

Guidelines on the Use and Control of Electronic Records for Statutory Compliance

This document, the “Guidelines on the Use and Control of Electronic Records for Statutory Compliance” is a detailed and comprehensive guideline identifying issues that must be addressed in providing compliance evidence in the form of records for statutory authorities and is to be read in conjunction with AQIS Meat Notice 2007/01.

Issue Date: 4th August 2004

Version: Draft 00.2

This document is part of a set of three documents:

1. Quick Guide for Use and Control of Electronic Records for Statutory Compliance
2. Guidelines on the Use and Control of Electronic Records for Statutory Compliance
3. Use and Control of Electronic Records for Statutory Compliance Self Audit Checklist

Table of Contents

| | | |
|-------|---|----|
| 1 | Introduction | 5 |
| 2 | Electronic Records Principles for Statutory Compliance Evidence..... | 7 |
| 2.1 | What are Electronic Records for Statutory Compliance Evidence..... | 7 |
| 2.2 | Guiding principles for the Management of Electronic Records for Statutory Compliance | 8 |
| 2.3 | Design for Electronic Records for Statutory Compliance..... | 8 |
| 2.4 | Statutory Compliance Record Collection | 8 |
| 2.5 | Storage and Custody of Statutory Compliance Record | 9 |
| 2.6 | Statutory Compliance Records Originals and Copies..... | 9 |
| 2.7 | Personnel Involved with Statutory Compliance Records | 9 |
| 3 | Electronic Information Risk Assessment and Management Plan for Statutory Compliance..... | 10 |
| 3.1 | Risk assessment | 10 |
| 3.1.1 | Establish the context | 11 |
| 3.1.2 | Identify the risks | 11 |
| 3.1.3 | Critical Needs Determination for Statutory Compliance Records | 11 |
| 3.1.4 | Analyse the Risks to Statutory Compliance Records | 12 |
| 3.1.5 | Assess the Risks to Statutory Compliance Records..... | 12 |
| 3.2 | Treat the Risks to Statutory Compliance Records (Risk Management Plan)..... | 12 |
| 3.2.1 | Monitoring and Review | 12 |
| 4 | Management Responsibility for Statutory Compliance Records | 14 |
| 4.1 | Statutory Compliance Records Management Policy Statement | 14 |
| 4.2 | Responsibilities..... | 14 |
| 4.2.1 | Objectives of Defining Responsibilities and Authorities | 14 |
| 4.2.2 | Authorities and Responsibilities within the Organisation | 14 |
| 5 | Electronic Statutory Compliance Record/ Information Access and Authenticity..... | 16 |
| 5.1 | What is Authentication?..... | 16 |
| 5.2 | What is Identification? | 16 |
| 5.3 | What is Access? | 17 |
| 5.4 | Using Authentication for Digital Signatures | 17 |
| 5.4.1 | Purposes | 17 |
| 5.4.2 | Outline of Process | 18 |
| 5.4.3 | Associated Functions | 19 |
| 5.4.4 | Standards..... | 19 |
| 6 | Creation, Maintenance, Availability, Access, Archive, Retrieval and Destruction of Statutory Compliance Electronic and Non-Electronic Records | 20 |
| 6.1 | The Creation of Statutory Compliance Records | 20 |
| 6.2 | The Maintenance of Statutory Compliance Records | 21 |
| 6.3 | The Availability of Statutory Compliance Records | 21 |
| 6.4 | Access to Statutory Compliance Records | 22 |
| 6.4.1 | Workstation Security | 23 |
| 6.4.2 | Network Security | 23 |
| 6.4.3 | Physical Security | 24 |
| 6.4.4 | Personnel Security | 24 |
| 6.5 | Archiving of Statutory Compliance Records | 24 |
| 6.6 | The Retrieval of Statutory Compliance Records..... | 25 |
| 6.7 | The Destruction of Statutory Compliance Records..... | 25 |

