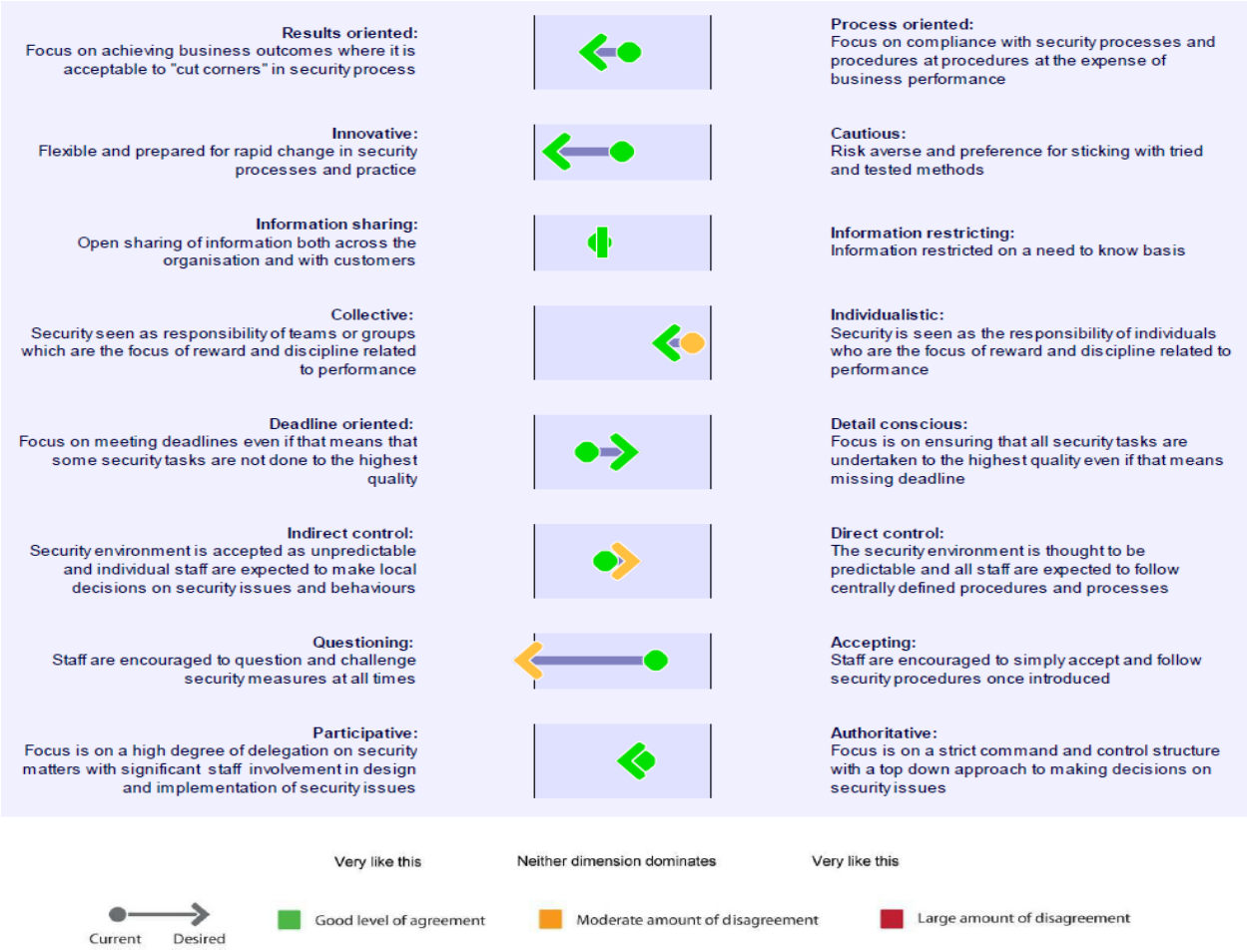
News story to launch the month	888 hits
Refresher 'new activities' news story	410 hits
Team 'quick pack'	112 hits
Facilitators' prompts	94 hits
Video views	62
Code of practice call	Not available
Information security call	51 participants
KIM call	38 participants
Yammer conversation	17 participants
Survey responses	100 (as of 22 May)

Observations / insight gained

- Although the news story received a healthy number of hits, the resources and activities were not taken up in large numbers e.g. <2% of staff joined the most popular Skype call
- The right sort of question Yammer elicited some powerful personal disclosure / emotional content. Empathic conversations were held and there were many 'likes'. However, there seem to have been a tiny number of people involved
- The survey response was particularly disappointing, as it was given a push more than once
- The Skype calls seemed to lend themselves to clarification discussions or practical / problem-solving transactions. Therefore, demonstrates use for collaboration. But also note that presentations were mainly providing information.

Annex E

Dimensions of Security Culture



(Example copied from CPNI SeCURE tool Senior Stakeholder Survey)