CEN

WORKSHOP

AGREEMENT

CWA 15262

April 2005

ICS 35.040

English version

Inventory of Data Protection Auditing Practices

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No.:CWA 15262:2005 D/E/F

Contents

Summary

Under supervision of CEN/ISSS, an inventory of data protection auditing practices has been carried out. Furthermore, the extent to which the practice of data protection audit could benefit from standardization has been assessed. The results of the inventory are taken up in chapter 4, the results of the assessment are taken up in chapter 5. A list of the material that is considered useful and that wholly or partially qualifies as best practice data protection audit material can be found in the annexes.

Preface

Attention for data protection and trust
Each organization processes personal data. Within the EU, processing personal data is subject to data protection legislation. Attention for the management of protecting personal data is important, not only because data protection is mandatory under the EU directive (95/46/EC) but also because data subjects expect their data is handled in accordance with their expectations and their privacy is respected. Therefore trust, privacy and data protection are inextricably linked.

A breach of privacy can destroy trust and consequently damage relationships between customers and their suppliers, employees and their employers, citizens and the government institutions etceteras. Since personal data is being processed using more and more complex and interrelated information and communication technologies, privacy (including security) and trust are essential conditions for doing (e-) business and running (e-) government processes. Because of the number of current and expected transactions and activities carried out online, privacy, data protection and trust become more and more important values.

Importance of a data protection audit
Trust can be realized by demonstrating compliance. Assurance whether personal data is handled in compliance with data protection principles can be provided by a data protection audit. An audit (especially when carried out on a regular basis) helps the organization:

- to identify non-compliance issues and/or to detect risks in it's own data protection management infrastructure;
- to maintain compliance with relevant privacy laws.

The data protection audit contributes to preventing privacy breaches (resulting in sanctions and/or negative reports). Also, for some organizations the data protection audit is an important tool in showing compliance with data protection requirements (e.g. via a privacy certificate); a positive outcome can be used by these organizations as a publicity advantage with regard to the competitors.

Background
The IPSE Expert Group found that there is a significant amount of audit activity going on in the privacy arena. Some Commissioners/Supervisory Authorities have audit powers or may carry out audits as part of investigation into allegations of noncompliance. Some have developed audit methodologies in their jurisdictions. Most of the large accountancy audit firms have developed or are developing a privacy practice which offers audit services. These may be developed from existing security or consulting practices and thus approach the privacy issues from a particular, and possibly sometimes limited, perspective. Legal firms with privacy practices have also developed data protection audit services. They may audit against the national law or the Directive, or to Safe Harbour. Such audits may be part of a wider project to achieve legal compliance. An audit may be a useful tool to raise the level of data protection awareness in a business.

Audit is a flexible tool. It can be used as a mechanism to assure compliance internally, whether the audit is carried out by a third party or in-house; it can be used as a mechanism to offer external assurances of compliance, in which case an audit will often be conducted by a

separate body. Auditing can assess compliance with internal policies; national laws or EU Directives; codes of conduct, or contractual obligations.

The IPSE Expert Group has not found any centre of expertise in this area. The field is growing but is still in its infancy. The Group consider that a study of this developing area would help focus on the developments. In particular it would enable an assessment of the extent to which a similar methodology could be applied to the different types of audit with a view to considering standard audit techniques. It could act as a focus for disseminating information. There is a need to explore how privacy audits might differ from traditional audits or security audits; consider what qualifications, experience or expertise might be required in auditors and review which parts of an audit would benefit from standardization. It would also be useful to clarify issues such as terminology.
Source: IPSE report on Data Protection, 2002 (available at www.cenorm.be/isss).

Towards a standard data protection audit practice
For multinationals, that are active in EU member states, it would be efficient to have one standard data auditing practice based on the EU as a baseline. Before considering such a baseline it is interesting to find out 'What's out there?' and to explore to what extent the practice of data protection audit could benefit from standardization. These subjects are addressed in this document.