| | | |
|---------|---|----|
| 7 | Disaster Planning, Management and Recovery Related to Statutory Compliance | |
| Records | | 27 |
| 7.1 | Records and disasters | 27 |
| 7.2 | Disasters Affecting Statutory Compliance Records | 27 |
| 7.3 | Counter Disaster Management for Statutory Compliance Records | 27 |
| 7.4 | Counter Disaster Plan for Statutory Compliance Records..... | 28 |
| 7.4.1 | Content of the Plan..... | 28 |
| 7.4.2 | How to Prepare the Response and Recovery Plan | 29 |
| 7.4.3 | Lists and Supplies | 29 |
| 7.4.4 | Implementing the Plan..... | 29 |
| 7.4.5 | Training and Testing..... | 30 |
| 7.4.6 | Recovery and Restoration | 30 |
| 8 | Training of Personnel Related to Statutory Compliance Records Management | 31 |
| 8.1 | Training programme requirements | 31 |
| 8.2 | Personnel to be Trained in Relation to Statutory Compliance Electronic Records | 31 |
| 8.2.1 | Methods of Training..... | 31 |
| 8.2.2 | Evaluation and review of training..... | 32 |
| 9 | Incident Identification, Reporting and Response in Relation to Statutory Compliance | |
| Records | | 33 |
| 9.1 | Incident Management Procedures..... | 33 |
| 9.2 | Fault logging | 34 |
| 9.3 | Continual improvement..... | 34 |
| 9.4 | Corrective action..... | 34 |
| 9.5 | Preventive action | 34 |
| 10 | Internal and External Audits Related to Statutory Compliance Records | 36 |
| 10.1 | Conducting Audits for Statutory Compliance Records..... | 36 |
| 10.2 | Audit Reporting for Statutory Compliance Records | 36 |
| 10.3 | Audit Corrective Action for Statutory Compliance Records | 36 |
| 10.4 | Frequency of Audits and Corrective Action Follow-Up for Statutory Compliance | |
| Records | | 37 |
| 11 | APPENDIX – Reference Material..... | 38 |

IMPORTANT NOTICE AND QUALIFICATION

This document does not purport to provide legal advice. Compliance with this document does not guarantee compliance to any Act, Law or Regulation - it is a statement of best practice only.

The document comprises technical and industry information, and has been compiled from information sources believed to be accurate at the time of document assembly. In addition the information so obtained is believed to be in-keeping with other facts known by the authors and is therefore believed to be a reasonable representation of the situation as documented in this publication when compiled.

Due to the fact that the underlying standards, Acts, Laws, Regulations, technologies, industries position and government policies are in a constant state of change, the facts and information presented in this document may cease to be accurate after a certain period of elapsed time. Accordingly persons reading and deriving concepts of ideas from this document are encouraged to seek updated information, subsequent to publishing in order to reach appropriate conclusions based on the most reliable sources available. Pursuant to these limitations of content, Management for Technology Pty Ltd shall not accept any liability whatsoever for the direct or indirect usage of the information in this document, or in its subsequent use in respect of certain products, business decisions, practices or other processes outside its original purpose or outside reasonable time of the document release.

Organisations are encouraged to seek both legal and other expert advice when implementing any of the ideas or concepts outlined in this document.

COPYRIGHT

© 2004 Management for Technology

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Any existing Copyright material contained in this document is used under the Copyright Act "fair use" privilege allowing limited copying, without permission of the copyright holder, for certain purposes including criticism, news reporting, parody, teaching and research.

1 Introduction

During the everyday operations of business information is created, collected, stored, used, moved, copied, distributed and destroyed. This information is likely to be in many different formats and styles. These formats and style may include paper and/or electronic forms.

Businesses use this information for making operation and strategic decisions such as fulfilling customer orders, determining production requirements, exporting product as well as many others. Some of this information is necessary for the purposed of statutory compliance requirements. This document is mainly focused on the statutory compliance recording requirements for record predominately in an electronic form. However the principles in this document can be applied to all business information in either electronic or non-electronic form.

This document should be used as a guide that outlines the necessary principles that must be address for statutory compliance records.

The terms “statutory compliance records” and “statutory compliance electronic records” used through this audit checklist can be considered interchangeable. Many of the management and control requirements for electronic records apply equally to paper and non-electronic records.

Organisations may create paper records from electronic data. These paper records could then be signed as a means of approval for creation of statutory compliance records. In this case the paper record is the statutory compliance record and any electronic information (other than for the purpose of calibration, accuracy and identification of source) used for its creation is not considered to be a “statutory compliance record”. The action of a suitably trained and authorised person signing a paper record to authenticate both the existence of the record and the information contained in the record, is suitable evidence for the purpose of statutory compliance records.

The level of complexity for statutory compliance electronic records can vary greatly from organisation to organisation.

Organisations that have policies and procedures for printing out detailed time period reports that are suitably authorised, filed and used for statutory compliance records are readily able to be audited and can generally comply with the “Guidelines on the Use and Control of Electronic Records for Statutory Compliance”.

Organisations that try and have all their electronic data capture, electronic recording, electronic storage and electronic reporting systems comply with the “Guidelines on the Use and Control of Electronic Records for Statutory Compliance” generally have very complex and a very large number of policies and procedures to address the various electronic systems. This high level of complexity and large volume of procedures makes proving compliance to the guidelines difficult and time consuming.

