Outsourcing personal data processing to the cloud

Session 28

Thursday, November 8, 2012

11:30-12:30

Chris Mitchell

Professor of Computer Science

Royal Holloway, University of London

CLOUD SECURITY ALLIANCE CONGRESS 2012

MIS TRAINING INSTITUTE

Agenda

- The cloud data protection challenge
- Cloud security standardisation and data protection
- Context and structure of the ISO/IEC 27018 standard
- Draft contents of the ISO/IEC 27018 standard
- The way ahead

Security and privacy

- Much has been said about the security and privacy risks of cloud use.
- This is because cloud inevitably involves storage (and possibly processing) of data by a third party (the cloud provider).
- In a privacy context, a cloud service provider must show it meets the legal and regulatory obligations arising from *Data Protection* legislation and regulations.

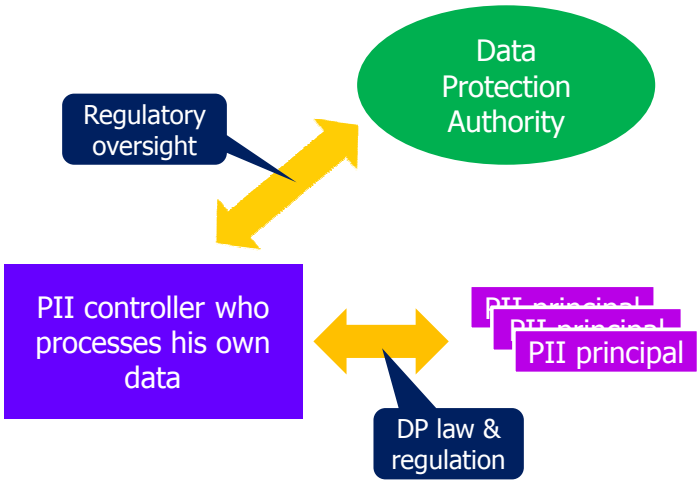
What is 'data protection'?

- In Europe (& some other countries / regions) policy and law provides for:
  - **the protection of information relating to private individuals from inappropriate collection, use and disclosure, and to ensure its timely disposal**.
- The European *Data Protection Directive* (95/46/EC) is implemented in EU national laws (e.g. the *Data Protection Act 1998* in the UK).
- Only some parts of this policy and law apply directly to a cloud service provider processing personal information for someone else (see the Annex).

Data protection vocabulary

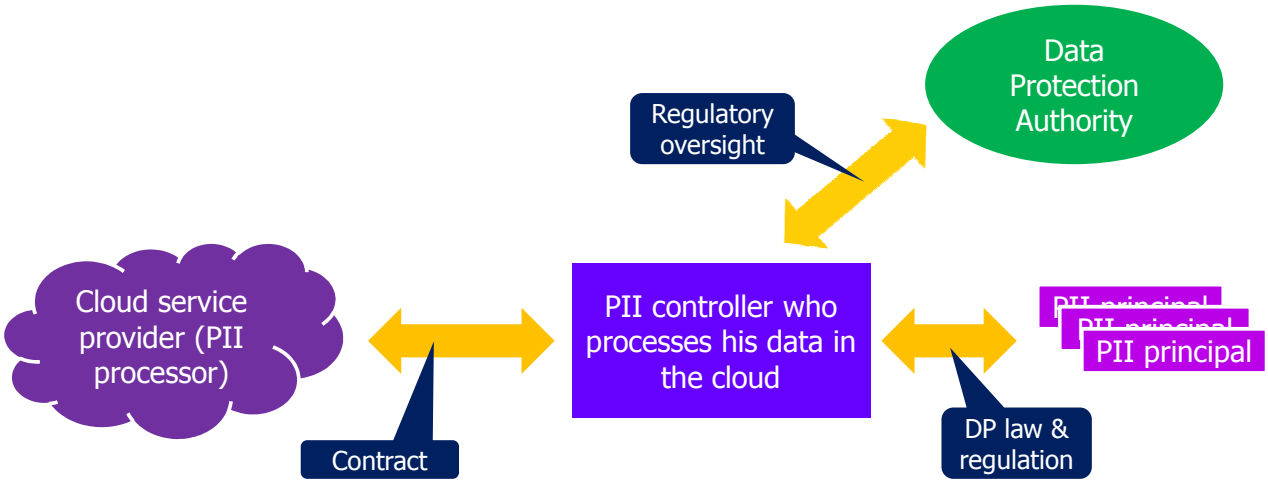
- **personally identifiable information (PII)**:
  - any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal;
    - **personal data** is sometimes used instead of PII.
- **PII principal**:
  - natural person to whom the personally identifiable information (PII) relates;
    - **data subject** is sometimes used instead of PII principal.

