“Privacy Assurance Module” concept

Discussion Notes (TA, RW)

30th July 2009

1. Value proposition
2. Conceptual model
3. PII good practice layer
4. Delivery model

Value proposition

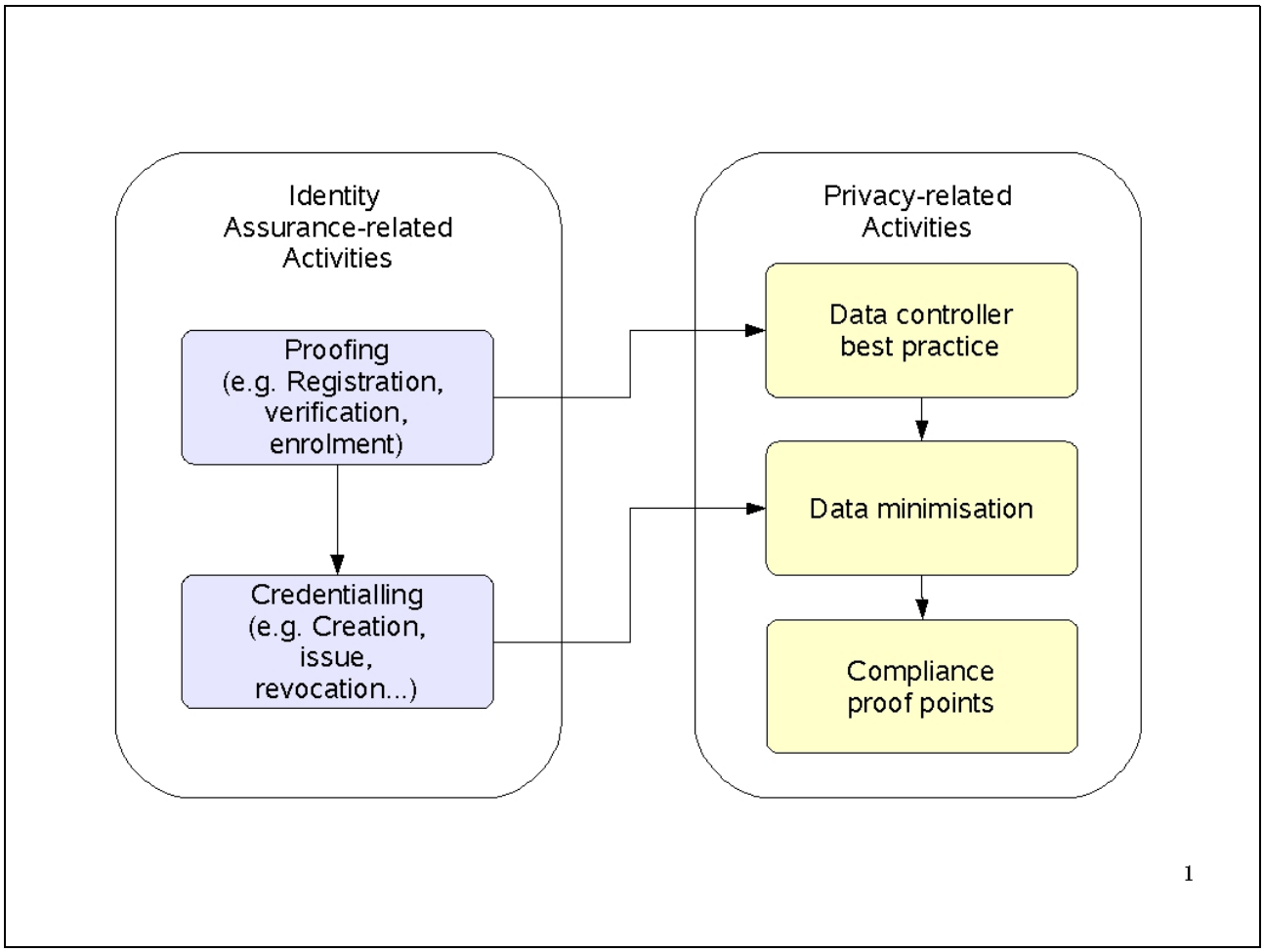
Organisations which adopt the Identity Assurance Framework have some incentive to do so (regulatory compliance, decreased liability, risk minimisation, combinations of these and other factors...). However, even a well-executed identity assurance process will give rise to privacy-related issues – for example, around the appropriate processing of personal data collected in the course of the process itself. Therefore there is a value to the same organisation in adopting measures which reduce the risk arising out of identity assurance activities.

There may be ways to further quantify this value – for instance, if the organisation has to indemnify itself against data breaches, consequential damage or improper use of personal data.