This document is part of a set of three documents that should be used collectively, these are:

1. Quick Guide for Use and Control of Electronic Records for Statutory Compliance
2. Guidelines on the Use and Control of Electronic Records for Statutory Compliance
3. Use and Control of Electronic Records for Statutory Compliance Self Audit Checklist

This document has been prepared based on material contained in various Australian (Commonwealth, State and Local Government) and International Acts, Standards, Codes of Practice and Guidelines for electronic information creation, collection, storage, authenticity, reproduction, distribution, control and destruction for the purpose electronic records for statutory compliance. The reference document have for the purpose of simplify and easy of reading been listed as an Appendix to this document.

2 Electronic Records Principles for Statutory Compliance Evidence

2.1 *What are Electronic Records for Statutory Compliance Evidence*

Electronic records for statutory compliance can be divided into three general categories:

- Records that are electrically-stored;
- Electronically-generated records and
- Records that are partially electronically-generated and partially electronically -stored. The difference hinges upon whether a person or an electronic tool (computer) created the substantive content(s) of the records.

Electronically-stored records refer to records that are of a human expression but stored/produced in electronic form. E-mail messages, word processing files, voicemails and digital images are examples.

In contrast, electronically-generated records contain the output of electronic equipment programs, untouched by human hands. Examples are log files, telephone records, ATM transaction receipts.

A third category of electronic records is a combination of records that are both electronically-stored and electronically-generated. An example is a financial spreadsheet that contains both human statements (input to the spreadsheet program) and electronic processing (mathematical calculation performed by the spreadsheet program).

In general, electronic records for statutory compliance are just like any other statutory compliance requirements. However the following characteristics warrant special processes for its management:

- design—computer systems will only create and retain electronic records if specifically designed to do so;
- volume—the large volume of electronic records causes difficulties with storage and prolongs the discovery of a specific electronic record;
- co-mingling—electronic records relating to a specific wrongdoing are mixed with unrelated electronic records;
- copying—electronic copies can be immediately and perfectly copied after which is difficult, and in some cases impossible, to identify the original from the copy. In other cases, a purported copy may be deliberately or accidentally different from the original and hence evidentially questionable;
- volatility—electronic records can be immediately and deliberately or accidentally altered and expunged; and
- automation—electronic records may be automatically altered or deleted

Electronic records for statutory compliance management processes must be technologically robust to ensure that all relevant electronic records are stored, located and presented. They must also be legally robust to withstand judicial scrutiny.

2.2 Guiding principles for the Management of Electronic Records for Statutory Compliance

The guiding principles for the management of electronic records for statutory compliance include the following:

- Obligation to provide statutory compliance records;
- Design for statutory compliance;
- Rules of statutory compliance;
- Statutory compliance records collection;
- Custody of statutory compliance records;
- Original, copy and original copy; and
- Personnel.

2.3 Design for Electronic Records for Statutory Compliance

Ensure that electronic systems and procedures are capable of establishing the following:

- a) The authenticity and alteration of electronic statutory compliance records;
- b) The reliability of electronic equipment programs generating such statutory compliance records;
- c) The time and date of creation or alteration;
- d) The identity of the author of an electronic statutory compliance record; and
- e) The safe custody and handling of statutory compliance records.

This applies to the design or acquisition of new electronic systems or the upgrade of existing electronic systems.

There are many possible methods to achieve each of these requirements. One method is to create a paper or electronic time period report that is approved/ authorised either by physical signature or electronically by a suitable approved electronic signature. This paper or electronic record is then securely stored and made available when required. This approach ensures that any loss or alteration of original information is able to be detected by comparison to the stored authorised and time stamped "snap shot" record. The stored authorised and time stamped "snap shot" record forms the record for evidence instead of the less readily controlled and possibly transient information maintained in databases, data servers and other accessible data storage systems.

2.4 Statutory Compliance Record Collection

Collect statutory compliance information in a sound manner. Ensure that statutory compliance information collection procedures are both:

- Technologically robust to collect all relevant statutory compliance records;
- Legally robust to maximize evidentiary weighting.

There are many possible methods to achieve these requirements. One method is to have an approved quality management system that outlines the operational and technology activities that occur in the creation, collection, authenticity, storage and access of paper or electronic time period reports that form statutory compliance records.

2.5 Storage and Custody of Statutory Compliance Record

Establish procedures for the safe storage, custody and retention of statutory compliance records.

There are many possible methods to achieve this requirement. One method is to maintain a log recording all access to and handling of statutory compliance records. The log must include both electronic and physical access.

2.6 Statutory Compliance Records Originals and Copies

Determine if you are handling the original statutory compliance record or a copy of the original statutory compliance record. Ensure that any actions performed on the original or a copy is appropriate and are appropriately documented. Original statutory compliance records should be preserved in the state in which it is first identified—it should not be altered, and in instances where alteration is unavoidable, then any changes must be properly documented.

