Project N°: 262608

Acronym: Data without Boundaries

DELIVERABLE D3.3

(Research Data Centers and ISO27001 – A Guide)

WORK PACKAGE 3

(Enhancing legal, information security and researcher accreditation frameworks for access to data)

REPORTING PERIOD:	From: Month 18	TO: Month 48
PROJECT START DATE:	1st May 2011	DURATION: 48 Months
DATE OF ISSUE OF DELIVERABLE:	March 2015	
DOCUMENT PREPARED BY:	Partners 24, 6, 9 and 18	ONS, NSD, IAB, UKDA

Combination of CP & CSA project funded by the European Community
Under the programme "FP7 - SP4 Capacities"
Priority 1.1.3: European Social Science Data Archives and remote access to Official Statistics

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 262608 (DwB - Data without Boundaries).

Table of Contents

Chapter 1 – Implementation Guide to ISO 27001 9

1.1 Management Commitment and Support 11
1.2 Develop a Plan 12
1.3 Understand the Standard 12
1.4 Management Processes 14
1.5 Define Scope 15
1.6 ISMS Policy 17
1.7 Risk Assessment and Risk Management 17

Chapter 2 - Risks, and risk management 25

2.1 Risk components 25
2.2 Risk Treatment 26
2.3 Data controls 28
2.4 User controls 32
2.5 Environment controls 37
2.6 Gap Analysis 47
2.7 Certification 47

Chapter 3 - Case Study - The UKDA experience 48

3.1 Why choose ISO 27001 certification? 52
3.2 Elements of certification 53
3.3 Achieving certification 57
3.4 Cost of implementing against benefits gained 62
3.5 Alternatives to ISO 27001 63
3.6 Concluding remarks 66

Chapter 4 - Recommendations 67

Practical implementation recommendations: 69

Chapter 5 - Summary 70

References 74

Annex A. Control/security measure requirements 76

Acknowledgements

The report was prepared by Trond Pedersen (NSD), Paul Wearn (ONS), Richard Welpton (UKDA), Atle Alvheim (NSD), David Schiller (IAB) and Paul Jackson (ONS).

Early versions of this report have been discussed during meetings in Bergen July 13.2013 and in Essex November 12. 2013.

The authors gratefully acknowledge feedback from Mus Ahmet (UKDA) and James Noel (ECSC) at the Essex meeting.

Preface

The ideals of evidence-based policy making and the Information Society generates a constant need for knowledge production, and the most relevant knowledge of such kind is generated through research. The research community plays an important role in stimulating policy analysis and debate and assessing the effectiveness of government programs. Research needs data, and good and relevant data become the single most important component necessary to build a science-based understanding of the functioning of the modern society.

Well-developed official statistical systems combined with a variety of both academically and commercially driven data gathering programs and research projects are producing a wealth of data and information about various aspects of the European societies. However, through this system of data production runs a dividing line. Although data from the official statistical system is of great relevance and interest for research purposes, access is regulated because the data are collected and collection is justified for other purposes than strict research. Data produced by the statistical system are protected and access is prohibited through intricate arrangements, combining judicial, economic, technological and practical retrieval-related factors. Data are locked in systems, fenced by rigorous rules, sometimes treated as an economic commodity, not being adequately documented and often not being intended for flexible alternative use.

In the majority of European countries social science data archives have been established to facilitate efficient dissemination and to secure the longer-term preservation of large parts of the available data resources. Data archives are institutions that do not to any significant degree collect data themselves, they are broker institutions established mainly to preserve and make available for potential use what others may have collected. However, as broker institutions these archives are also highly dependent upon the legal, institutional, collaborative and technical frameworks for their efficient functioning.

There are significant difference in focus between production oriented statistical authorities and dissemination oriented data archives, contrasting the focus on law and confidence, risk assessment and data protection against the focus on scientific relevance, analytic use and cost-benefit terms. To build efficient and relevant bridges across this divide there is need for rules, systems, capacity and confidence. And to build confidence, the most important factor is information security.

The scope of this deliverable is to present a framework for the design and management of an ISO27001 compliant information security standard, where the target users are European research data access centers. For the most part, this means national statistical institutes (NSIs) and national data archives (DAs). The ISO27001 standard is a generic process/lifecycle oriented information security management system (ISMS) which can be used across all sorts of businesses. We will therefore focus on the known desirable features of research data access centers when reviewing the security standard and present an implementation guide.

Production related activities are basically outside the security related concerns, although we need to know the details of why and how it is done. Many National Statistics Offices include access to microdata as one of their dissemination activities, placing the role alongside their core function of dissemination of statistics. Those statistics offices that retain access to microdata functions are in a position to extend their corporate information security controls to include the activity of access to microdata. Other National Statistics Offices (NSOs) separate the dissemination of statistics from providing access to microdata, delegating the latter role to a partner such as a data archive or research data centre. Such a delegation is possible only when the partner is known to manage the data to equivalent information security standards. One of the purposes of this guide is to enable potential dissemination partners of NSOs - data archives and research data centers - achieve a recognisably high standard of information security and gain the trust of the NSO.

The most important components of an information security management system (ISMS) for handling and deposit of data so that confidentiality is protected are:

- Physical barriers
- Technological barriers
- Good routines/management

To summarize, the known desirable features related to European research data access centers need to be seen from two perspectives:

Secure storage and appropriate handling of research data, to build confidence and maintain quality of resources
Efficient law-abiding data sharing and dissemination, through appropriate information systems and transparent and clear access policies

One may argue that quality of data depends on good routines for documentation and curation/preparation/preservation and that we should single this out as a third desirable feature. However, as our focus lies on the information security aspect, we choose to play down this component.

This implementation guide will use the two desirable features mentioned as a backdrop in the discussion of suitable security measures (referred to as controls in the ISO27001) and -routines. Clearly, high level of security on one hand and easy access to research data on the other may not be compatible. The solution is to seek a balance. Such a balance must in any case be consistent with current rules and regulations.

Some organisation may have already achieved ISO27001 accreditation or a standard based on this. For such organisations this document can be seen as a benchmark or health check so they can measure themselves against it. Others may be starting from scratch and would see this as

an implementation manual, when trying to establish the international standards and key features of using statistical data and establish rules and regulations for movement of data.

The report highlight the risks elements, mainly distinguishing (1) careless loss and unintended malicious behaviour from (2) malicious breaches for statistics and data crossing borders. There are different players and two ends to such a process. Risk is minimized through agreed standards and tight security, but empirically the most efficient component of bringing down unwanted incidents goes through educating the user.

This deliverable ensures a consistent approach to information security across borders. Consistency and transparency will lead to a circle of trust which leads to a pathway for data to cross boundaries through a network of equivalent services, where partnerships can be built on commonly adopted standards and grow organically.

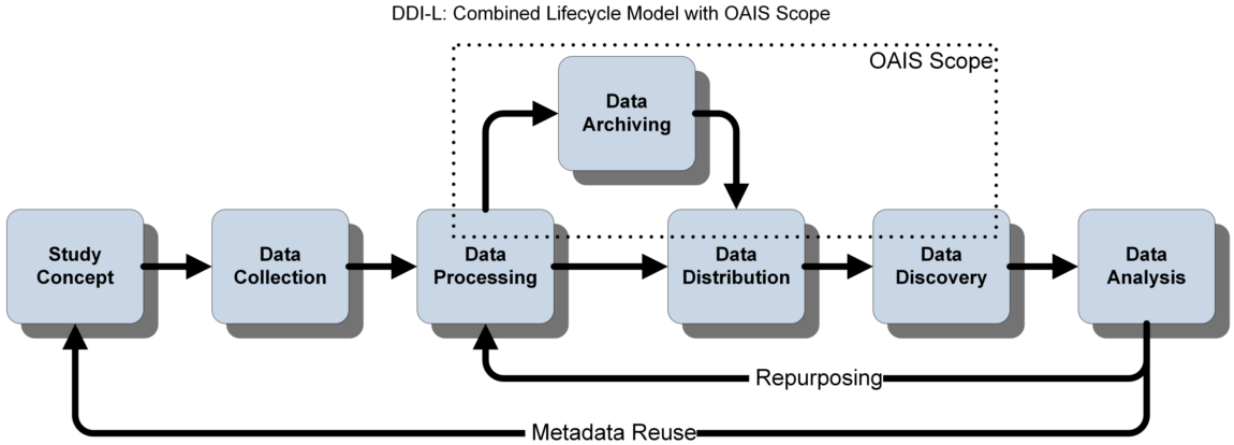
The overall aim of the report is to encourage an adoption of a common understanding of information security.

Chapter 1 – Implementation Guide to ISO 27001

Introduction

If we use the DDI Lifecycle model and the OAIS Reference model as tools to illustrate, a research data access facility may be defined as an OAIS, an *Open Archival Information System,* an institution that picks up the data when they are already produced and quality checked and from there on takes responsibility for data maintenance in all its user-oriented aspects, discovery and dissemination processes and management of long term curation of such resources.

Figure 1: An illustration of the research process and parts covered by research data access facilities[1].



Defining the "research data access facility" as the same as the OAIS could be somewhat simplistic, since we reduce it to integrating parallel production tracks that are ingesting and storing their data in parallel ways into specialised institutions aiming to support research use. Reversely, the neutrality of the OAIS framework do not see much relevant difference between types of production lines, and in reality the difference of the production lines, technology employed and justifications given for data collection, most likely will be of significant

[1] This illustration is copied from the UK Data Archive website. It refers to the UK Data Archive work on integrating the DDI Lifecycle perspective in appropriate data documentation procedures.

importance for what kind of data maintenance and dissemination culture institutions develop. What we are trying to say is that data security could be handled according to the same set of principles and the same systematic procedures across different producers and production systems and could function to build down such differences.

ISO27001 states that "…the organisation shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS within the context of the organisation's overall business activities and the risk it faces…", in other words it's important to start off by identifying the core business activities and assets in addition to estimate the risks involved.

According to the introductory chapter of ISO27001, the adapting of an ISMS such as ISO27001 should be a strategic decision depending on the needs, objectives, security requirements and the size and structure of an organisation. Small problems need simple solutions, while the complex ones require a more widespread solution.

The main ISO27001 clauses 4.2.1 a)-i) states that the organisation shall define the scope, an ISMS policy and a risk assessment approach, identify, analyse and evaluate the risks, identify, evaluate options for, select control objectives and controls for treatment of risks, in addition to obtain management approval of the proposed residual risks as well as authorization to implement and operate the ISMS.

Finally, the organisation shall according to clause 4.2.1 j) prepare a Statement of Applicability (SoA) which lists the control objects and controls selected and the reason for their selection, the control objectives and controls currently implemented, and also the excluded control objects and controls from the list in Annex A and the justification for their exclusion. The SoA will serve as a summary of decisions concerning risk treatment.

Lloyd's Register Quality Assurance Ltd (LRQA) has developed a list of 10 points containing the steps needed to meet the requirements of the ISO27001:

- Management Commitment and Support
- Develop a Plan
- Understand the Standard
- Management Processes
- Define Scope
- ISMS Policy
- Risk Assessment and Risk Management
- Risk Treatment
- Gap Analysis
- Certification

We will review all the steps listed, and adjust the requirements to the relevant business cases (OAIS will be used as business reference model), key assets and scopes of a typical European research data access centre. When talking about research data access centers, we are basically discussing NSIs and DAs. As NSIs have a broader role than disseminating data compared to DAs, we will not analyse the business as a whole, but focus on data management and dissemination. The business of data ingestion (data collection/data production) will be considered outside the scope of this deliverable.

1.1 Management Commitment and Support

Ideally, the motivation and direction fostering and guiding security policy will come from top management. As implementing an ISO27001 compliant ISMS may be time and resource demanding process, success will come more easily if, at the very least, management understands the reasons for implementing an ISMS and fully support its design and operation.

1.2 Develop a Plan

Success is more likely with a meaningful and realistic plan, making it possible to measure performance against the plan and then be prepared to change it in the event of unforeseen circumstances.

It is important to have a cost-benefit evaluation in mind when planning to implement the ISMS. One can choose to implement the ISMS only for critical business areas, and exclude parts as long as it does not compromise the information security. As an example, one can implement an ISMS covering the research data access facilities only, while other facilities like meeting rooms, cafeterias, receptions etc may be outside the scope. However, it is vital to have plausible reasons for such judgments, and to make sure information security is not influenced significantly.

1.3 Understand the Standard

As with any project, to implement an ISMS a prospective user needs to familiarise himself with the standard, understand the criteria that have to be met, the structure of the standard and hence the structure of the ISMS and associated documentation.

The ISO27001 standard is a generic process/lifecycle oriented information security management system (ISMS) which can be used across all sorts of businesses. It is considered as a specification of best practice for an ISMS. The main part of the standard is relatively short (12 pages), with the following 3 components:

- Introduction and scope description
- How to implement the ISMS
- In-depth description on management roles and responsibilities

In this ISMS framework all except the introductory part is regarded as mandatory requirements (needed for an institution to be ISO27001 accredited).

As security measures are central aspects of any ISMS, those listed in Annex A of the ISO27001 standard are important to get familiar with. The various measures listed cover most aspects of a relevant ISMS. The list is based upon common practices in connection with information security, and is intended as a menu. The extent of security measures will naturally depend on the needs of the respective institutions, therefore a user does not have to pick all of the measures from the list. This is also stressed in the ISO27001 document. The minimum requirement is that all relevant legal and contractual obligations are covered. The supplementary ISO27002 is a code of practice for information security and is meant to be used as an implementation support. It contains a broad list of controls or measures related to information security, i.e. those already listed in the Annex A of ISO27001, but goes more into detail in the explanatory part as well as giving recommendations on practical implementation (almost like a manual). Central concepts are “control objectives” and “controls”, what needs to be protected and how to protect it.

It is worth noting that the generic nature of the ISO27001, and the fact that the required documents produced as output may be in any form or type of medium, implies that a satisfactory ISMS implementation does not necessarily mean that a user has to start from scratch. Some organisations may already have or be on the way towards an ISO27001 compliant ISMS without knowing it. However, a prospective user must ensure that all the requirements are covered and adjusting existing procedures may be as resource consuming as developing new ones.

The documentation shall include records of management decisions, in addition to the following:

- Documented statements on the ISMS policy and objectives
- General specification of the scope

- Procedures and controls in support of the ISMS
- Description of the risk assessment methodology
- Risk assessment report
- Risk treatment plan
- Procedures needed to ensure effective planning, operation and control, and description of how to measure the effectiveness of controls
- Records required by the standard (Document conformity with requirements and the effective operation of the ISMS. Examples: “Visitors’ log”, audit reports and completed access authorization forms)
- The Statement of Applicability containing a list of the selected control objectives and controls, and the reasons for their selection. In addition, one must also list what is already implemented, as well as the exclusions and justification for their exclusion.

All the documents listed above may be in any format or type of medium.

1.4 Management Processes

These processes are critical to the effective implementation of an ISMS:

- Top management have significant impact on the effectiveness of the management system. Adequate resources (people, equipment, time and money) should be allocated to development, implementation and monitoring of the ISMS
- Internal audits verify that the management system is operating as intended and identifies opportunities for improvement
- Management review provides the opportunity for top management to assess how well the management system is operating and supporting the business

Obtaining management approval of proposed residual risks, and authorization to implement and operate the ISMS is required.

