EXECUTIVE SUMMARY

Privacy impact assessments (PIAs) are widely used in the UK, especially by government departments and agencies, local authorities, national health service (NHS) trusts and even by companies, according to a survey carried out in early 2013, which found that more two-thirds of respondents were conducting privacy impact assessments.

The UK was the first country in Europe to develop and promulgate a privacy impact assessment methodology. The Information Commissioner's Office (ICO) published a PIA Handbook in December 2007, followed by a revision in June 2009.

The Cabinet Office accepted the value of PIA reports and stressed that they will be used and monitored in all departments as a means of protecting personal data from July 2008 onwards. PIAs have thus become a "mandatory minimum measure" in the UK government and its agencies.[1]

Following the ICO's lead, the European Commission introduced its proposed Data Protection Regulation in January 2012, Article 33 of which would make PIAs mandatory for both public and private sector organisations throughout Europe[2] where processing operations are likely to present specific risks to the rights and freedoms of data subjects.

While the ICO's PIA Handbook would appear to have had some success, the ICO has had concerns, which prompted the regulator to put out a tender in late 2012, the aim of which was

- To understand how privacy impact assessment (PIA) can be better integrated with existing project and risk management tools, and
- To help make PIA a more practical and effective tool.

Trilateral Research & Consulting won the tender. Work began on the present study was in mid-January 2013. Among other things, the study aims to provide input to the ICO, which intends to produce a further revision of its PIA guide in the coming months.

Methodology

Trilateral employed several different methodologies to determine to what extent PIAs are used in the UK, how they are used, comments by users on their efficacy, the extent to which they are integrated in project and risk management, how they could be better integrated, and recommendations for improving the PIA guidance.

[1] See Cabinet Office, Cross Government Actions: Mandatory Minimum Measures, 2008, Section I, 4.4: All departments must "conduct privacy impact assessments so that they can be considered as part of the information risk aspects of Gateway Reviews".

http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf. Gateway reviews are undertaken by an independent team of experienced people and carried out at key decision points in government programmes and projects to provide assurance that they can progress successfully to the next stage.

[2] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012.

First, we analysed the ICO's PIA Handbook and developed an analytical framework consisting of a two-column table with 16 "**touch points**". These touch points are key points or elements of the ICO PIA methodology. We converted these touch points into questions, which we used throughout our study to interrogate other PIA methodologies, PIA reports, project and risk management methodologies. The aim was to locate similarities between these approaches and PIA that will provide opportunities for integration.

Second, for comparative purposes, we examined three other PIA frameworks.

Third, we compiled all of the publicly available UK PIA reports that we could find and analysed several of them using the "touch points".

Fourth, we sent out a questionnaire to 829 companies, central government departments and agencies, local authorities and NHS trusts, asking about their use of the ICO PIA Handbook and the extent to which they include privacy risks in their project and risk management practices.

Fifth, we conducted 12 in-depth case studies based on interviews with a mix of respondents to our survey and, in particular, from the private sector.

Sixth, we then analysed four project management methodologies and 15 risk management methodologies using our 16 touch points to see where we could find some commonalities. We also looked for "open doors", by which we mean any points in a project and/or risk management process where a PIA could be introduced.

Seventh, we conducted a "horizontal" analysis or comparative analysis of our findings, which eventually led us to the formulation of recommendations to the ICO.

The following pages summarise some of the key findings.

The PIA Handbook

The Handbook cautions that, because organisations vary greatly in size, the extent to which their activities intrude on privacy and their experience in dealing with privacy issues makes it difficult to write a "one size fits all" guide. Indeed, from the results of our survey and our analysis of existing PIA reports, the ICO was prescient – almost all organisations have adapted the guidance from the ICO Handbook according to their perceived needs.

According to the Handbook, a PIA is necessary for the following reasons: to identify and manage risks; to avoid unnecessary costs through privacy sensitivity; to avoid inadequate solutions to privacy risks; to avoid loss of trust and reputation; to inform the organisation's communication strategy and to meet or exceed legal requirements.

The PIA Handbook does well to emphasise that a PIA should not only consider personal data, but four different types of privacy, i.e., privacy of personal information, privacy of the person, privacy of personal behaviour and privacy of personal communication. Unlike Article 33 of the EC's proposed Data Protection Regulation, which is focused on only a data protection impact assessment, the Handbook ICO adopts a much wider view of privacy.[3]

[3] ICO, PIA Handbook, p. 14.