One method is to create a paper or electronic time period report that is approved/ authorised either by physical signature or electronically by a suitable approved electronic signature. This paper or electronic record is then securely stored and made available when required. This approach ensures that any loss or alteration of original information is able to be detected by comparison to the stored authorised and time stamped “snap shot” record. The stored authorised and time stamped “snap shot” record forms the record for evidence instead of the less readily controlled and possibly transient information maintained in databases, data servers and other accessible data storage systems. Any copies of either electronic record or paper records must show that they are copies by either a physical mark or electronic mark or stamp. Eg date/ time stamp.

2.7 Personnel Involved with Statutory Compliance Records

Ensure that personnel involved in the design, production, collection, analysis and presentation of statutory compliance records have appropriate training, experience and qualifications to fulfil their role(s).

3 Electronic Information Risk Assessment and Management Plan for Statutory Compliance

3.1 Risk assessment

This section of the document covers the process of identifying and minimising exposure to certain threats to statutory compliance records and recordkeeping systems.

Risk management process can be defined as:

the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

Risk management methods underpin successful counter disaster strategies and other management activities that organisations may adopt. Risk management strategies enable organisations to assess risks and the extent of planning and treatment methods that are required to mitigate or manage the risks.

Senior management have the responsibility to ensure that risk identification, analysis and assessment are carried out on a regular basis and that effective methods are implemented to safeguard the statutory compliance records and recordkeeping systems.

As risk management involves high level planning, a senior officer or officers with the required knowledge should be responsible for the program and ensure that it is implemented organisation-wide. It should cover statutory compliance records in all formats, including statutory compliance electronic records.

The recommended methodology, based on that in Australian/New Zealand Standard, AS 4360 - 1999, *Risk Management*, involves the following steps:

1. Establish the context
2. Identify the risks to statutory compliance records and recordkeeping systems
3. Analyse the risks in terms of probability and effect
4. Assess the risks in terms of acceptability and priorities for treatment
5. Treat the risks by identifying, evaluating and implementing options (this involves developing and implementing a Risk Management Plan)
6. Monitoring and review

3.1.1 Establish the context

The organisation must review and determine the level of exposure and most cost effective solution to meet the statutory compliance requirements. There are many possible solutions and each specific organisation must determine their respective context for statutory compliance record systems.

One method that an organisation may identify is that for statutory compliance record purposes there are very few records to be created, authorised and stored. The organisation may determine that creating paper copies of electronic information maybe the most cost effective solution. These authorised paper copies are created in duplicate and one of the copies is held off site in a secure storage facility. This approach meets the requirements of statutory compliance.

3.1.2 Identify the risks

The next step in the process is to identify all potential risks to statutory compliance records and recordkeeping systems, their possible causes and consequences. There are many different documented methods, models, tools and systems for risk identification, it is not the purpose of this document to provide such methods, models, tools and systems. Obtain suitable methods, models, tools and systems based on the nature, size and complexity of your organisation.

A few of the risks include:

- Natural perils: such as earthquakes, cyclones, bushfires, floods, vermin
- Structural or building failure: such as malfunctioning sprinklers, heating or air conditioning systems, leaks in roofs, poor wiring
- Industrial accidents: such as chemical spills
- Suitability of record for statutory compliance: are they authorised, accurate, relevant, current and accessible
- Technological disasters: such as viruses and computer equipment failures
- Criminal behaviour: such as theft, arson, espionage, vandalism, and
- Accidental loss through human error.

One of the most important ways to identify potential disasters is to conduct regular risk audits of statutory compliance record systems.

3.1.3 Critical Needs Determination for Statutory Compliance Records

Organisations may have also determined their critical needs for statutory compliance records and relevant equipment, buildings, personnel and systems.

A critical needs determination is based on information gathered from within and outside the organisation based on operational, strategic, legal and moral requirements of the organisation. If the recovery lead-time for replacing any equipment, buildings, personnel and systems is unacceptable then a backup alternative is usually necessary.

3.1.4 Analyse the Risks to Statutory Compliance Records

The next step in risk management for statutory compliance records is to analyse risks in terms of probability and effect. This involves looking at the risks identified and estimating the likelihood of their occurrence in the context of existing control measures. The consequences of particular risks also need to be considered. The aim of this assessment is to separate the minor acceptable risks from the major risks and to provide information to assist in the assessment and treatment of risks.