Central elements are monitoring, reviewing and controls to detect errors, identify attempted security breaches, determine whether actions taken were effective, measuring the effectiveness of controls etc. In addition, reviewing risk assessments and conduct ISMS audits at planned intervals.

Implementing identified improvements in the ISMS and ensuring that the improvements achieve their intended objectives etc

1.5 Define Scope

It is essential that the logical and geographical scope of the ISMS is accurately defined, so that the boundaries of the information security system and security responsibilities can be identified.

Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organisation, its location, assets and technology, including justifications for any exclusion from the scope.

Business area:

- Data production (of limited relevance, i.e. outside immediate scope, but significantly dependent upon institutional legitimacy)
- Data management and archival storage (relevant)
- Data processing (relevant)
- Administration/management (relevant)
- Data dissemination (highly relevant)
    - Aggregates/tabulations for general publication
    - Anonymized public use files (PUFs)
    - Anonymized scientific use files (SUFs)
    - Licensed files (requires specific permissions)

- Onsite data laboratories, closed environments
- Remote Access facilities
- Remote Execution facilities

As already mentioned in chapter 1.2, an organisation can chose to implement an ISMS only for selected business areas while keeping the remaining businesses outside the scope. DAs and NSI typically operate with separate sections divided by topic area and type of service. Pure IT-related services as well as methodological departments may be held outside the scope. The same goes for support services (cantinas, receptions, maintenance etc). The typical scope would be critical businesses related to handling, storage and dissemination of research data and technical systems supporting such business activities.

As the main businesses/objectives/goals of a research data centre is to provide quality research data for research purposes, **the key asset will naturally consist of research data**. We may distinguish different types of data:

- Aggregate statistics (tables), i.e. publication ready anonymised data or data on non-human primary units.
- Micro level survey data, data collected primarily for research or statistical use.
- Micro level register data, reuse of data primarily collected for or generated through alternative administrative processes.

No matter what type of data, safeguarding data confidentiality is essential from a legal point of view. Confidentiality is also important for building trust, between institutions and between the data access facility and the population. The national laws and regulations set the premises for confidentiality. If data confidentiality is convincingly secured, trust will be built both national and international.

It is essential for a research data access centre to secure the following key assets:

- Research data
- Confidentiality

- Trust

The scope of such access centers should be to have an ISMS that make the organisation able to handle, archive and disseminate research data in an appropriate, i.e. an efficient and secure way, so that confidentiality is secured and confidence built. The laws and regulations set the premises. However, good security routines are in themselves important in order to build trust, even though they are not strictly required in the legal sense of the word. Therefore, it might be instrumental to go beyond the legal requirements. However, as an important mission is to provide easy access to quality data for research purposes, institutions should try to balance the need for security against the researchers needs.

1.6 ISMS Policy

Define an ISMS policy in terms of the characteristics of the business, the organisation, its location, assets and technology.

Define an ISMS policy that includes a framework for setting objectives and establishes overall sense of direction and principles for action with regard to information security, and takes into account business, legal, regulatory and contractual requirements.

The policy is all about formulating principles and rules for protecting the research data. As most research data centers have well implemented security measures, the task will be to formulate principles that are followed on a general level. This will go some more further than defining the scope.

1.7 Risk Assessment and Risk Management

The risk assessment is the foundation on which an ISMS is built. It provides the focus for the implementation of security controls and ensures that such measures are applied where they are most needed and most cost effective.

The process should consider the threats and vulnerabilities associated with the assets and the impact of their exploitation. It is necessary to determine the level of risk and identify the controls to be implemented to manage those risks.

- Identify a suitable risk assessment methodology
- Develop criteria for accepting risks and identify acceptable levels of risk
- Identify the risks, i.e. the assets and asset owners, threats to those assets, vulnerabilities and possible impacts
- Analyse and evaluate the risks
- Evaluate options for treatment of risks:
    - Applying appropriate controls
    - Accepting risks (within the risk accepting criteria)
    - Avoiding risks
    - Transferring risks to other parties (outsourcing)

In the context of research data access centers, a risk assessment should focus on risks associated with the business of processing, archiving and dissemination of micro level research data.

There are a number of possible risks that can do damage to an organisation's key assets, in our case research data: Hacking, disclosure (with or without intention), computer virus, break in, fire, earthquakes, loss of knowledge due to staff turnover, technical failure, loss of data or metadata, misinformation etc.

Examples of risk assessment methodologies are discussed in ISO/IEC TR 13335-3, *Information technology – Guidelines for the management of IT Security – Techniques for the management of IT security*

OCTAVE Allegro

OCTAVE Allegro is a risk assessment method which we highly recommend. It focuses primarily on information assets in the context of how they are used, where they are stored, transported, and processed, and how they are exposed to threats, vulnerabilities, and disruptions as a result. It is a very user friendly method, and the technical report describing OCTAVE Allegro presents a set of forms to use under the risk assessment process. One of the purposes is to help the user keeping the assessment on a non-abstract/practical level. The method operates with the terms *information assets* and *information containers*. Containers are places where information assets are stored, transported, and processed. By controlling the containers, the user also controls the information. People may also be regarded as information containers according to OCTAVE Allegro.

The risk assessment steps of OCTAVE Allegro:

1. Establish risk measurement criteria: Identify relevant impact areas such as reputation, and define what constitutes hence low, medium and high impact to the organisation's business. Rank the impact areas by importance.

2. Develop an information asset profile: Identify information assets that are regarded as critical to the organisation's mission/business, as well as those that are important due to regulatory compliance. The selected assets, if compromised, should have an adverse impact on the organization's business if one of the following occurred:

    a. The asset were disclosed to unauthorised people
    b. The asset were modified without authorization
    c. The asset were lost or destroyed
    d. Access to the asset was interrupted

    Perform a record/check of which type of security requirements are relevant for each asset from the following list (perform a rank based on requirement importance afterwards):

    - Confidentiality, including who has authorization to view this information asset
    - Integrity, including who has authorization to modify this information asset
    - Availability, including who this asset must be available for in order to secure the business. Also timeframe should be specified.
    - Other, such as regulatory compliance protection requirements, including specification

3. Identify information asset containers: Map where the information assets are stored, transported, and processed. According to OCTAVE Allegro, the risk to the containers are inherited by the information asset. The containers are divided into technical containers, physical locations and people in one dimension, and between internal (under direct control of the organisation) and external in the other dimension

4. Identify areas of concern: Identify possible weakness areas related to an information asset

5. Identify threat scenarios: Use a so called threat tree as a tool to present a more detailed threat description. Start with threat category (suggestion: human actors using technical means, human actors using physical means, technical problems, and other problems) and then use branches to go more and more into detail

6. Identify risks: risk can be formulated as en equation:

   Risk = Threat + Impact

   By mapping the impact (=consequence) of all the threat scenarios listed, we will have all the input needed in order to complete the risk assessment.

7. Analyse risks: Put an impact value for each threat scenario based on the risk measurement criteria formulated in step 1. Start with each threat scenario/consequence and put a value (low, moderate, high) for each impact area (defined in step 1). Compute a risk score for each impact area by multiplying the impact area rank by the impact value, and then total the score to produce a relative risk score that serve as tool to prioritise the control implementation.

8. Select mitigation approach: For each risk, chose to either accept (relevant if low impact), mitigate (relevant if medium to high impact) or defer (decision put on hold due to need for more information/additional analysis, not an imminent threat or with significant impact). There are two ways of mitigating risks:

   a. Avoiding risk through appropriate controls
   b. Limit risk through strategies to limit the adverse impact if risk is realized

Typically, both a. and b. will be chosen depending on the cost of implementing the appropriate control. Such cost must always be balanced against the value of the asset and the potential impact. The mitigation may result in residual risk which one can choose to either accept or mitigate further.

One may also use a "Relative Risk Matrix" as a prioritisation tool. This is a table with adds threat probability as an extra dimension (in addition to risk score). Both risk score and probability are grouped into three categories (low, medium, high). By doing it this way, the criteria for mitigating will be the pool of risks placed in the group with the highest relative risk score and the highest threat probabilities.

The last phase of step 8 is to choose suitable security measures/controls related to each risk identified through step 1-8 that is chosen to be mitigated. This is naturally the most interesting part from the perspective of this deliverable. The strategy suggested by OCTAVE Allegro:

1) For each risk, note the container(s) in which the control will be implemented
2) Describe the control to be implemented and any residual risk to the asset once the control is implemented

In relation to the process of archiving, maintenance and dissemination of data, there are two important types of risks a serious research data access centre has to deal with:

- Loss of data (the data itself)
- Loss of confidentiality (the data content)

Loss of data can be related to loss of data containers due to theft, disasters etc, or to data corruption due to system errors, virus attacks, misuse, bad routines and similar. Data corruption implies both loss/destruction of data and unwanted altering/tampering of data (breach of data integrity).

Loss of confidentiality refers to the internal side (employees) as well as the external (data users or possible third parties (service providers)).

There are several sources of risks that we have to deal with. One way of operationalizing is to use the Ritchie[2] security model which divide the overall data security into four risk areas related to a use situation that may be controlled/manipulated to minimize risk:

a) The data
b) The data output (analytical outcomes/derived product)
c) The user
d) The practical/technical environment

Although all risk areas need to be controlled to some extent, good control mechanisms in one area may lead to a lower required security level in another area. In other words, the security areas are interrelated. As an example: If the data themselves are regarded as unidentifiable (anonymized), then the areas b) through d) may not be that relevant to control.

In real life there is no such thing as unidentifiable data. Through various ad hoc methods such as web browsing as well as merging with other data sources through identifiers or variable values (statistical/indirect merging), one can find more information about the individuals in a data set and ultimately manage to identify indirectly. Therefore there will always be need for some level of user control (c) in addition to the more general need for a secure technical environment (d).

[2] Ritchie F. (2011) *Provision of ONS data for analysis: safe use, not safe data*, mimeo, Office for National Statistics, June; or, Office for National Statistics (2011) *Data Access Policy*, July.

Ritchie F. (2011) *Secure Data Service Risk Assessment*, mimeo, Office for National Statistics

Ritchie F. (2013) "International access to restricted data: A principles-based standards approach". *Statistical Journal of the IAOS* v29:4 pp 289-300. DOI 10.3233/SJI-130780

Ritchie F. "*Designing a national model of data access*" 2009, mimeo, Tokyo-HIT Extended version of SJIAOS paper, including discussion of decision-making process

From a confidentiality point of view, the areas a) and b) is all about disclosure control. To secure the data itself or the data analytical outputs are more or less the same. We are talking about different ways of protecting the confidentiality of individuals represented by the data. If it is the output or the actual data doesn't matter much, the problem at hand will be the same: How do we protect individuals from being identified? The components a) and b) could therefore be discussed and treated as one, due to their similarity. Naturally, the risk of data loss will not be controlled through managing the risk areas a) and b), and may be regarded as irrelevant in this context.

The Ritchie security model regards information security as a product across (at least) four to seven components involved in a use situation, with factors varying in strength:

1. Input: Secure data, usually regarded as a question of data anonymisation. If we anonymize the data, we solve most of the problem. This technology is common for sample-based data.
2. Output: Secure results, control to hinder those analytical results can be used to identify individuals in the data matrix, rules for number of IO in a table cell. This is the way we treat analytical outcomes when they are published to the general public.
3. Secure analytical techniques, some analytical technologies are more "dangerous" than others; cross-tables are more dangerous than a single regression coefficient.
4. Users: Secure institutions: the legal tendency to identify responsibility, institutions may be made responsible for their employees.
5. Secure projects: Quality of actual research projects, only projects of some academic quality are allowed to access data.
6. Secure researchers: Authorization of single researchers, only professionally qualified researchers are authorized for certain types of data use.
7. Technology: Secure situation (technology and communication). Access is dependent upon a secure user environment.

Such a security model could be implemented in many varieties. The problem is to define a combination that give acceptable security of data use at the same time as it gives acceptable user flexibility and access to rich collections of data. The empirically based conclusion is that educating the user is the single most efficient action to promote secure use of data and in many countries therefore focus is on legal control and authorization of projects and users since it is close to impossible to develop a purely technical security solution. Most practical solutions therefore is a combination where users responsibility for the situation and potential sanctions against individuals, projects or institutions fills in as a major part completing the picture. To get a functioning security model for data use, building circles of trust and awareness of sanctions seems to be the most efficient way to go.

Chapter 2 - Risks, and risk management

Introduction

Building on a systematic security model combining trust with technology, we need to specify sets of rules or policies for the major components. What data should be available, what categories of users are legitimate and what rules should be formulated for analytic outputs. Then we may specify rules for who will be allowed to do what on which data and link analysis of related risks to such a paradigm.

2.1 Risk areas/components. What type of risks is there and what risks do we face?

- ***The environment (safe environment)***
    - Storage mediums and other relevant types of equipment used to store/handle the data (PCs, servers, software, etc)
    - The surroundings (offices, storage rooms, buildings etc)
    - Systems related to the physical security, incl. the equipment/system security
    - Type of access (remote access, safe rooms, etc)

- ***Disclosure (safe data)***
    - It's all about systems, i.e. systems to secure confidentiality
        - Working routines
        - Software
        - IT-security
        - Systems related to protections of confidentiality

- ***The human factor (safe users)***
    - Users/researchers
        - Unawareness
        - Lack of knowledge

- Employees at research data centres
  - Unawareness
  - Lack of knowledge

These three components are related/interconnected: Good measures in one area leads to lower risk factors in the other areas.

2.2 Risk Treatment

The risk assessment identifies risk levels which are then compared with the acceptable level of risk determined by the organisation's security policy. Once they have been determined, implement controls to mitigate these risks.

Clause 4.2.2 in ISO27001 presents a list of operational requirements. This includes formulating and implementing a risk treatment plan, implementing the selected controls, implementing training and awareness programmes, manage operation of the ISMS etc.

The ISO27001 standard consistently operates with the terms "control objectives" and "controls", meaning hence "*what* the organisation seeks to control" and "*how* to control it". For each of the 39 control objectives in Annex A, there are multiple controls to choose from. As the list is not exhaustive, the user is free to consider additional controls objectives and controls.

The control objectives and controls in Annex A/ISO27002 are organized in the following 11 main areas:

a) Security policy

b) Organisation of information security

c) Asset management

d) Human resources security

e) Physical and environmental security

f) Communications and operations management

g) Access control

h) Information systems acquisition, development and maintenance

i) Information security incident management

j) Business continuity management

k) Compliance

As an overview of what kinds of security measures ISO27001 covers, a synopsis of all objectives and objective controls are presented in Annex A, presented in an easy-to-read fashion.

The controls presented in the standard cover most of the need for information security related to the business of archiving, handling/processing/curation and dissemination of data. However, as the standard is generic, not all measures will be equally important/ relevant. In addition, the range of measures tend to be technically oriented and not that focused on methodology related to disclosure control. We will therefore introduce more specific controls in this area than the standard has to offer.