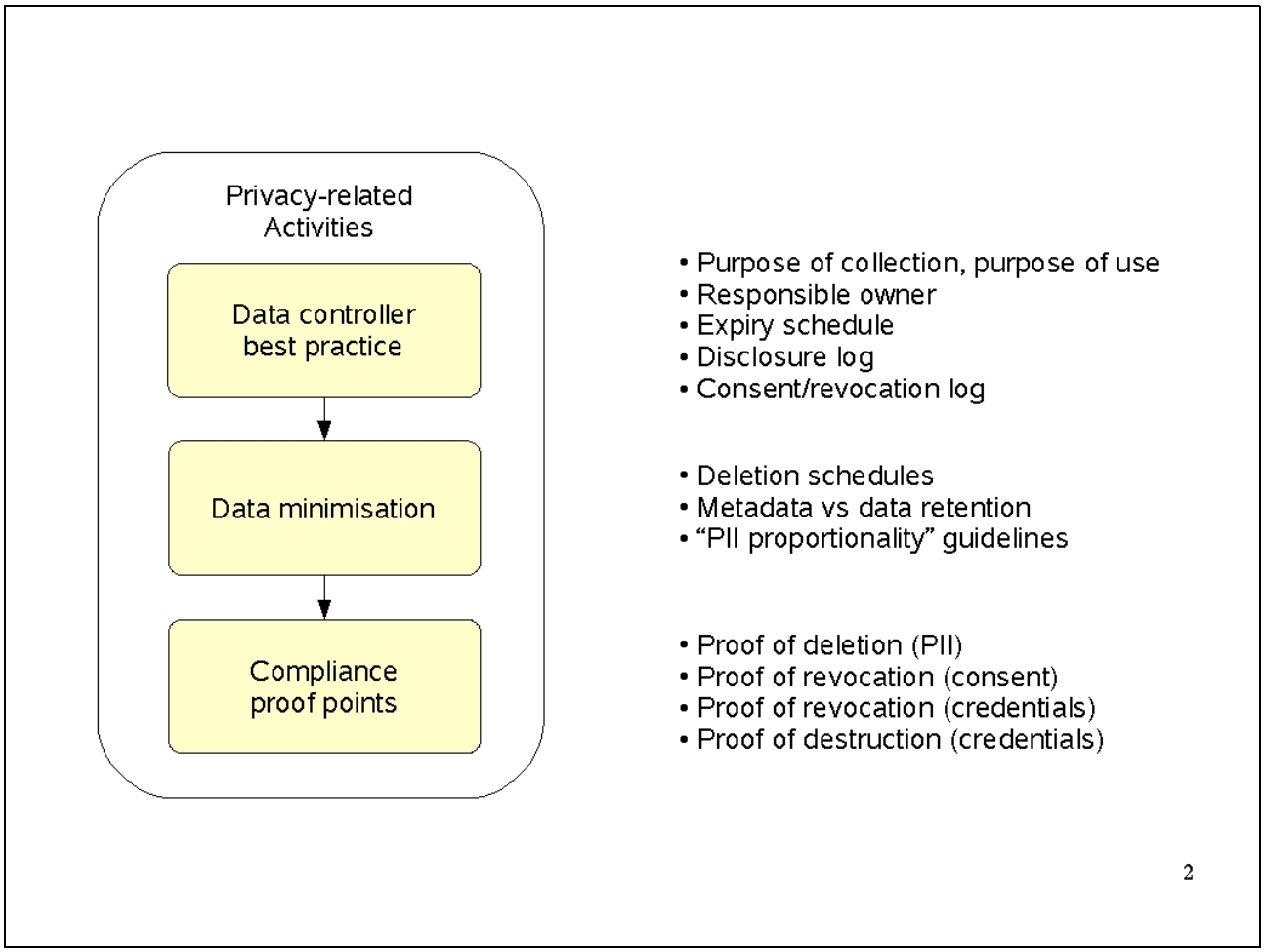
There may also be a need to adjust for differences between one regulatory regime and another – for instance, if the identity assurance requirement extends across borders, and the two countries involved have different definitions of what constitutes personal data, what constitutes a data breach, or different approaches to data protection/privacy law.

This document outlines an approach based on complementing the IAF with a 'privacy module' (as opposed to setting out to create a stand-alone “Privacy Assurance Framework” from scratch in its own right). This should reduce the initial investment of time required to produce an offering of value to adopters.

Conceptual model



PII good practice layer



Delivery model

What kinds of event could trigger the use of an IAF Privacy Module?

Assume an organisation has already implemented the Identity Assurance Framework. Then assume that the organisation plans a project which involves the processing of personal data; particularly for public sector organisations, this might give rise to a need for a Privacy Impact Assessment. When this happens for the first time, the process can be quite onerous.

However, if an IAF Privacy Module were used to apply structure and repeatability to the exercise, subsequent cycles should be easier, quicker and more cost-effective. The Privacy Module could also be used to generate a repository of PII meta-data which would reduce the assessment effort for other projects which plan to 'touch' the same inventory of personal data.