Although other PIA guidance documents also mention these four types of privacy, the ICO Handbook provides more detail and clarity with regard to what is at stake. We strongly support the ICO's view of privacy as being more than just data protection. We think Article 33 is seriously deficient in reducing a "privacy impact assessment" to only a "data protection impact assessment". Organisations that carry out a DPIA may be fully compliant with data protection legislation, but could still intrude dangerously into an individual's privacy. Such a risk is greatly diminished if all types of privacy are considered, as the ICO Handbook rightly argues.

The Handbook foresees the utility of integrating PIA with risk management practices. It notes that "[r]isk management has considerably broader scope than privacy alone, so organisations may find it appropriate to plan a PIA within the context of risk management".

We distinguish between a PIA *process* and a PIA *report*. Engaging in a PIA is itself a valuable learning exercise for organisations, and some would argue that this process is more important than the report itself. The report is meant to document the PIA process, but in fact the PIA process extends beyond a PIA report. Even after the PIA assessor or team produce their report, which in most cases should contain recommendations, someone will need to make sure the recommendations are implemented or, if some are not, explain why they are not.

The PIA Handbook distinguishes between a full-scale PIA and a small-scale PIA. We think this is confusing for organisations. We do not think it is so easy to determine whether a full-scale or small-scale PIA is appropriate – despite (or perhaps even because of) the criteria in Appendix 1 of the Handbook. We suggest that, in a revised Handbook, the ICO simply say that PIAs are scalable, and that the scope, length and intensity of the PIA will depend on how serious the privacy risks are and on the numbers of people who might be impacted.

As a PIA methodology, the ICO Handbook has many good points. In revising it, or producing a third edition, the ICO should be careful not to throw the baby out with the bathwater. In view of comments made in interviews and other exchanges with organisations, our overall recommendation is that the methodology be streamlined. In a revised PIA Handbook, the ICO may wish to consider preparing a somewhat high-level, principles-based PIA methodology, perhaps with an annex of exemplary privacy risks and questions that could be used to uncover those risks. Sectors or organisations could then use this streamlined, principles-based guide for further development of a sector- or organisation-specific PIA attuned to the specificities of their sector or organisation.

Other PIA frameworks

Following our review of the PIA Handbook, for comparative purposes, we analysed three other PIA frameworks, namely, the RFID Framework which was endorsed by the Article 29 Data Protection Working Party in February 2011, Article 33 of the European Commission's proposed Data Protection Regulation, which would make PIA mandatory where organisations processing personal data present risks to data subjects, and the PIAF methodology which emerged from a project funded by the EC's Directorate General Justice and in which Trilateral was a partner.

Several data protection authorities said in their responses to the PIAF questionnaire that they preferred a streamlined, short, easy-to-understand and easy-to-use methodology. Hence, PIAF produced a six-page "Step-by-step guide to privacy impact assessment" and a six-page "Template for a privacy impact assessment report".[4] We suggest that the ICO's third edition be like the "Step-by-step guide", but with two or three annexes identifying privacy risks, some questions aimed at uncovering those risks, and references to some particularly good risk assessment and risk management methodologies such as that of CNIL.

PIA reports

We then reviewed several publicly available PIA reports to see how well they track the guidance provide by the PIA Handbook. After a detailed search on the Internet, we identified 26 publicly available PIA reports in the UK, all of which bar two originate in the public sector. Of these, we selected several for more detailed analysis. Our interest in reviewing these PIA reports is to see how closely they track the ICO PIA Handbook, as represented by the 16 touch points. Further, our review of existing PIA reports helps to provide a view of how PIAs are currently practised by public and private organisations.