Data protection: basic relationships



PII controller (or sometimes **data controller**) is a person who (either alone or jointly or in common with others) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data protection: cloud relationships



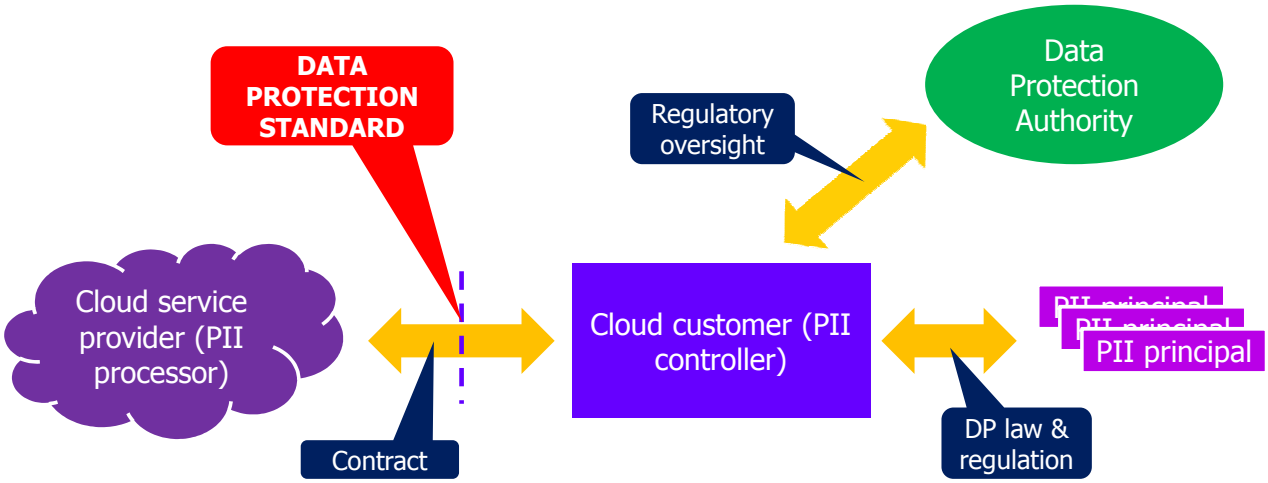
PII controller (or **data controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

PII processor (or **data processor**) is any person (other than an employee of the PII controller) who processes data on behalf of the PII controller.

Data protection & cloud: the issues

- PII controller keeps the legal responsibility:
  - Contract is a mechanism for the PII controller to deal with keeping the risk but outsourcing the processing.
- Using the cloud for processing PII also makes things more complex in other ways:
  - Outsourcing may now involve cloud service providers using services from other cloud providers; and
  - Many more small businesses, less expert in IT, outsourcing and data protection law, will use the cloud for processing PII.
- A suitable standard can assist with all of the above.

Data protection: cloud relationships



PII controller (or **data controller**) is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

PII processor (or **data processor**) is any person (other than an employee of the PII controller) who processes data on behalf of the PII controller.

Data protection obligations

- In every jurisdiction with data protection laws/regulations, public cloud providers must show potential PII controllers that their service meets legal needs.
- That is, they must show their service respects the regulations with respect to the obligations of PII processors.
- This is costly and time-consuming if done on a country-by-country basis.