Considerations in analysing risk also include:

- investigating the frequency of particular types of disasters
- determining the degree of predictability of the disaster
- analysing the speed of onset of the disaster (sudden versus gradual)
- determining the amount of forewarning associated with the disaster
- estimating the duration of the disaster
- considering the impact of a disaster on two scenarios:
 - vital records are destroyed
 - vital records are not destroyed

3.1.5 Assess the Risks to Statutory Compliance Records

Risk assessment involves assessing the acceptability of the risk and priorities for treatment. Low probability and low effect risks might be assessed and accepted, monitored and periodically reviewed. Higher risks should be prioritised and treated.

3.2 *Treat the Risks to Statutory Compliance Records (Risk Management Plan)*

Once risks have been assessed to determine which require treatment, the organisations needs to look at treating risks.

The treatment will involve the development and implementation of a detailed Risk Management Plan that outlines the responsibilities, authority, activities, controls, monitoring and reporting against the identified risks. The Risk Management Plan would be approved by senior management within the organisation.

Risk Management Plan addressing electronic statutory compliance should include:

- General controls that affect all computer systems, like organisation controls, systems development, maintenance, documentation controls, access controls, data and procedural controls, physical security, password systems and communication security, and
- application controls unique to specific applications, like input controls, processing controls and output controls.

For more information on control measures, consult the Australian/New Zealand Standard AS/NZS ISO/IEC 17799:2003

3.2.1 Monitoring and Review

Monitoring and review of risk management programs should be continuous and should cover short and long term risks, the implementation of treatment plans and the

effectiveness of control mechanisms to ensure changing circumstances do not alter risk priorities.

The Australian/New Zealand Standard AS/NZS 4360:1999 *Risk Management* notes:

Few risks remain static. Ongoing review is essential to ensure that the [risk] management plan remains relevant....It is therefore necessary to regularly repeat the risk management cycle.

4 Management Responsibility for Statutory Compliance Records

4.1 *Statutory Compliance Records Management Policy Statement*

Organisations should define and document a policy that addresses statutory compliance records management and should ensure that the policy is implemented and maintained at all levels in the organisation.

A statutory compliance records management policy statement is a statement of intentions. It sets out what the organisation intends to do and, sometimes, includes an outline of the programme and procedures that will achieve those intentions.

The policy statement should refer to and integrate with other approved quality management system documents within the organisation.

4.2 *Responsibilities*

4.2.1 Objectives of Defining Responsibilities and Authorities

The overriding objective of defining responsibilities, authorities and inter-relationships is to establish and maintain a statutory compliance records management regime that puts in place standard practices or business rules that:

- a) Require personnel to create records according to the statutory compliance and business needs and processes that adequately document the business activities in which they take part;
- b) Ensure that information and processing systems that support business activities create appropriate statutory compliance records as part of supporting those activities;
- c) Ensure the transparency of record processes and the adequacy of records systems throughout the active life of the statutory compliance records
- d) Ensure that statutory compliance records are maintained, stored and preserved for the period of their usefulness to the organisation and to external stakeholders; and
- e) Ensure that statutory compliance records are disposed of only in accordance with a defined approval process.

4.2.2 Authorities and Responsibilities within the Organisation

The organisation should define the authorities and responsibilities of all personnel involved in statutory compliance records management. These are likely to include the following categories.

- a) Senior management should be assigned the highest level of responsibility for ensuring a successful records management programme. Senior management support is translated into the allocation of resources at a lower level. It promotes compliance with records management procedures throughout the organisation.

-
- b) Records management professionals have primary responsibility for the implementation of ISO 15489-1. In particular, they establish the overall records management policies, procedures, and standards for the organisation and implement the processes outlined in ISO 15489-1:2001, clause 4.
 - c) Managers of business units or organisational groupings are responsible for ensuring that their staff create and keep records as an integral part of their work and in accordance with established policies, procedures and standards. They provide the resources necessary for the management of records and liaise with records management professionals on all aspects set out in ISO 15489-1:2001, clause 4.
 - d) Others in the organisation have specific records-related duties. They include, in particular, staff responsible for security, staff responsible for designing and implementing systems using information and communication technologies, and staff responsible for compliance.
 - e) All personnel create, receive and keep records as part of their daily work, and should do so in accordance with established policies, procedure and standards. This includes disposing of records only in accordance with authorised disposition instruments.

Where contractors carry out the organisation's statutory compliance records management programme, it is important to ensure that they meet the standards laid down in the organisation's policies.

5 Electronic Statutory Compliance Record/ Information Access and Authenticity

5.1 *What is Authentication?*

Authentication is a term used to describe the methods, tools and system to be able to ensure that a user or record either paper or electronic is what it is displayed to be. The methods, tools and system for authenticity involve various aspects including:

- User access,
- Electronic signatures,
- Database date time snapshots,
- Date time stamps and
- Off site 3rd party archiving

Terms like electronic signatures can be further defined. Electronically signed documents must use digital signatures that are:

- Uniquely linked to the signatory;
- Capable of identifying the signatory;
- Linked to the signed document in such a way that any subsequent change to the document will be detected.