From our analysis of 26 publicly available UK PIA reports, we found that

- The majority of PIA reports number fewer than 30 pages.
- The number of publicly available PIA reports is growing (slowly).
- The vast majority of publicly available PIA reports have been produced by government departments and agencies; we found only two from industry.
- Among the various stated purposes for producing PIAs are concerns about privacy impacts, and impacts on the organisation's reputation.
- Most of the PIA reports acknowledge the ICO PIA Handbook; some say they have consulted the ICO for advice on the preparation of the PIA reports.
- Some PIA reports have said that they will be updated if there are any changes in the assessed project, programme or other activity involving the processing of data. Only one such update has been found on the Internet; it is not known whether PIAs have, in fact, been updated.
- Most PIA reports appear to have been produced "in-house"; only two of the 26 publicly available PIA reports were produced by external consultants, and those two were the only discovered PIAs that emanated from the private sector. While there is nothing wrong with using external consultants to conduct the PIA – some argue that using external consultants will give the resulting PIA reports more credibility – generally organisations need to build up their own internal PIA expertise.
- Almost all of the PIA reports examined for our study show that they were undertaken before their projects were finalised, when there was still an opportunity for the PIAs to influence the design or outcome of the project; this is good practice.

Surveys

Trilateral conducted three surveys germane to this study. The first, conducted in May 2012, was aimed at determining whether UK organisations are conducting PIAs and whether they experience fewer data breaches because they are, as a consequence of conducting PIAs, more careful with personal data.

[4] Both papers can be found here: http://www.piafproject.eu/Events.html

The second survey was in support of our tender proposal to the ICO, and was aimed at finding out which risk management methodologies UK organisations were using and whether respondents felt PIA could be integrated with their risk management practice.

The third, and much larger, survey was part of this study and expanded upon the first two surveys. Its purpose was to find out what percentage of responding organisations were conducting PIAs and how many they have conducted and whether PIA could be integrated in their project and risk management practices. For this survey, the questionnaire was distributed in January 2013 to 829 contact persons in central government bodies, NHS trusts, local authorities, and FTSE100 and FTSE250 companies.

The main findings from the surveys were that:

- More than two-thirds of responding organisations have done a PIA.
- Some organisations have done one, two or only a few PIAs, while others claimed that they have done vastly more.
- Respondents used a wide variety of project and risk management standards and methodologies. In the public sector, the Treasury's Orange Book was the main risk management guide and PRINCE2 was the most widely used project management methodology.
- All of the respondents consider, or are in the process of considering, privacy risk as part of their overall risk management process, and therefore focus on "the wide range of risks to which the project/activity is potentially exposed". All of the respondents have established close collaboration between the risk manager and the data protection officer regarding privacy risks, with the data protection officer working closely with the risk manager "on relevant issues, and providing updates to one another as to current guidance/awareness".

It was extremely difficult to compile contacts for private companies. Very little contact information is available on their websites. Switchboard and call centre staff were often unwilling to connect to named members of staff or provide e-mail addresses. There was little information about privacy and data protection processes on company websites, other than the generic website privacy policy. Where there was data protection information provided, there was no specified contact provided, and queries were directed towards the generic "info@..." e-mail address. In addition, even if the website provided the company's annual report, this did not include any specific names and/or contacts and was often difficult to find. As a result of the lack of publicly available contact information, we were forced to initially rely on company information, provided by stock market websites, and then on social networking sites as well as Trilateral's own network of professional contacts. Overall, the extent of information asymmetry that appears to characterise the relationship between the public and companies is striking.

Case studies

We undertook more than a dozen in-depth case studies, based on interviews conducted with selected respondents to the questionnaire. The case studies were of two types. The first type concerned PIA and its integration in the project and risk management practices of the organisations. The second type concerned PIA and the policy-making process. We used the case studies to investigate more deeply how organisations have practically integrated PIA into their existing project and risk management methodologies and processes, as well as to identify key lessons learned from their experience of the integration and the use of the ICO PIA Handbook.

Among the highlights of the case studies are the following:

- Privacy is an important consideration for almost all of the organisations to whom we spoke. Many of them said privacy impacts were considered before or at the initiation of a project, e.g., at the procurement stage or formulation of a business case for a new project.

- To foster integration with project and risk management methodologies, more action needs to be taken. Several said it was important to gain buy-in from senior management and develop privacy awareness and culture within the company, sustained by effective communication and training. Organisations need to deliver a clear message to all project managers that the PIA process must be followed and that PIAs are an organisational requirement.

- Most said they adapted not only the PIA Handbook but also the project and risk management methodologies to meet their organisation's own, specific requirements.

- Most advocated a slimmed-down ICO Handbook and some said that the ICO should provide more practical tools and guidance on how to assess privacy risks, since organisations often do not have the knowledge and experience required to do so, and That the Handbook should more clearly indicate the benefits of PIAs.