0 Introduction

0.1 Background

The CEN/ISSS Workshop on Data Protection and Privacy agreed at its formal kick-off meeting on 3 July 2003 on the creation of a project team to draft various parts of the future CWA's of the Data Protection and Privacy Workshop.

Under supervision of CEN/ISSS PricewaterhouseCoopers (PwC) has prepared an inventory of data protection auditing practices to record best practice in this area. Furthermore PwC has assessed the extent to which the practice of data protection audit could benefit from standardization. The PwC team consisted of Daniëlla Goudswaard (main editor) and Erica Zaaiman (co-editor). Two industry reviewers reviewed the material prepared by PwC, Mr David Trower from IMS Health and Mr Werner Zwick from Deutsche Telekom.

The inventory of data protection auditing practices:

- provides information how audits can raise levels of awareness within a business;
- helps businesses considering an external or internal audit to understand the potential benefits;
- helps choosing an appropriate audit approach;
- illuminates the issues (or problems to be solved) arising in audits where cross jurisdictional compliance is a question;
- explores the training needs for auditors;
- assesses how compliance with the selected standard can be provided by the audit process;
- explores the areas of difficulty which may arise for auditors or firms involved in auditing.

0.2 Objective

The objective of this inventory document is:

- to give information on the current status of data protection audit practices regarding data protection audit material that can be considered as best practice;
- to give information on several audit related aspects (see bullets above);
- to give input for the discussion whether and to what extent the practice of data protection audit could benefit from standardization.

A meta-objective of this document is to give input for the 'way forward'. Besides providing information about data privacy audit material and exploring to what extent the practice of data protection audit could benefit from standardization towards a standard data protection audit practice, also recommendations regarding what kind of a data protection audit could benefit from standardization.

0.3 Audience

This document is prepared for the European Committee on Standardisation (CEN) that has adopted the IPSE (Initiative for Privacy Standardization in Europe) report.

This report makes several recommendations, amongst others to prepare an inventory of current data protection auditing practice, assessing the extent to which it could benefit from standardization.

Furthermore, organizations physically located (or doing business) in one or more of the EU member states considering a privacy audit, can use this document as background material when e.g. exploring what kind of best practice material is available and when exploring the possible benefits of the data protection audit, but also possible problems and issues that should be taken into account.

0.4 Status

This report has a final status. It is however important to realize that the list of collected audit material as taken up in this report is a picture: The material was collected actively by the Data Protection Workshop Team during the first half year of 2004. In the second part of 2004 several organizations contributed additional material. In the meantime, the data protection audit field is growing. An important indicator is the development of privacy certificates: Several data protection authorities (amongst others in the Netherlands and Switzerland) informed us that procedures of certification are being developed: Organizations can have a data processing operation certified (Netherlands) or can have systems, procedures or the organization certified (Switzerland) by approved and independent organizations.

1 Scope

This inventory should contribute to recording best practice in the field of data protection or privacy audits. We have considered an 'audit' to be a systematic and independent examination with the objective to give assurance. This is different from a 'self assessment': although a self-assessment can be done using an audit framework, the most important difference is that a self-assessment is not carried out by an **independent** (internal or external) auditor. Instead a self-assessment can be done by e.g. a line manager, a business process owner or an application owner.

2 References

IPSE report on Data Protection, 2002 (available at www.cenorm.be/isss)

Further: See Annexes A, B and C.

3 Definitions

For the needs of this document, the following definitions apply (Defined term: A short sentence defining the term in unambiguous terms):

Auditor:	The auditor is the internal or external party that carries out the audit.
Auditee:	The organization that is subject of the audit.
Data Protection Audit:	A data protection audit is a systematic and independent examination to determine whether activities involving the processing of personal data are carried out in accordance with an organization's data protection policies and procedures, and whether this processing meets the requirements of the EU Directive.