Security and privacy

- Data protection is fundamentally a *privacy* issue.
- However, the issue of concern is primarily a *security* one, since we are dealing with data processors.
- That is, PII processors must meet the necessary security requirements so that all data (including PII) is handled appropriately.

Nature of obligations

- The obligations of a PII processor to a PII controller include:
  - protecting integrity and confidentiality of PII;
  - processing PII only in accordance with the objectives and instructions of PII controller;
  - providing transparency with respect to relevant aspects of PII processing, including the location of PII storage and security breaches;
  - maintaining logical separation of PII belonging to different controllers.

Agenda

- The cloud data protection challenge
- Cloud security standardisation and data protection
- Context and structure of the ISO/IEC 27018 standard
- Draft contents of the ISO/IEC 27018 standard
- The way ahead

Existing work

- The Cloud Security Alliance has itself published a number of key documents.
- These are likely to play a major role in guiding ongoing *de jure* standardisation developments.
- Notable amongst the various outputs are:
  - Security guidance for critical areas of focus in cloud computing, v3.0, November 2011;
  - Cloud controls matrix, v1.2, August 2011.

Range of possible standards

- Various security aspects of cloud computing services can usefully be standardised.
- For example:
  - security and privacy requirements applying to cloud providers;
  - service interfaces;
  - security techniques specific to cloud;
  - privacy requirements applying to cloud users (PII controllers).

Growing attention

- Cloud security standards work is now being undertaken by both ITU-T and ISO/IEC JTC1.
- The ITU-T Focus Group on Cloud Computing has produced a general document (Cloud-O-064) providing key definitions and threat discussions, that is intended to provide a foundation for future standardisation.
- Two cloud security standards (ISO/IEC 27017 and 27018) are being developed within ISO/IEC JTC1/SC27.

ISO/IEC 27017

- The first of the new cloud security standards, ISO/IEC 27017, is entitled *Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002*.
- It will provide a security control framework and implementation guidance for use by cloud consumers and providers.

ISO/IEC 27018

- The focus on this talk is on the second of the two new standards, ISO/IEC 27018.
- ISO/IEC 27018 will codify security requirements on cloud providers to assist in meeting **data protection obligations** of PII controllers.
- The focus of 27018 is thus much narrower than 27017.

The role of ISO/IEC 27018

- To respond to the issue that when a PII controller uses a cloud data processing service how does it know the PII they are entrusting to the PII processor will be treated in a way that fulfils the PII controller's obligations?
  - **ISO/IEC 27018 will provide for audited certification against a data protection standard to facilitate the contract between cloud provider and cloud customer.**

ISO/IEC 27018 in summary:

- Controls that are applicable to a **PII processor**, not to a **PII controller**
- Controls are therefore primarily information security controls rather than privacy controls (so the ISO/IEC 27001 ISMS is appropriate as the management system)

Audited cloud provider certification to achieve:

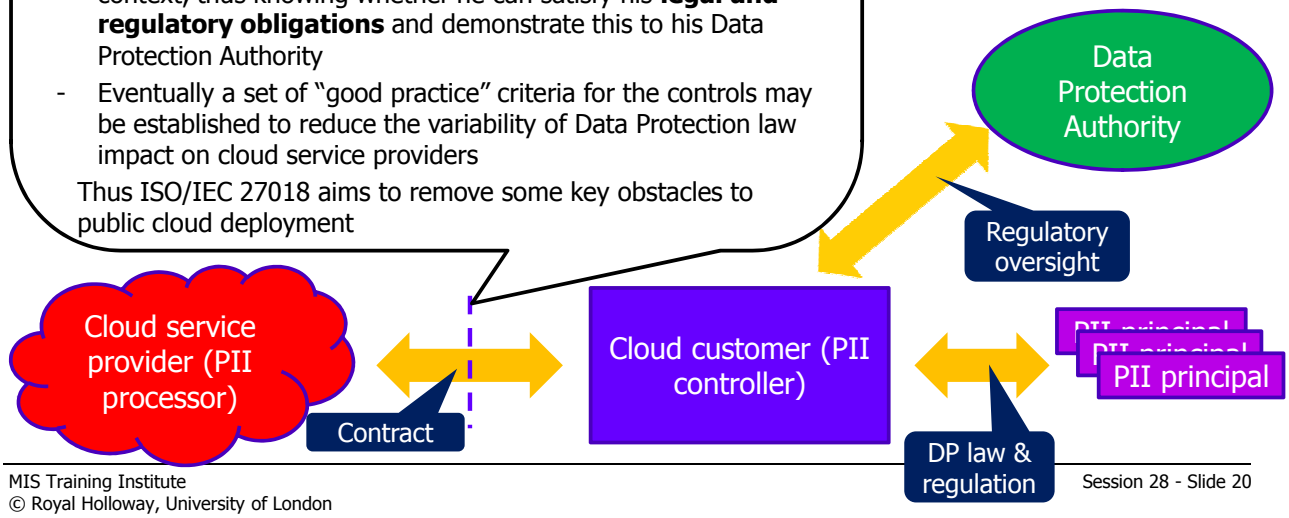
- Transparency in the **contract** relationship
- A **cloud customer** can select a **cloud service provider** knowing how the service provider operates in a data protection context, thus knowing whether he can satisfy his **legal and regulatory obligations** and demonstrate this to his Data Protection Authority
- Eventually a set of "good practice" criteria for the controls may be established to reduce the variability of Data Protection law impact on cloud service providers

Thus ISO/IEC 27018 aims to remove some key obstacles to public cloud deployment

The **PII Controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

The **PII Processor** is any person (other than an employee of the PII Controller) who processes data on behalf of the PII Controller.

Specifically these are EU data protection concepts, but may apply more widely in practice.



Parallel work

- In parallel with developing ISO/IEC 27017 and 27018, a wide-ranging study is ongoing within SC27 on *Cloud Computing Security and Privacy*.
- One of study's main goals is to consider possible additional New Work Items addressing cloud computing security and privacy.
- Its work will be based on National Body and Liaison Organisation contributions.

Agenda

- The cloud data protection challenge
- Cloud security standardisation and data protection
- Context and structure of the ISO/IEC 27018 standard
- Draft contents of the ISO/IEC 27018 standard
- The way ahead

27000 series standards

- The ISO/IEC 27000 series of standards are concerned with information security management systems (ISMSs):
  - 27000: ISMSs – Overview and vocabulary;
  - 27001: ISMSs – Requirements;
  - 27002: Code of practice for information security controls.
  - … many more …

ISO/IEC 27001

- The first main standard in the series lists requirements for the establishment and operation of an ISMS.
- It covers high-level operational and staffing issues.

ISO/IEC 27002

- ISO/IEC 27002 is probably the most celebrated and widely used member of the 27000 family.
- It owes its origins to BS 7799 (a UK standard) which became ISO/IEC 17799 and was later rebadged 27002.
- It provides a large catalogue of security controls to be used when implementing an ISMS.

Sector-specific standards

- Within the 27000 family are sector-specific standards, i.e. standards which apply 27002 to specific application domains.
- For example, ISO/IEC 27011 is focussed on telecommunications.
- It provides an interpretation of ISO/IEC 27002 aimed specifically at this sector.
- It also provides additional security controls relevant to this sector.

Structure of ISO/IEC 27018

- Both ISO/IEC 27017 and ISO/IEC 27018 are sector-specific standards building on ISO/IEC 27002.
- That is, these standards:
  - adopt the existing control set in ISO/IEC 27002;
  - add cloud-specific guidance to the existing controls; and
  - add additional controls and guidance relevant to the cloud.

ISO/IEC 27018 – title

- ISO/IEC 27018 has the title:

  Code of practice for data protection controls for public cloud computing services

ISO/IEC 27018 – status

- After a successful ballot result (agreeing to proceed), a preliminary working draft was circulated early in 2012.
- After discussions at May 2012 SC27 meeting in Stockholm, a first official working draft was circulated in June 2012.
- National Body comments in this draft were recently discussed at the October 2012 SC27 meeting in Rome.
- Was agreed to produce a second working draft for national body review and comment, and for discussion at the next SC27/WG2 meeting in Sophia Antipolis (France) in April 2013.