There is a broad specter of controls that should be considered when mitigating the risk of either disclosure or loss of data. As discussed in chapter 1.7, this deliverable will use a simplified version of the Ritchie security model as a framework for the categorization of possible controls to consider. The two components “safe data” and “safe output” both require controls/techniques for anonymization, whether we are talking about the data itself or the derived analytic output presented to the user/researcher, and will therefore be treated as one. Our model therefore consists of three components:

- The data (the actual data and derived output)
- The user (employees/ data providers or data users/ researchers)
- The practical/technical environment (the surroundings, equipment, systems etc)

2.3 Data controls

The measures discussed here is all about systems for disclosure control, and the risk needed to be controlled is breach of confidentiality as a consequence of viewing the data or data output. We take no position on whether the user is authorised or not, or if the information system has a satisfactory security level, but take this as granted. Those issues are dealt with in chapter 2.4 and 2.5 respectively.

Disclosure revealed through looking at the data may be controlled using various types of methodological anonymization techniques. In addition, good working procedures are also necessary in order to make sure that the necessary disclosure control measures are implemented properly.

As the ISO27001 standard is somewhat technical oriented, controls related to disclosure have minimal coverage. In order to secure confidentiality in a proper and systematically way when dealing with microdata, we recommend following the guidelines described in this chapter. Most of them are not to be found among the list of relevant/commonly used controls in ISO27002. This chapter should therefore be seen as an addition to the standard.

2.3.1 Methodological techniques

In most cases of data dissemination, and especially for PUFs and SUFs, there is a need for control of microdata to prevent disclosure. Confidentiality breaches may occur either through looking at the actual microdata, or through various types of data analysis output such as cross tables.

There are disclosure risks related to both direct and indirect identifiers. Direct identifiers are variables that contain precise and unique information about statistical units so that there is no doubt about the source for the associated information. Examples are personal id-numbers or social insurance numbers, names, and addresses. Indirect identifiers require more analysis than

just observing single variable values, but may however be a tool for disclosure through the use of combinations of variable values. A basic rule is that a variable is more identifiable the more detailed and the more visible the information is. Visibility may not necessarily apply to the visual aspect only, but also to the “searchability” through web tools such as Google.

There are a number of anonymization methods that can be considered to use on sensitive variables:

- Recoding
- Local suppression
- Post-randomization
- Microaggregation
- Adding noise
- Shuffling

Recoding and local suppression are non-perturbative methods which require manual considerations. The idea behind the first one is to combine value categories into new less informative categories. For continuous variables one can group values in order to discretize. Local suppression is a method in which censoring of values is performed. For instance, income amounts over a certain limit may be set to a fixed threshold value to prevent disclosure through the use of publicly available income sources. Typically, such censoring is performed upon extreme values that are considered unique and thereby a potential risk element that needs to be controlled.

There are also a range of automatic disclosure control methods to consider, also called perturbation methods. What they have in common is that real values are manipulated through the use of various types of randomization or aggregation methods. The idea is to inflict a random type noise to ensure that some level of uncertainty is inflicted, making it hard to identify a given individual at 100% certainty, while at the same time maintaining the original distribution.

Post-randomization is a probabilistic method that can be applied to categorical variables. The values of a variable are then changed into other categories by using pre-defined transition probabilities stored in a transition matrix. This manipulation is applied to each observation independently and randomly, which ensures different outcomes for each execution as long as no seed has been specified for the random number generator.

Microaggregation is a more straightforward solution with some similarities to the recoding method. However, microaggregation is typically applied to continuous variables. The idea is to replace original values with mean values or values derived from other arithmetic calculations. These calculations are performed on groups of records, and all values within each group are aggregated in such way. This serves as a form of aggregation as well as having an element of randomization.

Another way of anonymizing continuous variables is to add stochastic noise to the original data. Uncorrelated noise will preserve means, but variances and correlation coefficients between variables are not preserved. The solution to this is using correlated noise methods, i.e. noise derived from a distribution having a covariance matrix proportional to the covariance matrix of the original microdata. It is possible to add noise only to outliers as an alternative.

A more complex method is the use of shuffling, which will maintain all the original values, but in a rearranged order. The method can be summarized in the following steps:

1. Rank original variable values
2. Rank values of generated variable used to simulate the original variable
3. For all observations, replace the value of the generated variable with rank *i* with the original variable value with rank *i*
4. After completion of the value swap, the generated variable will contain only original values, but in a different order, and can be used to replace the original sensitive variable.

Before making decisions on with methodological solution(s) to use, it is recommended to enforce restrictions on the number of variables that are made available for dissemination for a specific research project, based on a need-to-know principle. Also limitations on population size could be considered, using random sampling.

If perturbation/randomization of data can be avoided through restrictions on variables and population size, and through the use of manual methods such as recoding and local suppression, as well as microaggregation, this will be preferable to most researchers as this will maintain the original data distribution. As researchers strive to describe and analyse real life causalities, an implication of this is that *real* data are preferable compared to synthetic data. However, perturbation techniques have some advantages as seen from the researcher perspective, and may be considered as a preferable option under the right conditions. For instance, more variables and observations can be made available, and on a more detailed information level, without risking confidentiality breaches. If the number of key variables are high, this automatically leads to a high number of unique combinations. In such cases perturbation techniques may be the only solution.

Recommended anonymization guidelines

1. Carefully choose the set of key variables, i.e. direct or indirect identifiable variables, using knowledge of both subject matter experts and disclosure control experts
2. Perform a frequency and risk estimation to evaluate how many observations have a high risk of disclosure given the selection of key variables.
3. Apply recoding to reduce uniqueness given the set of categorical key variables. Alternatively, data swapping may be considered.
4. Consider local suppression if recoding is used, to achieve a satisfactory level of anonymity. *k*-anonymity can be used as a measure. The parameter *k* is often set to 3.
5. Apply microaggregation to continuously scaled key variables. This will automatically provide *k*-anonymity for these variables.

6. Quantify the data utility of the microdata set (or output table) after the disclosure limitation methods have been applied, using typical estimates such as quantiles or correlations, as well as benchmarking indicators.

Most of the material in this subchapter, including the recommended anonymization guidelines, is taken from Templ et al. (2014). For more details and reference to further more literature of relevance, refer to this paper.

2.3.2 Working procedures

In addition to the actual anonymization manipulation of the data, there has to be good working routines in place to ensure that the risk of disclosure is minimized on a day-to-day basis.

It is recommended to have at least one employee with expertise in the methodological area in order to control the important security aspect of statistical disclosure. Expertise can be attained through employing or knowledge-building (education, courses, literature research etc).

Guidelines concerning statistical disclosure measures should be documented and made easily available for all employees having access to microdata. This includes a clear understanding or definition of which type of variables that are considered to be problematic in relation to confidentiality.

In addition to guidelines, forums or meetings should be held from time to time in order to exchange experience and to build knowledge about statistical disclosure.

2.4 User controls

There are two types of users of research microdata placed on each side of the table: The employees at the data centers (the data providers) and the data users (mainly researchers). The employees use the data mainly for archiving purposes and for processing prior to dissemination

of data, while researchers use the data as input in their analysis. Either way, the risks related to the use of data are essentially the same: Confidentiality breaches may arise from unawareness or carelessness, from lack of knowledge about legal or contractual requirements, or from people with bad intent. The last factor may not be that relevant in relation to employees, but still it is worth mentioning as a possible risk factor.

The measures discussed in relation to user controls are covered mainly by the part of ISO27002 that describes human resources security (Annex A, chapter d)), but also other parts of the standard are relevant in this context (Annex A, chapters f) and g)).

Relevant control objectives along with the corresponding chapters found in Annex A:
- Human resources security (d)
- Operational procedures and responsibilities (f)
- Practical user access management (g)
- User responsibilities (g)

2.4.1 Unawareness/carelessness/lack of knowledge

Risk resulting from unawareness/carelessness or just plain lack of knowledge may be controlled or minimized through:

- Internals (data providers):
    - Good documented working routines
    - Training programmes/courses
    - Frequent staff meetings (to exchange experience/knowledge)
    - Ensure sufficient competence when employing new staff
    - Transparency (incl. the legal requirements)
    - Authorization

- Externals:
    - Providing guidelines and other practical requirements (incl. legal requirements) when giving users access to data
    - Fines/penalty
    - Courses/training programmes
    - Accreditation
    - Verification/identification

The idea behind the concept “safe user” is that risk of disclosure may be controlled and minimized through a limitation of the type of users that are allowed to use the micro data. It is common to operate with a list of approved institutions of which only associated researchers are allowed to have access to micro data. By following such practice, there is some sort of guarantee that the researcher is serious. This will ensure that knowledge of relevant laws and regulations are in place, and that there is an understanding of what disclosure means as well as the implications and individual and institutional sanctions related. Moreover, experience and routines for safe handling of microdata will minimize the risk for disclosure through carelessness. A system for such accreditation should therefore be implemented.

It is not enough that a researcher is associated with an approved institution. The data access centre has to be sure that the user is who he says he is. Keywords here are identification and verification. A signed data request letter or emails using the official email address associated with the institution (not private or gmail-type addresses) will typically serve as identification/ verification. Meetings face to face are even better, but may often be difficult to practice.

Independent of the user itself, one has to make sure that all relevant laws and regulations are fully understood. There is no guarantee that an experienced researcher fully understands what it takes to secure confidentiality and the implications of disclosure. Therefore one has to communicate all requirements related to safe handling and use of the research data before the user is allowed to access it. This includes recommended practical arrangements and guidelines, as well as reference to all relevant laws and regulations. The latter may be in full text or just

referenced to. However, a summary version of the most important/relevant parts of official laws and regulations will help the user understand his responsibilities. The user must also sign an agreement that he has understood all requirements (practical and juridical), as well as a non-disclosure declaration. This applies also to data that are anonymized (SUF), as there is always some risk that people may be identified through various techniques (web browsing, advanced technological techniques, statistical matching etc). Data that are fully anonymized (PUF) do not require any type of user control as the risk of disclosure is non-existent. In addition to information about requirements in relation to actual data requests, it is recommended that these also are published on the data access centre's website in an understandable and easy-to-find way.

Other ways to control external users are to practice fines or other types of sanctions. Examples of punishments could be to impose a time limited ban of the person or the responsible institution, or to publish a list of those involved in disclosure episodes. Courses and training programmes may also be a good way to ensure proper use of research microdata. These can be held by external organisations or by the data access centre.

Disclosure risks associated with external users applies to the output data only, that is the data that are prepared and anonymized by the data access centre (direct access to licenced unanonymized microdata may also be an option, but this requires an extra set of legal requirements to be satisfied).

There is also a disclosure risk associated with the internal use of microdata. Employees at data access centers that are archiving, documenting, and processing such data are dependent on good documented working routines to ensure that disclosure may not be at risk. Otherwise there is room for individual interpretation of what is considered satisfactory or not. Training, courses, security briefings and meetings to exchange knowledge and experience are also important in order to ensure that the employees have proper competence in the data security field. The employment process should also involve knowledge about information security as

one of the relevant/required competence components. Terms and conditions stating responsibilities for information security should be agreed and signed.

Authorization is a tool to control that only the right people are given access to the various types of microdata. Employees should only be subject to authorization to handle data that are necessary in order to perform their individual work tasks. This ensures correct allocation of competence, but it also makes it easier to manage information security, as the number of people responsible for security operations is limited. There should be checks to verify that the level of access granted is appropriate to the business purpose, and privileges should be allocated to users on a need-to-use basis only.

User passwords should be handled in a correct way. This implies the following:
Employees should sign a statement to keep personal passwords confidential
Implemented procedures to ensure that passwords should not be stored on unprotected computer systems or in any other easily available forms (notes etc)

2.4.2 Bad intent

Authentication/authorization/accreditation may be used as a tool to ensure that only those with a legitimate need for data access are given permission to inspect or use the data. By doing this, one can eliminated a major part of the threat of disclosure posed by people with bad intent. Bear in mind that researchers are only interested in the bigger picture, not single individuals. By making sure that only researchers of a given professional qualification and motivation are allowed access to data, this type of threat will be dealt with and risks reduced.

Information about all relevant laws and regulations, including the implications of breaches, is necessary in order to ensure that there is no doubt neither in the user community nor in the public about the importance of confidentiality. This serves also as a way of building trust. Such information should be made easily available and visible, preferably on the data access centre's

websites. Information about sanctions/fines/penalties or other consequences should also be documented and presented in order to deter from intentional disclosure attempts.

2.5 Environment controls

Even though there are proper controls covering the data aspect and the user side, this is not sufficient unless the environment has a certain level of security attached. There are three types of environment that should be controlled in order to protect the data stored and handled by a data access centre. What may come first are the data containers. This is the mediums in which the data are stored or processed. These can be electronically, physical, or even human form. Secondly, we have the surroundings of the data containers such as facilities, offices, locations, and support equipment. Except from disasters (fire, earthquake etc), damages or breaches into the surroundings do not in itself pose a direct threat to the data, but will most certain enhance the risk level significantly. A third component is the overall information security management. The safety of the environment is highly dependent upon how the information security is managed.

The measures discussed in relation to environment controls has a broad coverage in the ISO27002 standard, as they are described in most of the sections (refer to Annex A, chapters c), and e) through j)).

2.5.1 Data container security

As discussed, data containers may be in form of electronical devices or storage/backup medias, physical form such as printouts or notes, or as human knowledge. All these types of containers need to be controlled in order to protect from data loss or disclosure. *Control* in this context typically means barriers to ensure secure storing or processing/handling of data, and to avoid unauthorised access to microdata.

Controls for data containers in form of human knowledge can be regarded as a subset of *user controls*. Relevant measures covering this dimension are therefore to be found in chapter 2.4.

There are a range of possible controls to consider. These are control objectives of relevance from the ISO27002 standard, along with the corresponding chapters found in Annex A:

- Asset management (c)
- Equipment security (e)
- Backup (f)
- Media handling (f)
- Maintain security of exchanged information (f)
- User responsibilities (g)
- Application and information access control (g)
- Security related to mobile computing and teleworking (g)
- Ensure correct processing in applications (h)
- Cryptographic controls (h)

There are several ways of storing/archiving data, but the most common practice among data access centers is to have a large amount of servers used for such purpose. In addition, CDs, memory sticks, hard disks (portable or stationary), even diskettes are used for various purposes: To transport data between users or equipment, for backup purposes, or for safe storage (separate from networks). Printouts must also be considered as data containers in need for security.

Not only is it necessary to control the containers used for storage or transportation purposes, but a data access centre also use the microdata within the processing system on a broad scale. All the involved software, hardware or processing applications using the relevant microdata/information as input should therefore be included when considering security measures. We will discuss this component further on in this chapter.

Data container management

An important security aspect is to have a proper management to assure that all relevant data containers are managed in a secure way. The first thing to do is to make an inventory of all important containers. This will help to provide an overview of the scope of the information security system, but also serve as a tool to recover from disasters or other malfunctions. Such a list should include all information necessary in order to perform a successful recovery, covering container type, format, location, backup information, licence information, and business value. In addition, responsibility should be allocated to ensure proper handling of the respective data containers. Each employee's responsibility area(s) can be attached to a business process or a defined set of activities, an application, or a defined set of data. Rules and guidelines for acceptable operations on/use of the various data containers should also be stated and communicated to all employees. Such guidelines could cover acceptable rules or restrictions on email or internet usage, and use outside the premises.

