Response to recommendations in the Trilateral report on PIAs

Recommendation	Response
1. We recommend that the ICO develop measures aimed at promoting a closer fit between PIA and risk- and project-management methodologies through direct contact with leading industry, trade, and other organisations in both the public and private sectors.	The ICO will develop an action plan to develop closer links with organisations which lead on specific project and risk management methodologies. We will look at how the externally-facing teams at the ICO can promote the use of PIAs. In particular we will include PIAs as part of the scope of an audit.
2. We recommend that, in revising its PIA Handbook, the ICO make the third edition much shorter, more streamlined, and more tailored to different organisational needs. It should be principles-based and focused on the PIA process. The ICO should undertake a consultation on a draft of a revised guidance document.	The ICO is producing a revised version of the handbook – which will be a PIA code of practice – and will publish a consultation draft in summer 2013.
3. We recommend that the ICO's guidance on PIA emphasise the benefits to business and public-sector organisations in terms of public trust and confidence, and in terms of the improvement of internal privacy risk-management procedures and organisational structures.	We agree that these are important elements of the PIA process, and will include this in the revised guidance.

Recommendation	Response
4. We recommend that ICO guidance help organisations to understand and evaluate privacy risk, whether or not they can integrate PIA into their risk-management routines and methodologies.	The ICO advocates a risk based approach to data protection, and this is reflected in its guidance and approach to regulation. For example, the Anonymisation code of practice focuses on understanding privacy risks in that context. We will continue this approach in our work.
5. We recommend that the ICO develop a set of benchmarks that organisations could use to test how well they are following the ICO PIA guidance and/or how well they integrate PIA with their project- and risk-management practices, especially where there are touch points.	The PIA code of practice will explain the principles behind an effective PIA process. Organisations should be able to develop their own benchmarks from the guidance.
6. We recommend that the ICO strongly urge PIA-performing organisations to report on how their PIAs have been implemented in subsequent practice, and to review the situation periodically.	The PIA code of practice will explain that following up and reporting on the findings of the assessment is an important part of the process.
7. We recommend that the ICO promote to organisations the benefits of establishing repositories or registries of PIAs. We recommend that the ICO compile a registry of publicly available PIA reports, or at least a bibliography of such reports.	The PIA code of practice will encourage the publication of PIA reports. The sector definition documents for FOIA publication schemes recommend that PIA reports are published. For example see the central government document. The ICO will initially focus on encouraging organisations to publish their own reports rather than establish a central repository. We will also look to

Recommendation	Response
	encourage sector-specific bodies to create repositories of PIAs carried out by organisations in their sector.
8. We recommend that the ICO take advantage of the current work within ISO to develop a PIA standard, and the BSI's technical panel's contribution to it.	We agree that a PIA standard would be useful, as long as it is not too prescriptive and remains focused on the PIA as a process. We will engage with BSI to assist in the planning of an ISO standard.
9. We recommend that the ICO audit the PIA process and PIA reports in at least a sample of government departments and agencies.	We have included PIAs in the list of possible controls checked when auditing organisations. This helps the ICO to understand how widely used PIAs are, and the impact they have on compliance.
10. We recommend that privacy risk be taken into explicit account in the Combined Code for companies listed on the London Stock Exchange.	The ICO will explore the options available to promote PIAs and understand how privacy risk can be approached in the private sector. We will look to build on our existing approach of promoting data protection as something which is of benefit to business, not a regulatory burden. The consultation on the draft PIA code of practice will ask respondents for their views on this area.
11. We recommend that privacy risk be inserted into government guidance such as the Treasury Orange Book and the Green Book on appraisal and evaluation in central government.	The 2009 Data handling review made PIAs a requirement for some central government projects. This helped to raised awareness of PIAs in government departments. We will consider the best ways to continue to promote PIAs, and this will be included in

Recommendation	Response
	the code of practice consultation.
12. We recommend that, at senior ministerial and official levels in government departments, and among special advisers, the ICO engage in dialogue to underline the importance of privacy and PIA while developing new policy and regulations and in the communication plans accompanying new policies.	We will look at the best ways for the ICO to communicate the PIA report and code of practice at senior government levels.
13. We recommend that the ICO encourage the Treasury to adopt a rule that PIAs must accompany any budgetary submissions for new policies, programmes and projects.	We will seek to explore with the Treasury some possible criteria for carrying out PIAs. However, we recognise that mandatory use of PIAs accompanying budgetary submissions may not be a practical option in all circumstances.
14. We recommend that the ICO encourage ENISA to support the ICO initiatives with regard to insert provisions relating to PIA in risk management standards as well as within ENISA's own approach to risk assessment.	We will promote the code at a European level with various stakeholders, including ENISA.
15. We recommend that the ICO accelerate the development of privacy awareness through direct outreach to organisations responsible for the training and certification of project managers and risk managers.	We will include this in the action plan for engaging with organisations developing privacy standards, and will cover this in the consultation.