In this document authentication for statutory compliance records is a means of:

- Preventing undetected modifications to an electronic document;
- Providing limited, but reliable, information about a person;
- Providing other functions of a signature in an electronic environment, in particular the signer indicating approval of the signed document.
- The infrastructure for authenticating information about people and systems.
- The mechanism for binding a signature to a digital document.

A document could be any type of digital data file, for example text, CAD model, digital video, digital sound recording, etc., and its presentation to people could be multi-media combination of different types.

5.2 *What is Identification?*

Identification is the means by which a user provides a claimed identity to a system. Authentication is the means by which this claim is validated. An identifier or user id is usually a series of non-secret characters that are used to attempt log in to a system. Until the user authenticates himself he will have no access to the system.

The identifier is a mechanism to allow the user access to various resources, files, directories, printers on the system. The identifier must be unique to the user so that he can be held accountable for any actions performed using that identifier. When the user changes his role, is transferred or promoted, then he should have his access rights changed to reflect his new role. When the user leaves his specific role within an organisation, his user identifier should be immediately removed from the system.

Authentication is required before the user can logon to the system. There are three types of "authentication" for users:

-
- Identification and Authentication based on what a **User knows**. Passwords and phrases are often used to authenticate users;
 - Identification and Authentication based on what a **User has**. Tokens such as magnetic cards, and smartcards are examples. A common application of magnetic cards is the use of an ATM where the user must possess the card and provide a pin number. Use of a challenge response system such as RSA Secure ID or RACAL Watchword is an example of the use of a smartcard;
 - Identification and Authentication based on what a **User is**. These are biometric measurements or features such as finger prints, retina scans, voice recognition used to authenticate the user.

5.3 *What is Access?*

Access must be considered both in a physical sense as well as in virtual sense. The levels of control and recording access must apply equally to physical and virtual access.

Access to statutory compliance records or systems and the respective virtual or physical storage locations must be controlled. There must be suitable systems to limit the access to only those authorised and only for the approved purpose.

Methods and systems for access are generally based on identification and authenticity systems. Organisations must maintain suitable records of both physical and virtual access to statutory compliance records as well as records of personnel with authorisation and the approved purpose for the authorisation.

5.4 *Using Authentication for Digital Signatures*

5.4.1 Purposes

A digital signature is a form of authentication and can be used to sign digital documents.

The usual purposes of signing documents are to:

- Identify the signatory;
- Provide certainty about the signatory's personal involvement in the act of signing;
- Associate the signatory with the content of a document;
- Attest the intent of the signatory to endorse or approve authorship of a text;
- Attest the intent of the signatory to associate themselves with the content of a document written by someone else;
- Attest the fact that, and the time when, the signatory had been at a given place.

Digital Signatures rely on having a Private Key that cannot be copied. Digital Signatures rely on securely publishing the Public Key so that its owner can be identified with confidence. This is achieved using a Public Key Certificate (PKC) which is a signed document containing the Public Key along with other information about the owner and optionally what the certificate should be used for.

A digital signature created with a Public Key Certificate and private key issued by a trusted authority should be acceptable for all these purposes apart from the last.

Place is always an issue in the virtual world, but could be attested to by another person in the same place at the same time. Time could be similarly treated, although trusted time stamping services are emerging.

5.4.2 Outline of Process

All users of a Public Key Infrastructure (PKI) have a registered identity that the user community believes to be valid and trustworthy. In particular, if an institution attests to a person's identity, then appropriate procedures and processes must be in place.

Using an authenticated digital signature typically involves the following steps:

1) The person wanting to digitally sign something must first acquire a Public Key and private key from a Certification Authority (CA). This process would normally involve them proving their personal or corporate identity if they were unknown to the CA. Public Key and key can be downloaded via Internet from CAs around the world.

2) The holder of a Public Key Certificate signs digital documents as required. Typically the mechanism is provided by a software package that they invoke and requires them to validate that they are the legitimate subject of the Public Key Certificate.

The underlying steps are:

- The document is hashed, this is a algorithmic process that adds up the numeric value of the bits in the document. If a single bit is changed, added or deleted then the hash value changes.
- The hash value is encrypted using the signatory's private key to create a digital signature.
- The document ie, data file, digital signature and a copy of signatory's Public Key Certificate are sent to its recipients.