Agenda

- The cloud data protection challenge
- Cloud security standardisation and data protection
- Context and structure of the ISO/IEC 27018 standard
- Contents of the draft ISO/IEC 27018 standard
- The way ahead

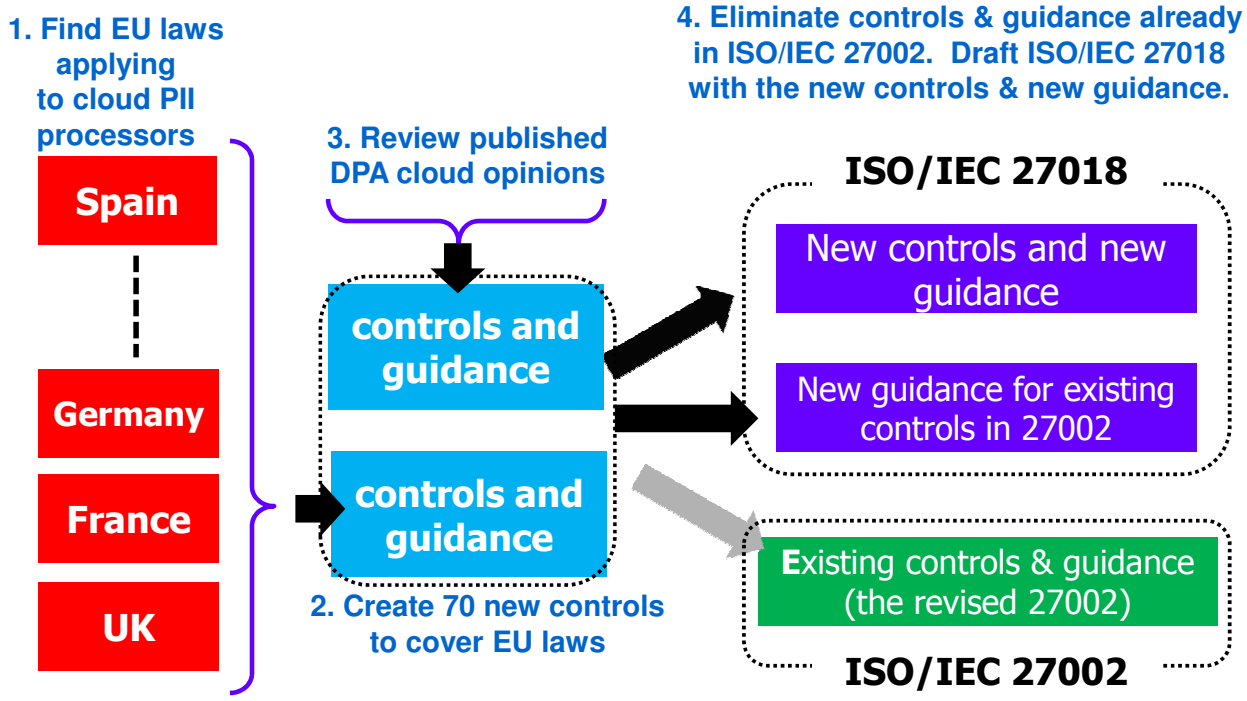
ISO/IEC 27018 – content

- Objective is to collect and organise security categories and their controls from current data protection regulations.
- Help public cloud service providers to comply with their obligations and make this transparent to their customers.
- Customers can select cloud-based data processing services that allow them to meet their obligations.

Generation of content

- The additional guidance and controls in the 1st working draft came from a detailed analysis of data protection legislation in a large number of countries.
- The goal is for ISO/IEC 27018 to meet the vast majority of requirements in all jurisdictions, thus greatly simplifying the acceptance process in each.
- Additional guidance and controls will come as a result of further expert review.