To ensure appropriate level of information protection, each employee should perform a systematical information classification for all relevant data containers under his responsibility area(s) using a fixed scale, as well as defining appropriate access restrictions. The classification should reflect business value, legal requirements, sensitivity, and criticality. This classification should be manifested through clear marking/labeling of all relevant data containers, especially for those classified with the highest rating. The marking/labeling must be performed on both electronic and physical container formats.

Data container security

In order to prevent damage to, or loss of data containers like servers, PCs, hard disks, CDs etc, it is vital to implement and maintain a set of measures and guidelines so that the risk of such events are minimized.

First of all, containers should be sited so that the risk of unauthorised access is minimized. For instance, information processing facilities like PCs should be positioned so that the risk of

information being viewed by unauthorised people during their use are as low as possible. Items requiring special protection should be isolated (locked in) when not attended, and offline. Typically this applies to containers of sensitive and/or direct identifiable data (via personal id, name, address etc).

All microdata should be protected by electronic barriers to ensure that only authorised people are allowed access to it. This means implementing good login and password procedures. For instance, PCs should be automatically locked after a period of inactivity, requiring a password to reopen.

Containers/equipment taken out of the premises should never be left unattended in public places due to the risk of theft. In addition, off-site use of data containers should not be allowed without strict authorization, and time-limited only. An off-site policy or a set of guidelines should be communicated to ensure everybody knows the correct working procedures. These should include a definition of work permitted and what type of information that may be held. A good practice is to completely avoid working on identifiable microdata when off-site, especially in public spaces. Extra care should be taken when working in public spaces, due to the risk of unauthorised remote access (hacking), overlooking, or virus attacks.

A clear desk policy should be maintained, both at the data access centers premises, and when working at home. Such policy implies that portable containers of microdata or confidential information, including written notes or printouts, should not be easily available to unauthorised people when unattended. Similarly, identifiable or sensitive information should not be left on printing facilities for others to see. Guidelines for good login/logout/ lock screen/password practice should also be implemented, and the staff should be reminded of such regularly.

All types of data containers should be returned, and access rights should be removed upon termination of employment.

Backup and media handling

In case of data loss or breaches to the data integrity due to operational errors, hacking/viruses, or disasters, it is essential to perform routinely backup of all microdata at fixed intervals or after significant changes made to the data processing or support system. Containers of such backup must be located in a completely safe external environment, i.e. outside the premises of the data access centre with appropriate level of physical protection. Without such remote backup, valuable microdata may be lost forever in case of disasters like fires, sabotage/breaking, water damage etc.

The necessary level of backup should be clearly defined, and the extent and frequency should reflect the business requirements and security requirements. In addition, accurate records of backup copies as well as restoration procedures must be kept. The integrity of the backup data should be tested regularly due to the fact that CDs have limited life span and that new data processing software may not be compatible with older ones. Sensitive backup data should be protected by encryption.

Disposal of media when no longer required should be done in a secure way, using formal procedures. Containers of confidential or sensitive microdata should be physically destroyed, or the content must be deleted and overwritten, so that the information is non-retrievable.

Secure data dissemination

A key business area of data access centers is to disseminate research data, and it's important that this is done in an efficient and secure way. Data may be disseminated through CDs, emails, internet, remote access facilities, or onsite data laboratories, and may have different levels of risks attached.

Public use files (PUFs) are considered fully anonymized and security measures in this case are not necessary. Typically this is aggregated data, but also microdata (individual level) may be

considered as PUFs as long as it is impossible to identify individuals through any means. Such files are therefore suitable for direct downloading through internet.

Scientific use files (SUFs) are anonymized data also, but there might be a possibility that disclosure can occur through statistical matching or combining with (ad hoc) information found on the internet. Care should therefore be taken when disseminating such data. In practice, SUFs should be treated as (identifiable) licenced files from an information security perspective. Licenced files typically consist of a large amount of detailed variables (and individuals), which makes it easy to identify individuals through combination of variables values. However, this extra risk is controlled formally/juridical through various types of permissions that the user must have in place before he are given access to the data. Nevertheless, data access centers still have a responsibility and obligation according to laws and regulations to make sure that all necessary security measures are implemented. Both SUFs and licenced files are typically disseminated through CD-transfers, personal handouts or onsite data laboratories, or remote access facilities. Email transfers may also be considered for SUFs, but special care should be taken dependent on the level of disclosure risk attached to the data. Cryptographic controls may be considered as a measure to prevent others to open transfer files should they come in wrong hands.

Formal exchange policies and procedures should be established to ensure correct transfer of microdata from the data access centre to the user, covering all types of communication facilities and transfer methods. The transfer procedures should be communicated to the data user to prevent misunderstandings. Measures to be considered: Cryptographic techniques, use of trusted personal couriers, use of mail packages, personal handouts only, ensuring correct addressing (both physical and electronic (email)) etc.

As onsite data laboratories and remote access facilities are controlled mainly through the use of safe surroundings, related security measures will be discussed in chapter 2.5.2.

Secure data processing

The data integrity may be compromised due to processing errors, and in the worst case microdata can even be lost (if no backup of the actual data is performed). The ISO27002 suggest several ways of dealing with this type of risk.

The design and implementation of applications should ensure that the risk of processing failures leading to loss of data integrity are minimized, e.g. one could consider limiting the use of add, modify and delete functions, prevent programs from running in the wrong order or running after a failure has occurred. Such measures should depend on the business impact of corruption of data.

Applications should be able to detect any corruption of information through processing errors or deliberate acts.

A manual evaluation of data output should be performed by the application operator, to check for errors caused by the data processing or potential errors in the input data.

2.5.2 Surroundings security

Safe surroundings are equally important as protecting the data containers themselves. Without a certain level of overall security, there will be a risk of exposing the data containers for unfortunate events that may lead to data loss or disclosure. Security measures in the following areas are necessary to consider:

- Location/safe site (offices, storage rooms, buildings etc)
- Physical security, incl. the equipment/system security
- Operational or support systems

These are control objectives of relevance from the ISO27002 standard, along with the corresponding chapters found in Annex A:

- Secure areas (e)
- Operational procedures and responsibilities (f)
- Protection against malicious code (f)
- Network security management (f)
- Monitoring (f)
- Network access control (g)
- Operating system access control (g)
- Security related to mobile computing and teleworking (g)
- Ensure security of system files (h)
- Security related to development of application system software (h)

The building should be physically secured and only authorised personnel be given access to the building. Electronic card control should be considered, with checkpoints in areas containing sensitive information. When working with sensitive information the use of photographic, video, or audio recording should be prohibited.

Research data access centers containing onsite laboratories should consider safe rooms. Such rooms should, in practice, have video surveillance in place to avoid unsupervised working practices.

Operating procedures should specify instructions for the detailed execution of each job including processing, handling and backup of information, recovery procedures in case of system failure, and implementing support contract.

There should be good procedures in place for the transfer of software from the development phase to operational status. Tests and checks should be performed to see if the version is ready for use. Such tests should be performed on separate domains and computers, and not tested on sensitive data. This is to avoid disclosure or unintentional data loss.

A formal policy should be established to protect against risks associated with obtaining files and software through external networks. In order to protect against malicious code, virus scans should be performed on a regular basis on networks, emails and webpages.

Special controls to protect confidentiality and integrity of data passing over public networks or wireless networks, as well as the connected systems and applications should be in place. These controls should include measures like network access control and cryptographic controls. It is recommended to use logging and monitoring to prevent unauthorised activities. The system should be monitored by keeping audit logs that includes information on user IDs, date/time of key events, terminal identity, and various information on system and application use.

The use of network services should be consistent with an established access control policy, which should include appropriate authentication methods to control access by remote users.

It is recommended to segregate the network according to the different security levels of the stored information. The purpose is to control damage to the network caused by data corruption and to ensure a proper differentiation of security based upon the risk assessment.

A useful way to evaluate the network security could be to perform penetration testing. These can be conducted by third parties to make the procedure independent and more realistic.

2.5.3 Management measures

In order to complete the information security system, there has to be a good management in place to ensure that all necessary procedures are implemented, reviewed, tested, audited, and monitored.

These are control objectives of relevance from the ISO27002 standard, along with the corresponding chapters found in Annex A:

- Monitoring third party service delivery (f)

- System planning and acceptance (f)
- Business requirement for access control (g)
- Ensure that security is an integral part of information systems (h)
- Technical vulnerability management (h)
- Proper reporting of information security events and weaknesses (i)
- Ensure consistent and effective handling of information security incidents (i)
- Business continuity management (j)

Statements of business requirements for new information systems or enhancements to existing information systems should specify the requirements for security controls. These controls should be evaluated as early as possible in the process of acquisition, development or enhancement of information systems. The security requirements should reflect the business value of the information involved, as well as the potential business damage caused by failure or absence of security.

Technical vulnerability management procedures should be implemented to reduce risks resulting from technical weaknesses. The list of data containers produced in relation to the data container management should be a prerequisite for such evaluations. Required information should include software vendor, version numbers, current software installed, and the person(s) responsible for the deployment of the software. Identified vulnerabilities should be treated by appropriate measures to address the associated risk. Depending on how urgently the risk needs to be addressed, the action could be carried out according to established updating procedures or implemented incident response routines (refer to Annex A, chapter i)).

It is recommended to implement good procedures for reporting of security events that may occur, as well as having effective incident response procedures. A good practice is to ensure that all employees are made aware of their responsibility to report incidents as quickly as possible. Management responsibilities should be established so that security issues are handled effectively. Actions should be taken according to a set of guidelines describing continuity plans,

incident analysis, containment, type of actions etc. Incident management is an important tool for a continuous improvement of the ISMS, and is therefore an essential security measure.

Major failures of information systems or disasters can result in interruptions to the business processes. Therefore it is essential to have continuity plans in place to minimize the disruption caused by such events.

Business continuity plans should identify all data containers involved in critical business processes. The degree of impact that incidents may have on the business should be analyzed in order to prioritize the implementation of appropriate preventive controls. Backups and use of alternative temporary locations are measures that may be considered (refer to Annex A, chapter j) for more details). Business continuity plans should be maintained and tested to ensure they are up to date and effective.

2.6 Gap Analysis

This assessor delivered activity offers the opportunity to focus on critical, high risk or weak areas of your system in order to create a certifiable system. It can also look at how existing management systems or procedures can be used within your chosen standard.

2.7 Certification

Certification is an external assessment of the management system, to ensure that it meets the requirements of ISO 27001. It is typically a two stage process consisting of a system appraisal and an initial assessment, the duration of which is dependent on the size and nature of the organisation.

Chapter 3 - Case Study - The UKDA experience[3]

This chapter presents the experience of the UK Data Archive (hereafter referred to as 'the Archive') in implementing and achieving certification for the international information security standard, ISO 27001[4]. The content may also be found in a separate paper (Welpton (2014)) made as a contribution to this deliverable.

Scope

This document presents an overview of the experience of the Archive in implementing the information security standard, ISO 27001.

Definition of Terms

ISO 27000 Group of Standards

An internationally recognised framework for implementing and maintaining information security standards.

ISO 27001

The specific standard which provides a model for establishing, implementing, operating, monitoring, reviewing and maintaining an Information Security Management System (ISMS). (ISO 27003 provides guidance in implementing an ISMS.)

[3] This chapter is produced by Richard Welpton, Secure Lab Manager, UKDA Richard Welpton gratefully acknowledge comments from Matthew Wollard, Hilary Beedham and Herve L'Hours

[4] This chapter specifically discusses ISO 27001:2005, and not ISO 27001:2013, a recent revision of the standard. Organisations currently certified to ISO 27001:2005 which wish to retain certification must comply with the new version by 2015.

[4]The British Standards Institute have published a guide: *Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013*. Available at: http://www.bsigroup.co.uk/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf.

Certification

Organisations that implement procedures to comply with ISO 27001, and are successfully audited against these by an accredited ISO 27001 auditor, will achieve 'certification'. Audit requirements and guidance are documented in ISO 27006 and ISO 27007.

Risk Register

A system for recording risks, measuring their impact and likelihood of occurring. The Risk Register should also contain remedial actions for mitigating the risk occurring.

Controlled Document

A UK Data Archive term to describe a document which contains a set of procedures describing a business operation. Controlled Documents are formally maintained and are reviewed as part of the ISMS.

ISMS (Information Security Management System)

Refers to the systems (procedures, committees, governance structures etc.) implemented by the Archive to ensure that information security protocols are upheld.

Roles and Responsibilities

Director of the Archive

Overall responsibility for Archive compliance for ISO 27001. Authority for some activities are explicitly delegated where appropriate.

ISMG (Information Security Management Group)

The ISMG has authority responsibility (delegated by the Director), for ensuring maintenance of ISMS, maintaining the Risk Register; preparing the Archive for ISO 27001 re-certification and regular audits; day-to-day assessment of new risks, threats, vulnerabilities; approving new or amendments to Controlled Documents relating to information security.

GOC (Governance Oversight Committee)

The GOC has authority responsibility (delegated by the Director) for approving new, or amendments to, Controlled Documents which do not relate to information security.

Section Managers

Section Managers are responsible for ensuring that staff in their sections are aware of their responsibilities for carrying out business operations in regard to their individual areas, particularly when handling confidential sources of data.

Archive staff

All members of staff at the Archive are responsible for ensuring security threats are minimised, and for carrying out approved procedures listed in relevant Controlled Documents. Staff should also make suggestions for improvements to procedures, and report observations (as these may help to improve procedures and reduce the risk of an information security event occuring), since they are part of the ISMS process.

Introduction

The Archive has been accredited for ISO 27001 for over four years now (each certification period is valid for 3 years subject to regular audit, and so the Archive has achieved initial certification once, and recertification in June 2013).

The Archive is the first academic department in the UK to have achieved ISO 271001 certification. In doing so, the Archive, via the UK Data Service, has been able to provide secure access to data deemed too confidential/sensitive to allow researchers to download. Certification to ISO 27001 has been instrumental in giving prospective data depositors of confidential/sensitive data additional confidence that the Archive can provide access to such data in a safe and secure manner.

Ensuring adequate information security measures are in place, reviewed and developed requires much time and devotion among Archive staff at all levels of seniority. ISO 27001 certification is considered a major asset to the Archive, particularly as data security continues to increase in importance in the UK data landscape. For example, the ESRC's Big Data Network, including the Administrative Data Research Network, focuses heavily on the implementation of data security measures.

While the process of developing and implementing information security measures would anyway be incorporated into our processes, ISO 27001 provides a formal framework by which these processes can be examined against, the results of which can easily be judged by data depositors.

This chapter presents a short overview of the Archive's experience in gaining certification to ISO 27001.

3.1 Why choose ISO 27001 certification?

For the Archive, achieving ISO 27001 certification is paramount to its ability to deliver access to data deemed too confidential or sensitive to allow researchers to download the data. These data are accessed in the Secure Lab, a secure enclave (a mechanism in which researchers log into an Archive server to access data, and undertake their research: consequently no data are ever downloaded from this server, and researchers receive statistical analysis from the server subject to confidentiality checks by Archive staff).

However, ISO certification covers the entire Archive and not just the systems that enable the Archive to deliver access to data via the Secure Lab. This is in part because the Secure Lab is not managed in isolation from other Archive activities. Access, user support, ingests processing, IT and human resource functions, to name but a few, all contribute to the successful running of the Secure Lab. Hence their activities will necessarily fall under the purview of the ISO 27001 framework.