From the various comments made by respondents in these case studies, the following are the key lessons that have helped to shape our recommendations:

- Ensuring the "buy-in" of the most senior people within the organisation is a necessary pre-condition for a successful integration of privacy risks and PIA into the organisation's existing processes. PIA processes need to be connected with the development of privacy awareness and culture within the company. Companies need to devise effective communication and training strategies to sustain a change in the mindsets of, and in the development of new skills for, project managers. The organisation needs to deliver a clear message to all project managers that the PIA process must be followed and that PIAs are an organisational requirement. Simplicity is the key to achieve full implementation and adoption of internal PIA guidelines and processes.
- An extensive and inclusive internal consultation, involving different parts of the organisation, is critical when defining the integration process. This will guarantee the full "buy-in" of all the interested and/or affected parties when the process is implemented.
- The documentation that the privacy team provides to support project managers when they do the PIA is important. Project managers must have all the information and the questions and answers they need to do a proper assessment. It is important to give them all the necessary data they need to allow them to make the necessary project adjustments in order to be fully compliant. Project managers need additional training and clear internal guidelines on how to do PIAs and complete PIA forms.

- All project plans should have a task on privacy, which will ensure that all of the privacy requirements are fully visible to and updated and monitored by project managers.
- Local authorities (indeed all organisations) need to establish central PIA repositories where all the PIAs conducted by the council are stored and can be accessed. This will promote a culture of sharing and benchmarking (i.e., councils can compare how well or badly they do in relation to privacy risks and PIAs), which in turn will support learning and self-improvement.

Project management standards and methodologies

Chapter 2 describes four popular project management standards and methodologies in use in the UK and abroad. These are:

- PMBOK
- PRINCE2
- Agile
- HERMES

For each methodology, we provide an overview followed by a table in which we "interrogate" the methodology using a set of questions derived from the PIA Handbook touch points. By developing a set of questions based on the PIA Handbook touch points to interrogate the project management methodology, we can determine whether there are sufficient commonalities between the PIA process and the project management process so that a PIA could be conducted in tandem with the project management process without disrupting it. Further, if there are a sufficient number of commonalities, then we assume that integration of PIA into the project management process will be possible without much difficulty. If there are an adequate number of touch points, we assume that it will be easier to convince project managers that they should take account of – or integrate – PIA in their project management process.

Even if there are not so many touch points, there is still a possibility of integrating PIA in the project management process through one or more "open doors" – i.e., points in the project management process where or when it would be possible to conduct a PIA.

The data collected from the January 2013 survey have been useful for identifying "open doors" that some of the surveyed organisations are already using in order to integrate privacy risks into their project management processes and adopted standards. Based on the responses, integration occurs, most of the time, at the project initiation phase, when the organisation needs to provide formal approval for, and finalise the scope and resources of the project. By taking the project life-cycle into consideration, we have identified possible open doors in three main phases: pre-project open doors, project-initiation open doors and project-implementation open doors.

Of the four PM methodologies reviewed, only one (HERMES) includes clear provisions for being compliant with a personal data protection law. By contrast, many of the risk methodologies say that organisations should comply with regulations; PIA does that, although it should also focus on risks that may not be covered by simple compliance with legislation. There is little emphasis in the project management methodologies on compliance.

Risk management standards and methodologies

Chapter 3 parallels the previous chapter to some extent. It describes 15 popular risk management standards and methodologies in use in the UK and abroad. The principal differences are that the risk management area is much more diverse in terms of available standards to be applied, and the scope of each differs. For each methodology, we provide an overview followed by a table in which we "interrogate" the methodology using the 16 touch points. We analysed the following:

- ISO 31000:2009 Risk management — Principles and guidelines
- Combined Code and Turnbull Guidance
- the Orange Book
- ENISA's approach to risk management
- ISO/IEC 27005:2011 Information security risk management
- IT-Grundschutz
- NIST SP 800-39 Managing Information Security Risk
- ISACA and COBIT
- CRAMM (Central Computer and Telecommunications Agency Risk Analysis and Management Method)
- EBIOS
- OCTAVE®
- NIST SP 800-30 Guide for Conducting Risk Assessments
- ISO/IEC 29100:2011 Information technology — Security techniques
- NIST SP 800-122, Guide to Protecting the Confidentiality of PII
- CNIL methodology for privacy risk management.