3) Each recipient processes the digitally signed document using software to:

- Decrypt the digital signature using the signatory's public key from the Public Key Cryptography, to reveal the hash value. The signer's Public Key Cryptography usually accompanies the signed document, although for some transactions it may be more appropriate to leave it in a repository.
- Calculate a new hash value (the Public Key Certificate provides details of the algorithm) and compare it with that produced by the signatory. If they are identical then the document has not been illicitly modified.
- If necessary validate (via Internet) the Public Key Certificate with the purported issuing CA, including checking their Certificate Revocation List (CRL) repository or using a service provider to establish that a Public Key Certificate is unrevoked.
- Optionally, check any policy statements or references in the Public Key Certificate to establish its suitability for the relying party's purpose. This is a risk management matter. • If the CA is unknown to the recipient then they may seek information about them and their processes to determine whether or not they are trustworthy for the recipient's purposes.

Public Key Certificate is issued with a period of validity. This means that the subject's use of the digital signature is valid in this period, unless the Public Key Certificate is revoked. A signed document may have a life far beyond this period of valid signing. The digital signature does not become invalid when the Public Key Certificate period of validity expires. However, if many years go by, technological advance may mean that it becomes theoretically possible to change the document and then apply a fraudulent signature.

5.4.3 Associated Functions

Most packages add a printable statement that the document has been digitally signed with details from the Public Key Certificate or attribute certificate.

Additional features associated with digital signatures could include:

- Appending the scanned image of the signatory's handwritten signature to a document when it is digitally signed;
- Trusted time notarisation stamping involving certified time from a trusted authority being added to a signed document.

The paper signature analogy can inhibit the creative use of digital signatures for authentication. For example:

- Authenticating messages between unattended devices; signed reports or instructions between devices can be communicated via Internet with assurance that false ones can be rejected;
- Providing a means of showing that a web page is authentic and not a spoof or worse; or
- Signing entries in a directory or database.

5.4.4 Standards

There are international as well as Australian standards for Public Key Infrastructure (PKI) and related systems/ methods and software. The selection and use of suitable Public Key Cryptography software must be documented and authorised within the documented statutory compliance records policies and management systems.

6 Creation, Maintenance, Availability, Access, Archive, Retrieval and Destruction of Statutory Compliance Electronic and Non-Electronic Records

The organisation must have documented management and operational systems based on approved policy for the creation, maintenance, availability, access, archive, retrieval and destruction of statutory compliance electronic and non-electronic records. These organisational documents must be suitably approved by the authorised senior management representative.

The requirements for the creation, maintenance, availability, access, archive, retrieval and destruction of statutory compliance electronic and non-electronic records have been broken down into specific sections of this document.

6.1 *The Creation of Statutory Compliance Records*

Capture is the process of determining that data/information should be made in to a record and kept. This includes both data/information created and received by the organisation. It involves deciding what data/information is captured, which in turn implies decisions about who may have access to those documents and generally how long they are to be retained.

Decisions about which documents should be captured and which discarded are based on an analysis of the organisation's business and accountabilities. The organisation may use a formal instrument such as a records disposition authority or guidelines that identify documents that do not need to be retained.

For the purpose of statutory compliance electronic records there can be considerable difference between electronic information manually or automatically collected that is stored in local or centralised systems and the actual evidence used for statutory compliance. An example is a printed report that is signed for originality, authenticity and filed for compliance audit purposes. In this instance the filed report is the statutory compliance record not the information collected or stored electronically.

The following questions are useful to determine the suitability of the implemented policies and methods for creation of statutory compliance records:

- Is the creation of statutory compliance records limited to those personnel with documented and approved authority?
- Does the equipment used for the creation of statutory compliance records have suitable controls to stop un-authorized creation?
- Are the statutory compliance records created in a timely and logical manner?
- Is there clear linkage back to the source information that went in to creating the records?
- If the information captured to create the records is from an electronic source, is there suitable calibration and related information to prove the accuracy of the information in the records?

6.2 The Maintenance of Statutory Compliance Records

The statutory compliance records must be maintained in suitable methods to allow for timely availability, access and use. These suitable methods must be able to differentiate records that do not form statutory compliance records from those records that are statutory compliance records.

The term maintenance is used to describe the following:

- The methods to store records (statutory compliance records and other records).
- All form of records – paper or electronic.
- All instances and locations of records (back up facilities, main facilities, working facilities, paper and electronic copies).
- Physical infrastructure.
- Virtual infrastructure.
- Disaster recovery plans and methods.

The following questions are useful to determine the suitability of the implemented policies and methods for maintenance of statutory compliance records:

- Is there a clearly documented and approved system for the maintenance of statutory compliance records?
- Once statutory compliance records have been created is there a method to check and verify or validate the records? Such as management reviewing and authorising summary reports?
- This there any automated electronic system in place to check the status of the statutory compliance records? Such as software to scans the records for viruses, faulty media (hard dish drives, etc) and fragmented or corrupted data?
- Is there a documented approved system implemented for maintaining mirrored or multi-system operational copies of statutory compliance records?