From 2007, the Archive began implementing information security controls as laid out by ISO 27001, although at this time the Archive did not deliberately set out to gain certification. However, when the Secure Data Service (the predecessor of the Secure Lab) contract was drawn up by our funding body, the Economic and Social Research Council, a discussion about the most appropriate information security to benchmark to conclude that ISO 27001 was the obvious choice.

However, ISO certification is only one of a number of measures that are required in order to assure data depositors that the Archive can safely manage its confidential data collections. In addition to ISO 27001, a number of other 'certification measures' are met:

- A 'penetration' test (whereby an 'ethical hacker' is hired to evaluate Archive technical systems to discover 'weaknesses' and recommend areas that could be strengthened);
- Certification from the Department of Business, Innovation and Skills (BIS), the Government department responsible for certification of government IT systems, and

also the Government department that provides funding to the ESRC, the Archive's funding council;.

- Reviews from individual data depositors (who may have specific requirements for how their data are managed, in addition to ISO 27001)[5].
- Review of possible implementation of ISO 16363 for Trusted Digital Repositories
- Other activities designed to foster understanding and 'trust' in Archive processes (for example, courses in managing data, participation in the UK Research Data Centre Network, to name only two)

The above exercises are specifically focused on particular Archive business activities (for example, 'reviews' by individual data depositors tend to consider how the Archive manages non-technical elements of providing access to data, such as application procedures, statistical disclosure control of research outputs etc.

ISO 27001 is much broader in scope, and indeed this is one of its key advantages: by achieving certification, the Archive can assure data owners that its entire set of operations enables secure storage and transmission of all its data sources, and that the major risks of disclosure of potentially sensitive data are minimised. The next section provides more information about the areas of implementation covered by ISO 27001. However, certification to ISO 27001 should be seen as one of a number of measures implemented to ensure the Archive is considered a 'trusted source of data'.

3.2 Elements of certification

As mentioned previously, ISO 27001 examines a fairly broad array of business operations to ensure that data security measures are upheld. Figure 1 below illustrates the broad scope of ISO 27001:

[5] These reviews are collaborative information sharing exercises, intended to foster confidence between the Archive and its data depositors, and ensure that best practices are designed and implemented by both all parties, and ensure that data depositors trust the Archive to deliver confidential/sensitive data access securely.

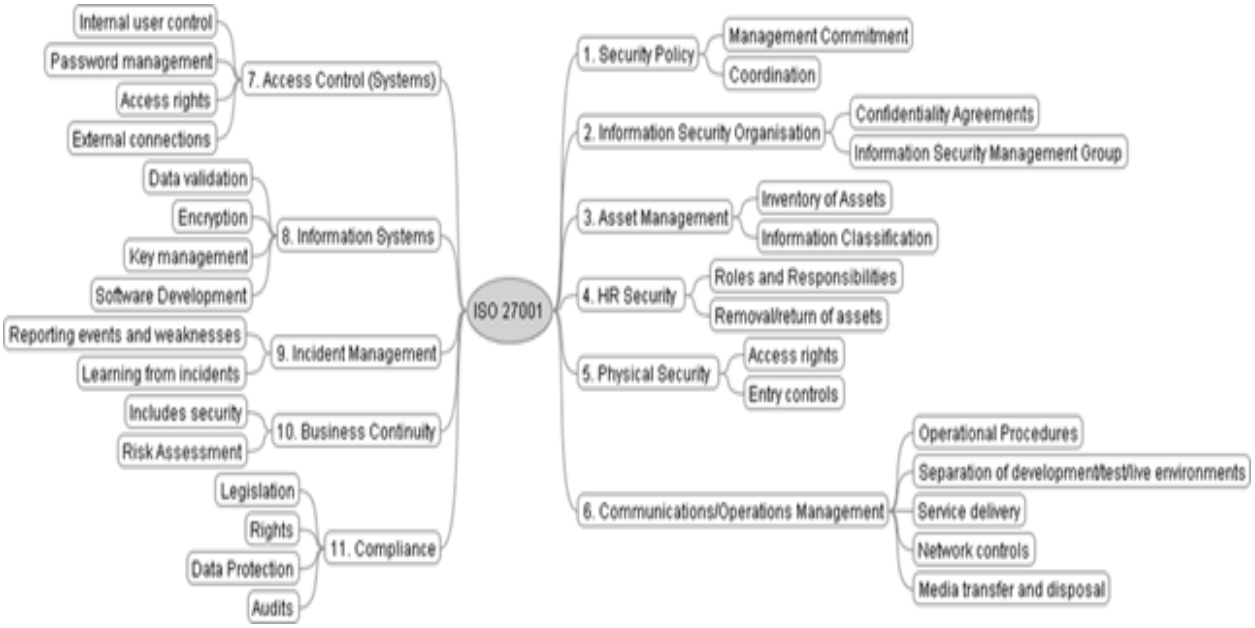


Figure 2: Overview of ISO 27001 framework

The eleven areas of ISO 27001 are now briefly described in the table below[6].

Table 1: Description of ISO 27001 framework

Element	Objective	Example
Security Policy	Ensuring management direction and support for information security	Does there exist an 'information security policy' document, approved by management, and communicated to staff?
Information Security Organisation	To ensure effective management of information security within the organisation	How is information security co-ordinated across the organisation? How is information security responsibilities divided? What are the risks relating to

[6] Adapted from "Information technology – Security techniques – Code of practice for information Security Management" ISO 27001 documentation

Element	Objective	Example
		external parties?
Asset Management	To achieve and maintain protection of organisation assets	Inventory of assets; ownership of assets; guidelines for classification; what system exists for information labelling and handling?
Human Resources Security	To ensure that organisation employees understand their information security responsibilities	Information security awareness, education and training; disciplinary process; screening of applicants for posts as part of Archive recruitment procedures
Physical Security	To prevent unauthorised access, damage, interference to the organisation's premises and information	What physical entry controls exist? Protection against external threats; secure disposal of equipment
Communications and Operations Management	Achieve appropriate and secure information processing facilities	How are operating procedures documented? How is capacity management controlled? What information handling procedures exist? What monitoring processes have been implemented?
Access Control	Ensure appropriate controls for information access are established and maintained	What User Access management exists? How are users identified and authenticated? What password management system is in place? Can networks be isolated?

Element	Objective	Example
Information Systems	Integrating security into information systems	Restrictions on changes to software packages; control of operational software; protection of system data; what cryptographic controls are in place?
Incident Management	To ensure that information security events and weaknesses are communicated and that corrective action is taken	How are information security events reported? Roles and responsibilities for investigating security events? How are corrective actions implemented and monitored?
Business Continuity	To counteract interruptions to business processes from effects of major failures of information systems or disasters and ensure their timely resumption	What is included on the Risk Register? What business continuity plans have been developed in response to possible disasters? Evidence that disaster recovery plans have been tested
Compliance	Avoid breaches of legal, statutory, regulatory or contractual obligations	Identification of application legislation; data protection and privacy of personal information; what information security audit controls are in place?

The examples above are but a very small set of 'controls' included in ISO 27001 requirements, and are intended merely to illustrate the depth and breadth of the certification.

3.3 Achieving certification

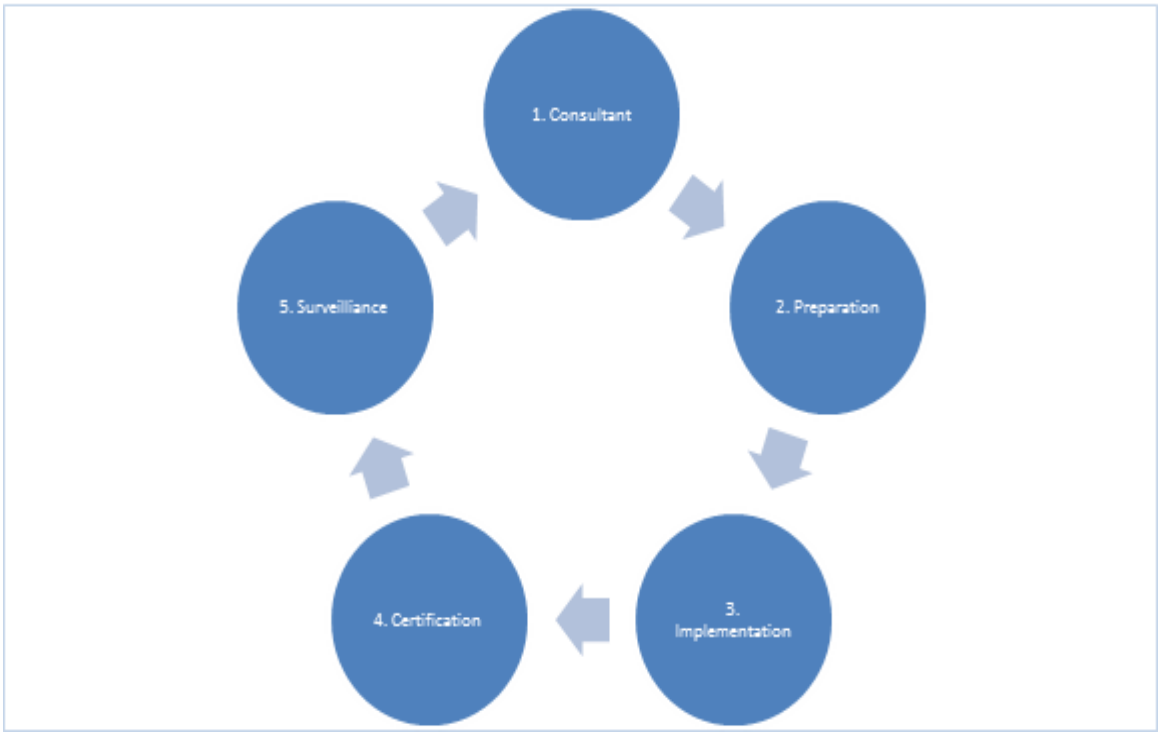
Our experience of achieving certification for ISO 27001 has been mixed, because the Archive did not have to start from scratch: many procedures relating to the above elements already existed, although perhaps not formally, or perhaps from a different context. Many of these procedures did require extensive review and modification, and so despite not necessarily beginning from a blank sheet, considerable effort was demanded of Archive staff at all levels.

To aid the process of certification, the Archive hired a firm of consultants to advise us on:

- Our current state of readiness
- Steps to ensure compliance with ISO 27001

The process of achieving initial certification, and ensuring continued certification, is illustrated below:

Figure 3: Lifecycle of ISO 27001 certification



The steps are explained as follows:

	Objective	**Example**
Consultant	To advise on state of readiness for certification; actions required to achieve certification	What procedures are already in place?
Preparation	Setting up an ISMS, oversight from ISMG; delegation of responsibility to Archive section managers for ensuring compliance from their areas; ensuring documentation in place to demonstrate compliance	Buy in from senior management required; buy-in from all staff required (requires support); creating an environment of security awareness. To achieve the above, the following were undertaken: Risk Assessment Analysis Internal Audit Corrective Action Plan (for which implementation was managed formally as an internal Archive project)
Implementation	Ensure procedures are in place and can be tested; create Risk Register to identify risks and how these can be controlled	Ensure that business operations are not impeded by controls; communication to staff about why ISO 27001 is required
Certification	To ensure compliance with ISO 27001	

	Objective	Example
Surveillance	6-monthly 'surveillance' audits conducted by the external ISO auditor to ensure compliance with controls	An opportunity to demonstrate 'continuous improvement': What procedures could be improved upon? Actions to be taken, implementation of new or improved procedures. Implemented for further certification.

The concept of 'continuous improvement' is important terminology widely used in ISO 27001 (and other standards too). Accredited institutions should foster an atmosphere of security-consciousness, and staff throughout the organisation should actively consider how procedures can be improved to prevent security lapses.

With regard to certification and the six-monthly 'surveillance' audits, the external auditor will visit the Archive and randomly assess a business area, but must ensure that the elements (see previous section) are all met. Before visiting the Archive, the auditor will request a list of procedures (written into 'Controlled Documents') and can ask to see that the procedures listed in a particular controlled document are being undertaken. When making an assessment, the following classifications are made:

- Observation
- Minor non-conformity
- Major non-conformity

An 'observation' indicates that the auditor has identified a procedure which works, but for which an improvement can be made. A 'minor non-conformity' occurs where a part of one of the 'elements' is not being met, and a 'major non-conformity' indicates that an entire element

is missing. It should be noted that an auditor who decides that a minor or major non-conformity is present will deny certification. Depending upon the seriousness of the non-conformity, the auditor will specify measures to be undertaken to ensure compliance, and provide a set amount of time in which 'corrective actions' should be implemented (known as the Corrective Action Plan).

The next part of this section describes the organisation arrangements for ensuring compliance with ISO 27001.

3.3.1 Structures

The Archive has established two committees to oversee compliance with ISO 27001:

- Governance Oversight Committee (GOC)
- Information Security Management Group (ISMG)

GOC is made up of a number of Archive section managers (to ensure there is Archive buy-in at a broad level), and is responsible for approving procedures (as set out in Controlled Documents) within the Archive which are not specifically related to information or data security. Examples include proposed changes to data access licences.

ISMG is a smaller group that takes responsibility for approving Controlled Documents with information and data security implications. The ISMG also prepares the Archive for re-certification and ensuring auditor recommendations are implemented. ISMG also meets quarterly and discusses the following:

- Review of internal auditing
- Review of incidents (and recommendations to ensure prevention)
- Changes to the Risk Register
- Legal/regulatory changes that may affect the Archive

ISMG also meet in addition to these meetings as required, and can invite other Archive staff to attend if necessary to discuss particular issues that may affect the ISMS.

3.3.2 Assessment of Risk

An effective ISMS is founded upon the identification and assessment of risk. There are many risks facing the Archive, for example, threats and vulnerabilities of IT hardware and software, premises etc. The business operations of the Archive can also contain risks, and as new operations are introduced (or existing procedures amended) so new threats and vulnerabilities can be identified and addressed.

Managing risk is therefore a necessary routine, and the framework of an ISMS should enable risks to be assessed and mitigated. The creation and maintenance of a Risk Register has proved to be an easy and informative approach to identifying and managing risk. This is reviewed at least quarterly by the ISMG, but can also be amended as needed.

Assessing risk in business operations underpins the system of Controlled Documents, whereby a proposal to introduce or alter a procedure is assessed (by GOC or ISMG, see above), to consider whether a risk is being introduced.

Items may be added to the Risk Register and assessed in terms of their likelihood of occurring and the impact to the Archive should the risk be realised. A numerical score allows the Archive to measure and categorise the seriousness and threat of the risk (which may be reduced given stated measures to mitigate the risk).

The process of managing risk should not be underestimated in terms of resources required. ISMG work proactively to review new potential threats and vulnerabilities to the Archive on a day-to-day basis. These potential threats and vulnerabilities arise from many different sources including (but certainly not limited to):

- Developments in technology (e.g. recent releases of internet browser applications exposed security gaps for which the Archive have addressed)

- Changes in working practices (e.g. increased demand for staff to work from home/remotely, sharing knowledge amongst partner UK Data Service institutions)
- Changes to the legal environment in which the Archive operates (such as changes in European data protection legislation)

Such issues appear as a regular agenda item at ISMG meetings, but in addition must be addressed as they are raised. The Archive must, to comply with its ISO 27001 certification, demonstrate how these issues have been considered and addressed.