All of these methodologies and standards have at least some touch points in common with PIA. ISO 31000, ISO 27005, ENISA, EBIOS, NIST SP 800-122 and CNIL's approach have quite a few.

From the survey and case studies analysis, we could regard the integration of privacy risk and PIA into the risk management processes as a necessary pre-condition for achieving an effective integration of privacy risk and PIA into project management processes. Furthermore, virtually all methodologies offer "open doors", points at which it would be possible to conduct a PIA, in whole or in part. We identified two categories of open doors: at *the risk corporate level* and at *the single-risk project level*. The corporate level refers to the integration of privacy risks and PIA into overarching, macro-corporate frameworks, while the single risk-project level indicates operational integration at the micro, individual project level.

Horizontal analysis

A horizontal analysis of the various project and risk management methodologies identifies some commonalities and differences with regard to the "touch points"– i.e., points of commonality between the PIA process and the project and risk management methodologies – and the "open doors" – i.e., where a PIA could interface with the project or risk management methodology or when in the project or risk management process a PIA could be conducted in whole or in part. We found that:

- Although the dominant project management methodologies (PMBOK and PRINCE2) differ significantly, they share a structured, process-driven approach to managing projects towards specific, well-defined business objectives. This structured approach provides a good basis for integration of PIAs. In each case, the methodology does not include any specific focus upon the core issues of privacy and data protection, but rather, provides a framework within which these issues can be addressed.

- ISO 31000 appears to be the most prevalent risk management methodology. It shares some "touch points" with PIA, but because it is a generic risk management methodology, it does not address some PIA issues – for example, it does not use the word "privacy", not is there any provision that might suggest recognition of data protection risks. However, communication and consultation with stakeholders are integral to the risk management process, hence, there are some "open doors" in the process where a PIA could be conducted. There is nothing in the standard that would be at odds with a PIA.

- There is some comparability between PIA and the Turnbull guidance. There is nothing in the Turnbull guidance that would act as a barrier to including a PIA in a listed company's risk management process.

- Although the Orange Book does not focus on risks to individuals, many of the points in its risk-management methodology seem compatible with PIA, and the way it addresses risk through an analysis of preventive and corrective controls could also provide a gateway for considering privacy impact as part of a mitigating strategy. So, too, could the Orange Book's concern with stakeholder expectations. Its discussion of potential risks brought about by new projects could also provide an "open door" if such projects involved new IT projects and systems, for which the need for a PIA could be identified within a privacy risk management routine.

- The ENISA risk management methodology meets many of the PIA "touch points". It offers several "open doors" (or interfaces) for integration of its risk management methodology with other corporate operational processes. Also of interest is ENISA's distinction between existing and emerging risks, and its approach to each. It manages existing risks using a somewhat tried and tested (but traditional) risk management approach, whereas it uses relatively elaborate scenarios to explore emerging risks.

- ISO 27005 has many "touch points" in common with the PIA Handbook. There are also several "open doors" for PIA to be done:
  - during the environmental scan (context establishment) phase
  - as part of the risk identification process (common to both ISO 27005 and PIA)
  - during the process of identifying controls (counter-measures) against the risks in preparing the risk treatment plan. The most appropriate part would be in identifying risks and, subsequently, controls.

Further observations

Before giving our recommendations, some further observations can be made on the basis of the analysis in the report:

- While there are commonalities between the project and risk management processes and the PIA process, most of the methodologies do not mention privacy risks or even risks to the individual. Nevertheless, to the extent that privacy risks pose risks to the organisation, the organisation should take account of such risks in their project and risk management processes, including listing such risks in the organisation's risk register. It should not be too difficult to convince organisations of the importance of taking privacy risks into account and regarding privacy risk as another type of risk (just like environmental risks or currency risks or competitive risks). Especially in industries that deal directly with the general public – for example, banking, entertainment, and retail – privacy breaches, not confined to "data breaches", can be a significant threat to the company's reputation. Based on examples of privacy breaches, it should not be too difficult to convince organisations about the need to guard against reputational risk.