Origins of content in ISO/IEC 27018



Europe versus International

- Is it OK to use European controls in an international standard?
  - **Controls are not mandatory. Their use (or not) is determined by a risk assessment. So ISO/IEC 27018 is a catalogue.**
  - **Non-EU countries may add their specific controls, and the PII processor's country-specific risk assessment will determine which data protection controls (if any) to apply.**

PII processor versus PII controller

- ISO/IEC 27018 only covers controls for the PII processor, not the PII controller.
- Thus 27018 not complete in the perception of Data Protection Authority (which interacts primarily with PII processor), but:
  - it solves a clear real-world problem that needs addressing quickly;
  - full set of controls will be included in a new standard (*Code of practice for protection of PII*) to be developed following a study of PII management in JTC1/SC 27.

ISO/IEC 27018 – structure

- The general structure follows (2nd edition of) ISO/IEC 27002, in which controls are listed under the following headings:
  - Security policy;
  - Organisation of information security;
  - Asset management;
  - Human resources security;
  - Physical and environmental security;
  - Supplier relationship management;
  - Communications and operations;
  - Access control;
  - Systems acquisition, development and maintenance;
  - Information security incident management;
  - Business continuity management;
  - Compliance.

27018: types of content

- Apart from the introductory material, the text of ISO/IEC 27018 will contain two main types of content:
  - cloud data protection specific implementation guidance;
  - additional (cloud data protection specific) controls.
- We next review these two types of content, with examples.

Implementation guidance

- ISO/IEC 27002 consists of a long list of (categorised) security controls, with implementation guidance in each case.
- Where relevant, ISO/IEC 27018 provides additional implementation guidance, specific to the obligations of a cloud provider relating to data protection.
- We next look at examples of this specific guidance.

Guidance – example 1

- **27002 control category**: *Separation of development, text and operational environments*
- **Cloud-specific guidance**:
  The use of PII in testing should be avoided; where the use of PII cannot be avoided, measures should be implemented to secure the testing environment.

Guidance – example 2

- **27002 control category**: *Management of removable media*
- **Cloud-specific guidance**:
  Measures should be put in place designed to ensure that the removal of physical media (e.g. USB sticks, CD-ROMs and other data carriers) and documents, containing PII, from the premises where the database/application of located, is subject to authorisation by an appointed responsible individual or relevant procedure.

Guidance – example 3

- **27002 control category**: *Information transfer policies and procedures*
- **Cloud-specific guidance**:
  A system should be put in place designed to record incoming and outgoing physical media containing PII, including the type of physical media, the authorised sender & recipients, the date and time, the number of media, and the types of PII they contain.

Guidance – example 4

- **27002 control category**: *Event logging*
- **Cloud-specific guidance**:
  Measures should be put in place designed to ensure that a security officer has a process for verifying the event log with a specified, documented periodicity, to identify irregularities and propose remediation efforts. Where possible, the event log should record whether or not PII has been changed (added, modified or deleted) as a result of an event. Where multiple service providers are involved in providing service at different layers of the cloud stack, there may be varied or shared roles in implementing this guidance.

Guidance – example 5

- **27002 control category**: *Protection of log information*
- **Cloud-specific guidance**:
  Log information recorded for purposes such as security monitoring and operational diagnostics may contain PII. Measures, such as controlling access, should be put in place designed to ensure that logged information is only used for its intended purposes.

Additional controls

- ISO/IEC 27018 provides a set of controls designed specifically to support data protection for public cloud service providers.
- We next look at key examples of such additional controls.

Extended controls – Organization #1

- **27018 control category**: *Confidentiality and non-disclosure agreements*
- **Control**:
  Measures should be put in place designed to ensure that individuals with access to PII are subject to a confidentiality obligation.

Extended controls – Communications/operations #1

- **27018 control category**: *Restriction of the use of printing*
- **Control**:
  Measures should be put in place designed to restrict printing of PII.

Extended controls – Communications/operations #2

- **27018 control category**: *Control and logging of data restoration*
- **Control**:
  Measures should be put in place designed to ensure that there is a procedure for, and a log of, data restoration efforts.
- **Implementation guidance**:
  This log should contain the person responsible, a description of the restored data, and the data that were restored manually.