3.4 Cost of implementing against benefits gained

Achieving certification of ISO 27001 is not a trivial task. Archive staff spend a significant amount of time ensuring operations comply with the elements of ISO 27001, and consider methods by which procedures can be improved. However, the relatively recent organisation of the GOC and ISMG structures, and the streamlining of management for Controlled Documents, has reduced the cost/burden of ensuring compliance and continuous improvement.

It must be emphasised that without the certification, the Archive would not contractually be permitted to hold and provide secure access to, the confidential sources of data that it can. In this sense, the benefits to the Archive accruing from ISO 27001 certification far outweigh the costs of implementation. However, there is no real reason why an organisation without receiving certification should not be trusted to do the same. However, certification inspires confidence, increases trust, and promulgates awareness across the organisation. It is the Director's opinion that the cost of implementation and certification is little more in real terms than the cost of implementation alone, and the benefits accrued by additional certification outweigh those additional costs.

More generally, the UK data landscape is increasingly changing and becoming shaped by organisations that maintain 'safe settings' for data, and those that do not. As more sources of confidential data are considered for access, and with an increase in public consultation about

the use of personal data, so organisations that can demonstrate competence with handling confidential data find themselves in positions of advantage. Indeed, one of the 'visions' of the UK Data Service is to maintain a status as a 'trusted source of data', and ensuring that we operate 'safe settings' is an important avenue for achieving this status.

This said, one issue about ISO 27001 auditing that the Archive has recently addressed is the 'relevance' to providing access to confidential/sensitive data, through the Secure Lab. Previously, audits did not examine closely the procedures in place for managing access to these data, or for managing data, user accounts etc. within the Secure Lab environment. As a result, data depositors who supply the Archive with confidential/sensitive data have visited the Archive to undertake their own audits'. This should not be encouraged due to the duplication of resources. The external ISO 27001 audit should prevent any duplication of effort in governance.

The reason for accrediting to ISO 27001 originally was to ensure the Archive could store and disseminate secure access to confidential/sensitive data. That the original audits did not scrutinise these operations too closely, resulting in further audits from data depositors, implied further resources were used for auditing than were necessary. The Archive should bear the costs of certification to ensure it can hold and disseminate access to these data, but in a way which is efficient given the limited resources of the Archive.

3.5 Alternatives to ISO 27001

This paper has provided a brief overview of the Archive's experience of implementing the necessary controls to achieve certification of ISO 27001, including a summary of the benefits and the costs incurred to achieve certification.

However, alternative standards do exist which should also be considered before a judgment on ISO 27001 can be made.

3.5.1 ISO 16363 Trusted Digital Repositories

A relevant set of controls for the storage and provision of access to confidential data is ISO 16363 Trusted Digital Repositories standard (hereafter TDR[7]). This standard sets out a number of criteria which accredited institutions should adhere to, and include:

- Organisational infrastructure relating to preservation of data
- Digital Object management
- Technical infrastructure and security risk management

The latter of these criteria clearly have considerable overlap with principles of ISO 27001, although perhaps not as extensively as the set of controls included in ISO 27001.

The Archive has already undertaken a test audit against ISO 16363 as part of the EU-funded APARSEN project[8]. At the time of writing this standard has no formal auditing mechanism which means that it is impossible to be certified against this standard. However organisations wishing to apply the controls described by the standard can do so on an informal basis.

3.5.2 Internal Government security standards

Research Data Centers (RDC) providing access to confidential sources of micro-data from within UK government departments comply with security standards set by CESG (the Communications-Electronics Security Group of the National Technical Authority for Information Assurance)[9].

[7] [1] I am grateful for Hervé L'Hours for providing me with information about this standard, including the metrics and audit specifications. More information about compliance with this standard can be found at http://public.ccsds.org/publications/archive/652x0m1.pdf

[8] D33.1B Report on Peer Review of Digital Repositories. Available at: http://www.alliancepermanentaccess.org/wp-content/plugins/download-monitor/download.php?id=D33.1A+Report+on+Peer+Review+of+Digital+Repositories

[9] My thanks to Daniele Bega, HMRC Datalab Manager, for providing useful references. The CESG framework, recently updated, is available to download. Download at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/299556/HMG_Security_Policy_Framework_v11.0_doc.pdf

All government departments must adhere to these standards and by virtue of location within a government department, an RDC located in one of these departments will necessarily comply with the standards.

Broadly, the standard covers risk management from a technical perspective. Many of the controls contained within the CESG framework are also included in ISO 27001. However, an RDC, such as the HMRC Datalab (which is the RDC based at the UK government department that collects tax revenue) is not required to meet ISO 27001 because it complies with the CESG requirements. This scenario is almost certainly true of other RDCs that are located within government departments.

3.5.3 Meeting security controls without formal certification

It is possible that an organisation can meet security requirements (controls), without receiving formal certification. For instance, an organisation could implement an ISMS, document procedures and demonstrate continuous improvement by conducting internal audits, without receiving certification to one of the standards mentioned above (indeed the Archive originally undertook this, see Section 2).

However, the benefit of undertaking formal certification with the accompanying auditing requirements is the ability to demonstrate continuous improvement through audit compliance and the implementation of recommended audit outcomes. The resulting certification assures current and prospective data depositors who supply the Archive with confidential data for dissemination of access, enabling smoother negotiations and increasing our ability to maintain our status as a 'trusted source of data'. One could argue therefore that implementing a robust ISMS without formal certification to a recognised standard is not actually an alternative given the benefits which certification confers.

In particular, certification to a formal standard (not necessarily ISO 27001 specifically), necessarily requires the development, implementation and review of 'quality' procedures (i.e.

procedures that have been formally considered, tested and reviewed as 'fit for purpose'). Indeed, compliance with a formal framework often leads to:

- improvement in work processes
- ability to meet contractual obligation (e.g. with data depositors)
- a publicly understandable statement of quality and reliability.

3.6 Concluding remarks

This chapter has presented the Archive's experience of becoming certified to the ISO 27001 information security standard. In summary, the Archive considers certification to ISO 27001 to be an asset that strengthens the Archive's ability to provide secure access to confidential/sensitive data. Indeed one of the visions of the UK Data Service, managed by the Archive, is to be considered as a 'trusted source of data'. Certification of the ISO 27001 has enabled this vision to be realised.

Maintaining certification of the ISO 27001 is not without cost (in terms of staff resources). However, we maintain that Archive processes demand the controls that constitute the framework of the ISO 27001, and the marginal cost of achieving certification is far outweighed by the benefits conferred.

We also conclude that certification of the ISO 27001 is not a panacea for all information security/governance arrangements. Compliance with the ISO 27001 forms part of an umbrella of activities undertaken by the Archive to ensure best-practice in data management is routinely followed.

Chapter 4 - Recommendations

1) A shared information security standard for research data centers must emerge that is fit for its purpose as a new social science infrastructure for Europe.

- There are two important requirements for a common approach to Information Security in Research Data Centers :

  i) The adoption and implementation of information security risk management should follow a common model, developed through exchange of expertise and a transparent architecture.

  ii) The 'circle of trust' concept should be used to ensure that standards in information security in RDCs becomes neither a race to the bottom, nor gold-plating, but a common core infrastructure standard that is fit for its purpose.

2) The necessary expertise to build a shared information security standard, and the mechanisms for promulgating it, already exists in the ERA.

- It is a responsibility of established RDCs with an ISO 27001 accreditation and with the confidence of one or more National Statistics Institutions, to form partnerships with other RCDs with the express purpose of assisting the partner RDC service to achieve compliance with the ISO standard.

- The established RDCs should recover the costs of that assistance. These costs represent a very substantial saving compared to external consultancy costs. Further, the investment stays within the ERA and builds the capacity and capability of the social science infrastructure of Europe.

3) **Benchmarking and audit is essential to retain the confidence of data depositors.**

- If the adoption of a common approach to information security is achieved, the costs of audit and benchmarking are reduced.
- A coordinating authority, such as CESSDA, should make the necessary arrangements for the spot auditing of the members of the emerging network of RDCs in the ERA.
- Transparency of benchmarking and audit is essential. An annual report on the changing threats, standards, and service delivery should be produced by the relevant coordinating authority.

4) **De-mystification is essential.**

- Coordination, partnership assistance, circle of trust recognition, transparency and coordinated benchmarking and audit, should enable new RDCs to be established with necessary background information about time, cost, and service constraints. The establishment of a new RDC should become routine. New RDCs should be built within the Circle of Trust from the outset. It is more efficient to build a new RDC to a common standard than to build a unique RDC and then re-engineer it to fit the standard at some later date.

5) **Shared information security standards and interoperability does not mean all RDCs are the same.**

- A diversity of modes of service is healthy.
- Different users and different data sources require different modes of service.
- In a one-stop-shop of social science data access services, each different mode provides a different service for any ERA user.
- However, diversity that is within the ecosystem is most desirable. Diversity that is incompatible with the ecosystem can be a threat rather than strength.
- The aim is a network of equivalent services which can build and extend organically

- We must ensure that our recommendations will encourage an adoption of a common understanding of the need for and character of information security across organisations.

Practical implementation recommendations:

1. Work out what sort of service the institution want to offer. Develop a clear Understanding of institutional business and define scope.

    - Public Use Files
    - Scientific Use File controlled use service using NSI
    - High end secure use file laboratory partner with NSI
    - Remote access or remote execution solutions

2. Using this guide, decide the levels of ISMS needed, plan, estimate and allocate required resources to implementation and maintenance

3. Self assess current practice against that target and establish and describe gaps between standard and current practice

4. Actively, deliberately, according to a priority plan, close the potential gap discovered

5. Find equivalents elsewhere the ERA and open the door

Chapter 5 - Summary

The ideals of evidence-based policy making requires relevant research based knowledge production, and the key to such production is efficient access to relevant data.

The purpose of this guide is to work out and to promote a common appropriate and efficient data security standard enabling data access centers, be it NSIs or DAs, to achieve a recognisably high standard of information security and develop circles of trust, to foster such efficient access to data.

The known desirable features related to European research data access centers need to be seen from two perspectives:

- Secure storage and appropriate handling of research data, to build confidence and maintain quality of resources.
- Efficient law-abiding data sharing and dissemination, through appropriate information systems and transparent and clear access policies

In addition to the two work-oriented points above, safeguarding data confidentiality is essential from a legal point of view. Confidentiality is important for building trust between institutions, and between the data access facility and the population. The national laws and regulations set the premises for confidentiality. If data confidentiality is convincingly secured, trust will be built both nationally and internationally.

The ISO27001 standard is a generic process- and lifecycle-oriented information security management system (ISMS), which can be used across a variety of businesses. It is considered as a specification of best practice for an ISMS, and contains the following 3 elements:

- Introduction and scope description

- How to implement the ISMS
- In-depth description on management roles and responsibilities

Adapting an ISMS should be a strategic decision depending on the needs, objectives, security requirements and the size and structure of an organisation. Small problems need simple solutions, while the complex ones require a more widespread solution. The supplementary ISO27002 is a code of practice for information security and is meant to be used as an implementation support, presenting an extensive list of specific information security measures to implement.

Risk assessment is the foundation on which an ISMS is built. It provides the focus for the implementation of security controls and ensures that such measures are applied where they are most needed and most cost effective.

In the context of research data access centers, risk assessment should focus on risks associated with the business of processing, archiving and dissemination of micro level research data.

There are a number of possible risks that can damage an organisation's key assets, in our case research data: Hacking, disclosure (with or without intention), computer virus, break in, fire, earthquakes, loss of knowledge due to staff turnover, technical failure, loss of data or metadata, etc.

The measures presented by the ISO27000 family of security standards cover most of the needs for information security related to the business of archiving, handling, processing, curation and dissemination of data.

This deliverable singles out three components that need to be controlled through appropriate measures in order to secure research data and confidentiality in practical use situations:

- The data (the actual data and derived analytic output)

- The user (employees/data providers or data users/researchers)
- The practical/technical environment (the surroundings, equipment, systems etc)

The data control is to a large extent about systems for protecting confidentiality. A number of methodological techniques and working procedures are suggested in this security area. Confidentiality breaches may arise from unawareness or carelessness, from lack of knowledge about legal or contractual requirements, or from people with bad intent. Therefore, such risks need to be controlled through recommended measures directed against data providers and researchers.

However, data security is also about the more prosaic day-to-day procedures. Controls for the data aspect and the user side are not sufficient unless the environment has a certain level of security attached. There are three types of environment that should be controlled:

- Data containers (mediums in which the data are stored or processed)
- The surroundings (facilities, offices, locations, and support equipment/systems)
- Overall information security management

Most of the information security measures listed in the ISO27001/27002 should be considered to some degree, but the most important is to have a clear idea why the various controls are necessary. The business area(s), type of research data processed and/or disseminated, risk(s) involved, the size of the organization and the legal framework all set the premises for which and how many controls to implement.

Some information security controls are regarded as more important than others, and are therefore specially recommended:

- Information security incident management (serves as a tool for continuous improvement of the ISMS)

- Training/education/courses/awareness programmes (effective tool to minimize risks related to “the human factor”)

Many, but definitely not all well established research data access centers (Data Archives and National Statistical Institutes) have implemented most of the necessary information security controls already. However, the ISO27001 also emphasise the importance of having a good system for managing the information security, information security and data protection is a continuous process. This may therefore be the most important area to focus on when implementing an ISO27001-compliant ISMS, the constant need for update and maintenance and the development of a data security awareness and culture. Important elements are:

- highly involved leadership (to ensure effective implementation and continuous focus)
- routines for continuous improvement through audits and security events
- good documentation

New research data access centers should focus equally on the recommended information controls and the management system.

References

R. A. Caralli, J.F. Stevens, L.R. Young, W.R. Wilson. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Technical Report, Software Engineering Institute, Carnegie Mellon University, 2007.

CCSDS. Reference Model for an Open Archival Information System (OAIS) - Recommended Practice. Recommendation for Space Data System Practices. CCSDS 650.0-M-2. CCSDS, Washington, 2012.

INCITS/ISO/IEC. American National Standard - Information Technology - Security techniques - Code of practice for information security management. INCITS/ISO/IEC 27002-2005 (ISO/IEC 27002:2005, IDT). ANSI, New York, 2005.

INCITS/ISO/IEC. American National Standard for Information Technology - Information technology - Security techniques - Information security management systems - Requirements. INCITS/ISO/IEC 27001-2005 (adoption of ISO/IEC 27001:2005, IDT). ANSI, New York, 2006.

ISO/IEC. Information Technology - Guidelines for the Management of IT Security - Part 3: Techniques for the Management of IT Security. ISO/IEC TR 13335-3, 1998.

LRQA. Top Ten Tips when Implementing ISO 27001. Lloyd's Register Quality Assurance Ltd, Coventry, 2012. URL http://www.lrqa.co.uk/images/12118-.pdf

M. Templ, B. Meindl, and A. Kowarik. Introduction to Statistical Disclosure Control (SDC). data-analysis OG, Vienna, 2014.

United Nations Economic Commission for Europe (UNECE). Managing Statistical Confidentiality & Microdata Access - Principles and Guidelines of Good Practice. Conference of European Statisticians, New York and Geneva, 2007.