- Many of the risk management methodologies include provisions for taking into account information security (as distinct from privacy risks), and specifically with regard to confidentiality, integrity and availability of the information. Few go beyond this with the notable exception of ISO 29100, which specifically addresses privacy principles, IT Grundschutz and the CNIL methodology on privacy risk management. One can note that the privacy part of IT Grundschutz was written by the German DPA, and that the CNIL is the French DPA. Helpfully, both the privacy part of IT Grundschutz and the guides published by the CNIL include catalogues of privacy threat descriptions supplemented by the corresponding privacy controls.

- Some of the project and risk management methodologies call for consulting or engaging stakeholders, especially internally, but some (e.g., ISO 31000, ISO 27005) externally as well. PIA does the same. Some of the project and risk management methodologies (e.g., ISO 31000, ISO 27005) call for reviewing or understanding or taking into account the internal and external contexts. This is true of PIA too.

- Some of the project and risk management methodologies emphasise the importance of senior management support and commitment, which is also important for successful PIAs. Some of the risk management methodologies call for embedding risk awareness throughout the organisation. Some call for training staff and raising their awareness, which is also essential to PIAs.

- Almost all of the methodologies are silent on the issue of publishing the project or risk management report, although some do attach importance to documenting the process. Similarly, most are silent on the issue of independent, third-party review or audit to the project or risk management reports. There is, however, a requirement for companies listed on the London Stock Exchange to include information in their annual reports about the risks facing the company and how the company is addressing those risks.

Recommendations

The final chapter of our report provides recommendations on the practical steps the ICO can take to promote a better fit between PIA and project and risk management standards and methodologies such as those described in this report. The recommendations are listed below, the detail of which can be found in Chapter 5.

Recommendations for the ICO

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.*

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.*

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.*

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.*

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".*

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.*

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.*

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.*

9. *We recommend that the ICO audit the PIA process and PIA reports in at least a sample of government departments and agencies.*

10. *We recommend that privacy risk be taken into explicit account in the Combined Code for companies listed on the London Stock Exchange.*

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.*

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.*

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.*

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.*

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.*

Recommendations for companies and other organisations

16. *We recommend that, to help embed PIA and to integrate it better with project and risk management practices, a requirement to conduct a PIA be included in business cases, at the inception of projects, and in procurement procedures. Organisations should require project managers to answer a simple PIA questionnaire at the beginning of a project or initiative to determine the specific kind of PIA that should be undertaken.*

17. *We recommend that senior management take privacy impacts into consideration as part of all decisions involving the collection, use and/or sharing of personal data.*

18. *We recommend that companies and other organisations review annually their PIA documents and processes, and should consider the revision or updating of their processes as a normal part of corporate performance management.*

19. *We recommend that companies and other organisations embed privacy awareness and develop a privacy culture, and should provide training to staff in order to develop such a culture. High priority should be given to developing ways of incorporating an enhanced PIA/risk assessment approach into training materials where information-processing activities pose risks to privacy and other values.*

20. *We recommend that companies and other organisations include contact details on their PIA cover sheets identifying those who prepared the PIA and how they can be contacted. The PIA should promote the provision of a contact person as "best practice". Such practice needs to be made mandatory certainly within any government organisation and any organisation doing business with the government. Such practice should also be promoted within standards organisations.*

21. *We recommend that public-sector organisations insert strong requirements in their procurement processes so that those seeking contracts to supply new information systems with potential risk to privacy demonstrate their use of an integrative approach to PIA, risk management and project management.*

22. *We recommend that companies and other organisations include privacy in their governance framework and processes in order to define clear responsibilities and a reporting structure for privacy risks.*

23. *We recommend that companies and other organisations include a PIA task, similar to a work-package or a sub-work-package, in their project plan structures in order to embed PIA better within project management practices, and that project managers monitor and implement this new privacy task, based on the identified privacy requirements, as is done in the case of other project tasks.*

24. *We recommend that, to foster internal buy-in for any newly adopted processes and procedures, companies and other organisations undertake extensive internal consultation with all parts of the organisation involved in risk management and project management, when thinking of integrating PIA into existing organisational processes.*

25. *We recommend that companies and other organisations include identified privacy risks in their corporate risk register, and that they update their register when new or specific types of privacy risk are identified by implementation teams.*

26. *We recommend that companies and other organisations develop practical and easy guidance on the techniques for assessing privacy risks and actions to mitigate them.*