Extended controls – Communications/operations #3

- **27018 control category**: *Logging of PII disclosures*
- **Control**:
  Disclosures of PII should be recorded, including what PII has been disclosed, to whom, at what time.
- **Implementation guidance**:
  The disclosure of PII does occur as part of normal operation, so regular operational access to PII will be logged. Additional disclosures, if any, should also be logged.

Extended controls – Communications/operations #4

- **27018 control category**: *Intended destination of PII*
- **Control**:
  Measures should be put in place designed to ensure that it may be ascertained where exactly (to which organization and/or to which individual) PII is intended to be transmitted using data-transmission equipment.

Extended controls – Communications/operations #5

- **27018 control category**: *Erasure of temporary files*
- **Control**:
  Measures should be put in place designed to ensure that temporary files and documents are erased or destroyed within a specified, documented period after they are no longer needed.
- **Implementation guidance**:
  PII processing systems should implement a periodic check that unused temporary files above a specified age are deleted from the filing system.

Extended controls – Communications/operations #6

- **27018 control category**: *Protecting data on storage media leaving the premises*
- **Control**:
  A procedure should be put in place designed to ensure that PII on media leaving the organization's premises is not accessible to anyone other than authorized personnel (e.g., by encrypting the data concerned).

Extended controls – Communications/operations #7

- **27018 control category**: *Use of unencrypted storage media*
- **Control**:
  Measures should be put in place designed to ensure that physical media and portable devices that do not permit encryption are not used except where it is unavoidable, and designed to ensure that any use of such media and portable devices is documented.

Extended controls – Communications/operations #8

- **27018 control category**: *Encryption of PII transmitted over public networks*
- **Control**:
  A procedure should be put in place designed to encrypt PII that is transmitted over public networks.
- **Implementation guidance**:
  In some cases, for example the exchange of e-mail, the inherent characteristic of public network systems might require that some header or traffic data be exposed for effective transmission. Where multiple service providers are involved in providing service at different layers of the cloud stack, there may be varied or shared roles in implementing this guidance.

Extended controls – Communications/operations #9

- **27018 control category**: *Disposal of hardcopy materials*
- **Control**:
  Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.

Extended controls – Access control #1

- **27018 control category**: *Unique use of identifiers*
- **Control**:
  If more than one individual has access to stored PII, then measures should be put in place designed to ensure that they each have a distinct identifier for identification, authentication and authorization purposes.

Extended controls – Access control #2

- **27018 control category**: *Records of authorized users*
- **Control**:
  An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.

Extended controls – Access control #3

- **27018 control category**: *Identifier management*
- **Control**:
  Measures should be put in place to ensure that de-activated or expired identifiers are not granted to other individuals.

Extended controls – Access control #4

- **27018 control category**: *Password storage*
- **Control**:
  While they are in force, passwords should be stored in a way which makes them unintelligible.

Extended controls – Compliance #1

- **27018 control category**: *Purpose – general*
- **Control**:
  Measures should be put in place designed to ensure that PII to be processed as part of a contract may not be processed for any purpose independent of the instructions of the PII controller.
- **Implementation guidance**:
  Instructions may be contained in the contract between the PII processor and PII controller.

Extended controls – Compliance #2

- **27018 control category**: *Geographical location of PII*
- **Control**:
  A policy should be put in place designed to specify and document the countries where it is possible that PII might be stored.
- **Implementation guidance**:
  The information about the countries where PII might be stored should be made available to customers.

Extended controls – Compliance #3

- **27018 control category**: *Maintenance period for administrative security policies and guidelines*
- **Control**:
  Measures should be put in place designed to ensure that administrative security policies and guidelines are maintained for a specified, documented period upon replacement (updating).

Extended controls – Compliance #4

- **27018 control category**: *No unilateral reduction in information security contract measures*
- **Control**:
  Data processing contracts between the PII controller and the PII processor should specify concrete, minimum technical and organizational measures designed to ensure information security.
  Such measures should not be subject to unilateral reduction by the PII processor.

Extended controls – Compliance #5

- **27018 control category**: *PII controller's commercial use*
- **Control**:
  Measures should be put in place designed to ensure that PII processed as part of a data processing contract is not used for purposes of advertising without consent of the PII principal.
  Such consent should not be a condition of receiving the service.