R. Welpton. Implementing ISO 27001: The Experience of the UK Data Archive. External report, UK Data Archive, Colchester, 2014.

Annex A. Control/security measure requirements

The control objectives of ISO27001/27002 are organised as subchapters a) through k) below, corresponding to chapters 5 through 15 of the ISO27002 standard respectively.

Note that a) and b) must be considered as overall objectives, while the clauses c) through k) goes more into detail on various practical aspects of information security (IS). The controls marked as "recommended" are mentioned as the most relevant ones in the ISO27002 standard.

Most of the objectives described below (marked by an "arrow-point") contain something called *implementation.* The purpose is to explain further what the controls/measures actually mean in practice. Those without the implementation part are considered straightforward and should be easy to understand the practical implications of. Some controls may also not be commented under the implementation heading due to the "straightforwardness" of the control description. This doesn't mean those are not important to implement.

a) Security policy

➔ Provide management direction and support for information security (IS)

Controls:

- IS policy document published and communicated with the purpose of providing management directions ***(recommended)***

Implementation:

- Management directions concerning information security should be communicated to the employees in a relevant, accessible and understandable way. If the policy document(s) are extensive and hard to read, a shorter and "to the point" version should be made for the purpose of communicating the content to the employees.

- The document(s) should be published on the organisation's intranet and/or handed out to each and every employee.
- Regular staff briefings should be held by management or appointed security person to ensure that the instructions are understood. In addition, the focus that these briefings represent will send a signal to employees that information security is a priority.
- The policy document should in short terms contain all that is relevant for obtaining proper information security, i.e. overall objectives, scope, the importance, framework for setting control objectives and controls, a brief explanation of the security policies, including compliance with legislative, regulatory and contractual requirements, consequences of violations, education, training and awareness requirements etc, general and specific responsibilities and reference to relevant documentation

- Policy review at planned intervals or if significant changes occur (review should include feedback, occurred incidents, trends related to threats and vulnerabilities, recommendations etc, but also decisions and actions on improvements)

Implementation:

Security briefings should be held regularly by the appointed security managers, to discuss incidents, trends and possible weaknesses to the IS. If necessary, policy reviews and adjustments to the IS policy should be conducted and communicated to the employees

b) organisation of information security

➔ Internal organisation: Establish a management framework to initiate and control the IS implementation

Selected controls:

- Actively support security through clear direction and commitment
- Responsibilities should be clearly defined ***(recommended)***
- Requirements for confidentiality or non-disclosure agreements should be identified and regularly reviewed

Implementation:

Like a), but more in (practical) detail. That is, management should maintain and communicate practical guidelines/instructions/framework concerning various aspects of IS to the relevant parties

➔ External parties: To ensure IS related to customers and the use of external parties ***(highly relevant)***

Selected controls:

- Identification of risks related to external parties
- Addressing security when dealing with customers and/or in third party agreements

Implementation:

- Management should implement IS requirements to be communicated to external users of micro data (customers) through employees working with micro data dissemination, to ensure proper use of the assessed micro data in accordance with the current laws, regulations and contractual agreements. A standard third party agreement should be implemented, to ensure that the customers understand their commitments. Security when dealing with customers should also be addressed through a set of guidelines/instructions.
- If use of external parties is needed, a risk assessment should be performed to identify the need for additional controls/measures. Access by external parties to

the organisation's information/assets should not be given before appropriate controls have been implemented.

- A third party agreement addressing all relevant security requirements should be made to avoid misunderstanding

c) Asset management

This part refers to proper management of all assets. The objective is to assure that all relevant assets are managed in a secure and proper way. This is done through inventory list, ownership responsibilities and rules for acceptable use of assets. A classification scheme (value, sensitivity) is also suggested as measure/control, to secure appropriate degree of security.

➔ Responsibility for assets (to achieve and maintain appropriate protection)

Controls:

- Inventory of all important assets should be drawn up and maintained (in case of disasters etc)
- "Ownership" of all assets should be designated
- Rules for acceptable use of assets should be implemented

Implementation:

- The main purpose of an inventory list is to help recover from disasters, but it may also be required for other business purposes like financial, insurance or safety reasons
- The asset inventory should include all information necessary in order to recover for disasters: Type of asset, format, location, backup information, license information and business value
- Type of assets may include both information and assets associated with information processing facilities:

    - Information (data, databases, metadata, archived information, operational or support procedures, contracts and agreements, system documentation, user manuals business continuity plans etc)
    - Software
    - Physical assets (computer equipment, communications equipment, removable media etc)
    - Services (general utilities like heating, lighting, power, or related to the operation of computers and communication)
    - People
    - Intangible assets like reputation or image
- Asset "ownership" may be allocated to a business process, a defined set of activities, an application or a defined set of data
- The "owner" should be responsible for an appropriately classification of all "his" designated assets, as well as defining and reviewing access restrictions and classifications. However, routine tasks may be delegated as long as responsibility remains with the "owner"
- Acceptable use of assets typically includes rules for email and internet usage, and guidelines for use of mobiles (outside the premises). All employees (and third parties having access to the organisation's assets) should be aware of the rules and limits

➔ Information classification (to ensure appropriate level of information protection)

Controls:

- Proper information classification in terms of value, legal requirements, sensitivity and criticality
- Implement an appropriate set of procedures for information labeling and handling

Implementation:

- Classification and associated protective controls should take account of business needs for information sharing
- Systematical classification, i.e. using a fixed scale. Conventions should also be made to incorporate reclassification over time. For example: Some data/statistics may initially be considered as sensitive or restricted, but after a period of time it becomes public. To avoid unnecessarily level of protection, it's important to revalue the classification. The "owner" should be responsible for the classification "his" assets.
- Procedures for information labeling must include information assets both in physical and electronic formats
- Output from information systems considered as sensitive or critical should carry an appropriate label. Output includes printed reports, recorded media (CDs, disks etc), electronic messages (emails etc), file transfers and screen displays.

d) Human resources security

...prior to, during and related to termination of employment

➔ Ensure that employees understand their responsibilities and are suitable for their roles (to reduce risk of theft, fraud or misuse)

Controls:

- Define and document security roles and responsibilities
- Screening
- Terms and conditions stating responsibilities for information security should be agreed and signed

➔ Ensure that employees are aware of information security threats and concerns, responsibilities, and are properly equipped to support the security policy

Controls:

- Active management to ensure that employees are properly briefed, are provided with guidelines, are motivated to fulfil the security policies, achieve a level of awareness on security relevant to their roles etc
- Awareness training and regular updates in organisational policies and procedures ***(recommended)***
- Formal disciplinary process for employees who have committed a security breach

➔ Ensure that employees exit an organisation or change employment in an orderly manner

Controls:

- Responsibilities for performing employment termination should be clearly defined and assigned
- All organisational assets should be returned
- Removal of access rights

e) Physical and environmental security

➔ Secure areas (to prevent unauthorised physical access)

Controls:

- Physical security perimeters (walls, card controlled entry, manned reception)
- Implement appropriate entry controls (security procedures)
- Physical security for offices and facilities
- Physical protection against disasters (if relevant)
- Guidelines for working in secure areas

- Controlling and possibly isolate access points, such as delivery and loading areas, from information processing facilities

Implementation:

- The strength of each perimeter should depend on the security requirements of the respective assets. This means all parts of the building housing the organisation doesn't necessarily need the same degree of protection.
- The building should be physically sound to avoid break-in (solid construction, locks, alarms, locking windows when not attended, external protection of windows at ground level etc)
- Manned reception area is an important security measure to ensure that only authorised personnel are given access to the building. Also check points in form of electronic card control should be considered, especially in connection with areas containing important/sensitive assets/information. A check point could also be placed at the main entrance to increase the general access security level
- Information processing facilities should be physically separated from those managed by third parties (if relevant)
- Minimum indication should be given of the purpose of the building/site, neither on the outside nor on the inside. In other words, one should avoid signs revealing activities regarded as protect-worthy. This could be locations used for production of sensitive data, or locations used for storing of such data.
- Personnel should only be aware of the existence of a secure area on a need to know basis
- Unsupervised working in secure areas should be avoided. This means in practice either video surveillance or at least two people as a minimum access requirement.
- Vacant secure areas should be locked and periodically checked. This typically applies to archive rooms used for storing of data, computer server rooms or rooms containing valuable equipment.

- Photographic, video or audio recording equipment should not be allowed in secure areas, unless authorised

➔ Equipment security (to prevent loss, damage, theft etc of assets)

Controls:

- Secure siting of equipment (to reduce risk from disasters or unauthorised access)
- Protection from power failures etc
- Protection of power and telecommunications cabling
- Equipment maintenance
- Secure off-site equipment
- Secure disposal of equipment (storage media)
- Guidelines for taking equipment off-site (authorization etc)

Implementation:

- Information processing facilities (PCs) handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorised persons during their use
- Storage facilities (PCs, hard disks, servers etc) should be secured to avoid unauthorised access. This means as a minimum good log-in and password procedures. PCs should be automatically locked after a period of inactivity, requiring a password to reopen.
- Items requiring special protection should be isolated. This could be PCs or hard disks containing sensitive data. Depending on level of risk and sensitivity, such equipment should be locked in when not attended, and offline.
- Equipment and media taken off the premises should not be left unattended in public places.
- Clear desk policy when working home
- Adequate insurance cover to protect equipment off-site

- Proper destruction of equipment containing sensitive information prior to disposal. This means deleting, overwriting and/or physically destroying so that such information is non-retrievable.
- Information, equipment or software should not be taken off-site without authorization. Employees with such permission should be clearly identified.
- Time limits for equipment removal should be set

f) Communications and operations management

This is a highly relevant security area which concerns the day to day operation of information processing facilities and the communication within the organisation as well as externally.

➔ Operational procedures and responsibilities (to ensure correct and secure operation of information processing facilities)

Controls:

- Documented operating procedures available for all relevant users
- Strict control of changes to information processing facilities and systems
- Segregation of duties (to reduce opportunities for unauthorised or unintentional modification or misuse of assets)
- Separation of development, test and operational facilities (to prevent operational problems)

Implementation:

- Operating procedures should specify instructions for the detailed execution of each job including processing, handling and backup of information, recovery procedures in case of system failure, implementing support contacts etc
- Changes to operational systems and software should be managed strictly. This includes logging, planning and testing, assessment of potential impacts, ensuring proper communication of change details to all relevant persons etc

- Defining rules for the transfer of software from development to operational status
- Development and operational software should be run on separate domains and computers
- Avoiding access to development tools or systems utilities from operational systems
- Sensitive data should not be used for test purposes

➔ Monitoring third party service delivery

Implement an appropriate level of IS and service delivery in line with third party service delivery agreements (so that all the requirements are fulfilled)

Controls:

- Ensure that security controls/measures, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party (refer to b))
- Regular monitoring, reviewing and audits of services, reports and records provided by the third party
- Managing changes to third party services (new technologies, locations, tools etc), i.e. re-assessment of risks, consider implementing new controls/measures and revaluation of third party agreement etc

➔ System planning and acceptance (to minimize the risk of system failures)

Controls:

- Capacity management (monitor, tune and make projections of future capacity requirements to ensure the required system performance)
- Establish acceptance criteria and carry out tests when introducing new information systems or upgrading (new versions)

➔ Protection against malicious code

Controls:

- Implement detection, prevention, recovery controls, and user awareness procedures to protect against malicious code
- Prevent unauthorised mobile code from executing (mobile code is software code which transfers between computers and performs specific functions with little or no user interaction).

Implementation:

- Establish a formal policy to protect against risks associated with obtaining files and software through external networks
- Installation and regular update of malicious code detection and repair software
- Perform scans for malicious codes on computers and medias, including files received over networks, emails and web pages
- The use of mobile code should be avoided. If such use is necessary, one should execute in a logically isolated environment, use cryptographic controls to authenticate the mobile code, or other measures.

➔ Backup

Control:

Perform backup of information and software, including testing, in accordance with agreed backup policy

Implementation:

- The necessary level of back-up information should be defined
- Produce accurate records of backup copies and documented restoration procedures

- The extent and frequency should reflect the business requirements, the security requirements of the information involved, and the criticality of the information with respect of the need for continued operation.
- Remote storing of backups in case of disasters
- Appropriate level of physical protection should be given to the backup material
- Regular testing to ensure the backup can be relied upon
- Sensitive backup data should be protected by encryption

➔ Network security management (to protect information and supporting infrastructure)

Controls:

- Adequately managing and controlling networks to protect from threats, and to maintain system, application and information security
- Network service agreement should include security features, service levels and management requirements

Implementation:

- Operational responsibility for networks should be separated from computer operations, i.e. employees should not work with both network operations and computer operations
- Special controls to protect confidentiality and integrity of data passing over public networks or wireless networks, as well as the connected systems and applications. Controls should include measures like network access control and cryptographic controls (refer to hence g) and h))
- Use of logging and monitoring
- The network service provider (either internal or outsourced) should sign a network service agreement containing management requirement, security features and service levels. The organisation should identify the measures (features, levels and requirements) necessary to obtain a specified level of

network security. One should also ensure that these measures are implemented by the service provider through monitoring and audits

➔ Media handling (to prevent disclosure and removal or destruction of assets)

Controls:

- Procedures for proper handling of removable media (disks, hard drives, CDs, printed media etc)
- Secure disposal of media when no longer required, using formal procedures
- Procedures for proper handling and storing of information
- Protect system documentation against unauthorised access

➔ Maintain security of exchanged information (external and internal)

Controls:

- Establish formal exchange policies, procedures and controls to protect the exchange of information through the use of all types of communication facilities
- Agreements for exchange of information between the organisation and external parties
- Secure transportation of media containing information
- Appropriate protection of information involved in electronic messaging
- Protection of information associated with the interconnection of business information systems

Implementation:

- Formal exchange policies, procedures and controls must be in place to protect exchange of information through all types of facilities

- A large number of possible measures may be used: Cryptographic techniques, not leaving sensitive information on printing facilities, procedures for use of wireless communications, guidelines for acceptable use of electronic communication facilities (email, internet etc)
- Agreements on how to exchange information with external parties should be in place.
- Various types of guidelines should be implemented to ensure a secure transportation of media containing information, i.e. physical transportation like transport, couriers, mail packages etc
- Measures to secure information associated with business information systems (internal systems related to the daily operation
- Measures related to correct use of email (and other types of electronic messaging), i.e. protecting messages from unauthorised access, ensuring correct addressing, legals (consider electronic signatures where relevant) etc

➔ Ensure secure use of electronic commerce services *(low relevance)*

Controls:

- Protect information involved in electronic commerce passing over public network
- Secure online transactions
- Protection of information integrity made available on a publicly available system

➔ Monitoring (to detect unauthorised activities)

Controls:

- Audit logs with recorded user activities and security events should be kept for an agreed period to assist in future investigations

- Establish procedures for monitoring system use (information processing facilities)
- Protection of log information
- Logging of system administrator and system operator activities
- Fault logging, including analysing and taking appropriate action
- Clock synchronization of all relevant information processing systems, using an agreed accurate time source

Implementation:

- Audit logs should include information on user ID, date/times of key events (login, logoff etc), terminal identity, and various information on system and application use. Refer to the ISO27002 standard for a complete list of information components.
- Monitoring of system use should contain much of the same information as in audit logs. The ISO27002 standard operates with five components: authorised access, privileged operations (using administrator rights), unauthorised access attempts, system alerts or failures, and changes or attempts to change system security settings and controls. Refer to the ISO27002 standard for a complete list of information components.
- Note: The extent of the monitoring and audit logs should be dependent on the risk involved, and care should be taken on respect of privacy protection, laws and regulations
- Note: If the users/employees administrator rights are limited or non-existent, then the need for extensive monitoring of system use should be lower or perhaps not relevant at all. However, any exclusion of monitoring controls should be justified (this goes for all the controls)

g) Access control

➔ Business requirement for access control (to control access to information, information processing facilities (PCs etc), and business processes)

Control:

Establish policy/framework for access control

Implementation:

An access control policy should be established and documented (and reviewed when relevant). Refer to ISO27002 for a complete list of components that the policy should take account of. The policy should reflect the security requirements based on the risk assessment. The access control rules should take account of policies for information dissemination and authorization. Naturally, the types of data access used as dissemination tool will have an impact on the choice of access controls.

➔ Practical user access management (to ensure authorised user access)

Controls:

- Formal user registration and de-registration procedure
- Privilege management (controlled allocation of privilege)
- User password management (formal management process for allocation of passwords)
- Regular review of users' access rights in a formal procedure

Implementation:

- Regarding formal user registration (for a complete list refer to ISO27002):
    - Each user ID should be unique so that users can be linked to and held responsible for their actions

    - One should check that the user has authorization from the system owner for the use of the system/service. Separate approval for access rights may also be appropriate
    - One should check that the level of access granted is appropriate to the business purpose
    - Giving users a written statement of their access rights
    - Requiring users to sign statements indicating that the conditions are understood
    - Ensuring service providers do not provide access until authorization is completed
    - Ensuring that redundant user IDs are not issued to other users
- Example of privilege management: Privileges should be allocated to users on a need-to-use basis
- Regarding user password management (for a complete list refer to ISO27002):
    - the users/employees should be required to sign a statement to keep personal passwords confidential etc. The statement could be a part of the "employment contract" containing terms and conditions of employment, refer to subchapter d).
    - establish procedures to verify the identity of a user prior to providing a new password
    - where relevant, users should be given a temporary password which they are forced to change immediately
    - passwords should never be stored on computer systems in an unprotected form

➔ User responsibilities

Controls:

- Users should be required to follow good security practices in selection and use of passwords
- Users should ensure that unattended equipment has appropriate protection
- Clear desk and clear screen policy, including secure printing practice (for example removing documents containing sensitive information immediately)

Implementation:

- Users should be advised to keep passwords confidential, to avoid keeping record of passwords using paper notes, software files or hand-held devices, to change passwords if there are suspicions of system or password compromise, to select quality passwords (hard to guess for other people, but easy to remember), to change passwords regularly, to not share passwords with others etc
- Users should ensure that unattended equipment has appropriate protection, i.e. log-off PC when session is over and locking the PC when leaving the office
- Using a clear desk policy, taking account of the information classification (refer to c)). Clear desk applies to papers and removable media, as well as clear screen (logging of unattended PC etc) and removing documents containing sensitive information from printers

➔ Network access control (to prevent unauthorised access to networked services, internal and external)

Controls:

- Policy on use of network services, i.e. only provide access to services that users are authorised to use
- Appropriate authentication methods to control access by remote users

- Automatic equipment identification to authenticate connections from specific locations and equipment (if access is restricted to certain locations or equipment)
- Control physical and logical access to diagnostic and configuration ports (those should be protected to avoid unauthorised access)
- Network segregation
- Restrictions on capability to connect to shared networks (for those extending across the organisation's boundaries)
- Network routing control

Implementation:

- The policy on use of network services should be consistent with the access control policy
- Appropriate authentication methods should be used to control access by remote users. Examples: Cryptographic based techniques, hardware tokens or a challenge/response protocol. Possible implementations could be private network solutions (VPN). Dedicated private lines can also be used to provide assurance of the source of connections. Dial-back procedures are also suggested in the ISO27002 standard.
- The use of equipment identification can be used if it is important that the communication can only be initiated from a specific location or equipment.
- Network segregation: Groups of information services, users and information systems should be segregated on networks
- Regarding restrictions on shared networks (those extending across the organisational boundaries): The capability of the users to connect should be restricted in line with the access control policy. The access rights should be maintained and updated. The restrictions may apply to messaging (emails), file transfers, interactive access, application access

➔ Operating system access control (to prevent unauthorised access to operating systems)

Controls:

- Secure log-on procedures
- User identification and authentication through unique identifier and suitable authentication technique
- Interactive systems for managing passwords to ensure quality passwords
- Restricted use of utility programs capable of overriding system and application controls
- Session time-out (after a defined period of inactivity)
- Restriction on connection times for high-risk applications

Implementation (for a complete list refer to ISO27002):

- Regarding secure logon procedures:
    - Not provide help messages during logon-procedure
    - Display general notice warning that access is only allowed by authorised users
    - Limit the number of unsuccessful logon attempts
    - Not transmit passwords in clear text over a network
- All users should have a unique identifier (user ID)
- A password management system should include (for a complete list refer to ISO27002) :
    - Enforce use of user ID and passwords to maintain accountability
    - Allow users to change passwords
    - Enforce choice of quality passwords
    - Enforce password changes
    - Force users to change temporary password a the first logon

➔ Application and information access control (to prevent unauthorised access to information held in application systems)

Controls:

- Restricted access to information and application system functions in accordance with defined access control policy
- Dedicated/isolated computing environment for sensitive application systems

Implementation:

Restrictions to access should be based on individual business application requirements and be consistent with the access policy, i.e. employees should only have access to applications they need to perform their job/duties

➔ Security related to mobile computing and teleworking

Controls:

- Formal policy and appropriate security measures to protect against risks of using mobile computing and communication facilities
- Policy, plans and procedures for teleworking activities

Implementation:

- When using mobile computing or communication facilities, i.e. laptops, ipads, mobile phones etc, in an unprotected environment, care should be taken to protect information. Not only should the facilities be protected from theft, but one should also consider the risk for hacking, overlooking, virus attacks, environmental hazards etc. As a consequence the mobile computing policy should include requirements for physical protection, access controls, cryptographic techniques, back-ups, virus protection and rules for connections to networks. Extra care should be taken in public places or meeting rooms.

- Teleworking (working other places than the office, e.g. at home, abroad or in external locations) should only be allowed if the implemented security measures comply with the organisation's security policy. One should consider the risk for theft of equipment, disclosure of information, unauthorised remote access to the organisation's internal systems or misuse of facilities. Teleworking should be authorised and controlled, and it should be ensured that all relevant controls are in place. The controls should cover the physical aspects (type of location, physical security) as well as technical/access security and rules on how the work should be done in practice (definition of work permitted, hours of work, what type of classification of information that may be held etc). Refer to the ISO27002 for a complete list of measures.

h) Information systems acquisition, development and maintenance

This subchapter applies to the information security and data integrity aspects related to the acquisition, development and maintenance of information systems. The controls and objectives listed below will therefore be relevant mostly for developers, system managers and managers responsible for acquisitions of information systems.

Information systems include operating systems, infrastructure, business applications, commercial (off-the-shelf) products, services and user developed applications. In other words; all types of computer or system tools used in the daily work of processing information.

➔ Ensure that security is an integral part of information systems

Control:

Statements of business requirements for new information systems or enhancements specifying requirements for security controls

Implementation:

- Statements of business requirements for new information systems or enhancements to existing information systems should specify the requirements for security controls.
- Security controls should be evaluated as early as possible in the process of acquisition, development or enhancement of information systems. Both automatic controls (within the system) and manual controls should be considered. The security requirements should reflect the business value of the information involved, as well as the potential business damage caused by failure or absence of security.

➔ Ensure correct information processing in applications ***(recommended)***

Controls:

- Validation of data input to applications
- Control of internal processing (to detect corruption of information through processing errors or deliberate acts)
- Controls for ensuring authenticity and protecting message integrity in applications *(low relevancy)*
- Validation of data output from applications *(low relevancy)*

Implementation:

- The information system should perform validation checks of data/value input to applications, to ensure the data is correct and appropriate.
- Applications should be able to detect any corruption of information through processing errors or deliberate acts.
- The design and implementation of applications should ensure that the risks of processing failures leading to loss of data integrity are minimized, e.g. one could consider limiting the use of add, modify and delete functions, prevent programs

from running in the wrong order or running after a failure has occurred. Note: These controls should depend highly on the business impact of corruption of data, i.e. if the consequence of failures for the business is non-existent or minimal then resources should be allocated to other types of security measures.

- Regarding validation of data output, the idea is that the output from processing data may be incorrect even though no errors have occurred during the processing phase. Such automatic output validation functionality could prove hard to implement as there are no obvious solutions to what qualifies as an incorrect (or correct) output. Typically, such evaluations are made manually by the application operator, using his experience and knowledge.

➔ Cryptographic controls

Controls:

- Implement policy on the use of cryptographic controls
- Key management (to support the use of cryptographic techniques) *(low relevancy?)*

Implementation:

- The objective of cryptographic controls is to protect the confidentiality, authenticity or integrity of information.
- The need for cryptographic controls should depend on the risk assessment, i.e. should be used if relevant

➔ Ensure security of system files

Controls:

- Procedures to control installation of software on operational systems
- Secure use of test data (avoid using sensitive data for testing purposes)

- Restricted access to program source code

Implementation (refer to the ISO27002 for a complete list of measures):

- Updating and installation of operational software, applications etc should only be performed by trained administrators. The condition is that the user has the right authorization.
- A rollback strategy should be in place before changes are implemented

➔ Security related to development of application system software

Controls:

- Implementation of changes controlled by use of formal change control procedures
- Technical review of applications after operating system changes
- Avoid or strictly control modifications to software packages
- Controls for preventing information leakage (through outbound media and communications)
- Outsourced software development should be supervised and monitored

Implementation:

- The project and support environment should be strictly controlled
- Managers responsible for application systems should ensure that all changes are reviewed to ensure that they do not compromise the security of the system
- Formal change control procedures should be implemented, i.e. using a list of procedures. Examples of components could be to maintain a record of agreed authorization levels, ensuring changes are submitted by authorised users etc.
- After changes to operating systems, business critical applications should be reviewed and tested to ensure there is no adverse impact on organisational operations or security

- Regarding controls for preventing information leakage, this could prove problematic due to privacy regulations and laws, especially when it comes to monitoring. Care should therefore be taken.

➔ Technical vulnerability management ***(recommended)***

Control:

Obtaining information about technical vulnerabilities of information systems, evaluate the organisation's exposure to such vulnerabilities, and takes appropriate measures

i) Information security incident management *(highly relevant)*

➔ Proper reporting of information security events and weaknesses

Controls:

- Report information security events through appropriate management channels as quickly as possible
- All employees should be required to note and report any observed or suspected weaknesses

Implementation:

- A formal information security event reporting procedure should be established, together with an incident response procedure
- A point of contact should be established, typically someone responsible for the overall security management of the organisation
- All employees (and third party users) should be made aware of their responsibility to report any information security events as quickly as possible
- Examples of security events:

- Loss of service, equipment or facilities
- System, software or hardware malfunctions
- Human errors
- Non-compliances with policies or guidelines
- Breaches to physical security
- Access violations

➔ Ensure consistent and effective handling of information security incidents ***(recommended)***

Controls:

- Establish management responsibilities and procedures to ensure effective response to information security incidents
- Mechanisms to monitor the types, volumes and costs of information security incidents (to identify recurring or high impact incidents)
- Correct collection of evidence (in case of legal actions after an information security incident)

Implementation (refer to the ISO27002 standard for more details):

- Guidelines for information security incident management procedures should be implemented. The guidelines should contain the following components:
  - Procedures for handling of different types of security incidents
  - Continuity plans, incident analysis, containment, planning and actions, communication with affected employees and reporting
  - Audit trails and evidence should be collected for problem analysis or various legal purposes
  - Recovery actions should be carefully and formally controlled

- Regarding correct collection of evidence, procedures should be in place so that the collecting of evidence is done according to the laws. Key factors are admissibility of evidence and the quality of the evidence

j) Business continuity management *(recommended)*

The purpose of the controls below is to counteract interruptions to business activities and protect critical business processes from effects of major failures of information systems or disasters

Controls:

- Maintaining a managed process for business continuity that addresses the relevant information security requirements
- Identify events that can cause interruptions to business processes, including the probability and impact assessment, and their consequences for information security
- Plans for restoring and maintaining operations and ensure availability of information following interruption or failure
- A single framework of business continuity plans to ensure consistency and to identify priorities
- Maintaining, testing and re-assessing business continuity plans (to ensure they are up to date and effective)

Implementation:

- The process for business continuity should include the following elements (refers to the first control in the list above):
    - Understanding the risks in terms of likelihood and impact in time
    - Identifying all assets involved in critical business processes, i.e. what assets should be covered by the continuity plan
    - Understanding the degree/magnitude of impact that security incidents are likely to have on the business

- Consider insurance
- Consider additional preventive controls
- Identifying sufficient resources to deal with the identified information security requirements, i.e. financial, organisational, technical and environmental resources
- Ensuring the safety of personnel, information processing facilities and other properties
- Formulating and documenting business continuity plans
- Regular testing and updating of implemented plans and processes
- Ensuring that the management of business continuity is incorporated in the organisation's processes and structure. Responsibility should be assigned at an appropriate administrative level

- Regarding framework for business continuity plans; this should be maintained to ensure all plans are consistent. Such framework should consider the following:
  - The conditions for activating the various plans
  - Emergency procedures
  - Fallback procedures (move essential business activities to alternative temporary locations)
  - Temporary operational procedures (until recovery is completed)
  - Resumption procedures (how to return to normal modus)
  - A maintenance schedule which specifies when the plans will be tested
  - Awareness, education and training to create understanding of the business continuity processes
  - Specify the responsibilities
  - Specify the critical assets and resources needed to perform the various emergency procedures

k) Compliance

➔ Ensure compliance with legal requirements

Controls:

- Explicit define and document all relevant statutory, regulatory and contractual requirements, as well as the organisation's approach to meet these requirements
- Implement procedures to ensure compliance with legislative, regulatory and contractual requirements on the use of material regarding intellectual property rights and on the use of proprietary software products ***(recommended)***
- Protection of important records (from loss, falsification etc), in accordance with statutory, regulatory, contractual and business requirements ***(recommended)***
- Ensure data protection and privacy in accordance with relevant legislation, regulations and contractual clauses ***(recommended)***
- Deter users from using information processing facilities for unauthorised purposes
- Cryptographic controls should be used in compliance with all relevant agreements, laws and regulations *(low relevancy?)*

➔ Ensure compliance with security policies and standards, and technical compliance

Controls:

- Managers should ensure that all security procedures within their area of responsibility are carried out correctly
- Regularly check information systems for compliance with security implementation standards

➔ Establish effective information system audits (to minimize interference)

Controls:

- Carefully plan audits and checks on operational systems to minimize risk of disruptions
- Protect access to information system audit tools (to prevent misuse or compromise)