Agenda

- The cloud data protection challenge
- Cloud security standardisation and data protection
- Context and structure of the ISO/IEC 27018 standard
- Draft contents of the ISO/IEC 27018 standard
- The way ahead

Where are we in the process?

- At the time of preparing these slides (after the October 2012 Rome meeting) we are at 2nd Working Draft, hoping to go for a 1st Committee Draft (CD) ballot in mid 2013.
- If this occurs then, with luck, we could move to a Draft International Standard (DIS) ballot in late 2013, with publication in the first half of 2014.

What next?

- Every time a new draft is produced (in the SC27 6-monthly cycle) there is the opportunity for national bodies to make comments.
- These comments are reconciled and incorporated into the document at or after the internal meetings.
- If you are interested in getting involved, please work through your national standards body (e.g. ANSI in the US).

Contributions welcome!

- Necessary to get broadest possible consensus on the developing standard, so it is of maximal use.
- I welcome all input as editor, so please email me (at me@chrismitchell.net) if you are interested in getting involved in reviewing and/or providing input.
- I maintain a small mailing list ...

Acknowledgements

- I would like to thank the organisers of event for giving me the opportunity to make this presentation.
- I must also thank John Phillips of Microsoft, and Microsoft itself, for their support.

ANNEX

DATA PROTECTION LEGISLATION IN UK/EU

UK Data Protection Act 1998

- The UK Data Protection Act 1998 is derived from and implements the EU Data Protection Directive (95/46/EC)
- The UK Data Protection Act 1998 requires data controllers to comply with eight data protection principles, summarized as follows, which require personal information to be:
  - 1st principle – Fairly and lawfully processed;
  - 2nd principle – Obtained only for specified purposes and not further processed in a manner incompatible with those purposes;
  - 3rd principle – Adequate, relevant and not excessive;
  - 4th principle – Accurate and up-to-date;
  - 5th principle – Not kept for longer than is necessary;
  - 6th principle – Processed in line with the rights afforded to individuals under the legislation, including the right of subject access;
  - 7th principle – Kept secure;
  - 8th principle – Not transferred to countries outside the European Economic Area (EEA)) without adequate protection.

EU/UK Data Protection Act principles
Personal information shall be (part 1):

Principle	Applies to the PII controller?	Applies to the PII processor?
1. Fairly and lawfully processed	**YES**	**NO**: the controller takes the decision and instructs the processor.
2. Obtained only for specified purposes and not further processed in a manner incompatible with those purposes	**YES**	**NO**: the controller obtains the personal information and decides the purpose of processing.
3. Adequate, relevant and not excessive	**YES**	**NO**: the controller takes the decision on what personal information to hold.
4. Accurate and up-to-date	**YES**	**NO**: the controller keeps personal information accurate and up-to-date; the processor does not know what the data means.

Note: Some of this is simplified. There are some cases where "**Applies to the PII processor?**" is **NO** but in practice the PII processor has to provide some information to the PII controller or implement some specific capability. ISO/IEC 27018 takes account of these situations.

EU/UK Data Protection Act principles
Personal information shall be (part 2):

Principle	Applies to the PII controller?	Applies to the PII processor?
5. Not kept for longer than is necessary	**YES**	**NO**: the controller takes the decision and instructs the processor.
6. Processed in line with the rights afforded to individuals under the legislation, including the right of subject access	**YES**	**NO**: the controller takes the decision and instructs the processor; the controller provides subjects with contact point and access.
7. Kept secure	**YES**	**YES**: the processor must also keep personal information secure.
8. Not transferred to countries outside the European Economic Area (EEA)) without adequate protection	**YES**	**YES**: the processor states where personal information may be stored and the controller decides whether or not to use the processor's service.

Note: Some of this is simplified. There are some cases where "**Applies to the PII processor?**" is **NO** but in practice the PII processor has to provide some information to the PII controller or implement some specific capability. ISO/IEC 27018 takes account of these situations.