6.3 The Availability of Statutory Compliance Records

Statutory compliance records must be available when required by the authorised personnel. These needs for availability vary from day to day management requirements to that of statutory compliance audits and even legal evidence.

Availability means the authorised personnel being able to readily and easily locate one or more records based on specific selection criteria. This could be based on a date and time, a range of dates and times, production batches, specific carcasses or cartons, or any other meaningful selection basis.

Methods for controls must ensure availability only to those so authorised to access records.

The location where statutory compliance records are available is a critical element of the statutory compliance records system. If records are archived, stored off site and there is only limited time access to the storage facility this type of arrangement will not provide suitable availability.

Statutory compliance records must be able to be readily differentiated and selected from non-statutory compliance records.

The speed that statutory compliance records can be selected and retrieved is an important element of the design of the statutory compliance records systems.

The following questions are useful to determine the suitability of the implemented policies and methods for availability of statutory compliance records:

- Is there a clearly documented and approved system that controls the availability of statutory compliance records?
- Is the availability of statutory compliance records limited to authorised personnel for approved purposes?
- Are the statutory compliance records readily available in a timely and logical retrieval manner?

6.4 Access to Statutory Compliance Records

Who can access and how they can access statutory compliance records is a very important requirement of the statutory compliance records system.

Access relates to physical as well as electronic and the level of authorisation of personnel. Specific access issues include the following:

- Access control systems on physical locations of statutory compliance records with methods for verifying and recording access events.
- Do personnel that access statutory compliance records have suitable security systems in place, such as access control cards, identification cards and a system to limit or withdraw access rights.
- Workstation access and control methods.
- Network security, connection to other network and vulnerability,

The following questions are useful to determine the suitability of the implemented policies and methods for access to statutory compliance records:

- Is there a clearly documented and approved system for controlling access to statutory compliance records?
- Has the physical and virtual access statutory compliance records been identified, documented and systems implemented for control of the access?
- Is there a documented and approved operational instruction(s) for the use of Workstations or other electronic equipment related to statutory compliance records?
- Is there a documented and approved operational instruction for electronic Networks (including Network Planning, Network Configuration, Segregation of Networks, Firewalls, Monitoring of Network, Intrusion Detection, and Internet Connection Policies)?
- Has the organisation documented and approved systems for personnel security (user authenticity, access levels, maintenance and identification) related to statutory compliance records?

6.4.1 Workstation Security

All user workstations that have access to statutory compliance records should be located in secure areas. When users leave their workstations or terminals they should log off the system or lock the terminals either physically by use of key locks etc or logically using software such as password protected screen savers. An unattended workstation can be used by unauthorised personnel to:

- Gain unauthorised access to data;
- Be used to perform an unauthorised transaction for which the user who was logged in will be accountable for;
- Insert malicious software (virus, etc),
- Change, create or delete statutory compliance records for various purposes.

Inactive terminals in high-risk areas should have automatic shutdown following a period of inactivity.

To prevent unauthorised computer access, security facilities at the operating system level should be used to restrict access to computer resources. These facilities should be capable of:

- Identifying and verifying the identity, and if required, the location of the authorised users;
- Recording successful and failed system access attempts ;
- Providing authentication processes;
- Where appropriate, restricting the times of connection to users.

Typically the operating system controls who can use an application, have access to a directory or print to a specific printer etc. These operating system controls provide an initial line of defence identifying who is a legitimate user that has access to statutory compliance records. Application access controls determine what functions within the application each user can perform and control the access to statutory compliance records.

6.4.2 Network Security

Networks have four main vulnerabilities to attackers: These are

- Through connection to public networks (The Internet);
- User workstations;
- Dial in lines;
- Communications facilities.

To ensure the security and confidentiality of statutory compliance records in networks and the protection of the supporting infrastructure the organisation should establish operational procedures and responsibilities to ensure the correct operation of the networks. Access to both internal and external networks should be controlled.

The special area of virus prevention policies and methods must be adequately defined, documented, approved and implemented to ensure the prevention of access to and potential damage of statutory compliance records.

Areas that must be considered and documented are:

- Network Planning.

-
- Network Configuration.
 - Segregation Of Networks.
 - Firewalls.
 - Monitoring Of Networks.
 - Intrusion Detection.
 - Internet Connection Policies.
 - Virus protection

6.4.3 Physical Security

Physical security is an important element of any system that includes statutory compliance records. The physical security relates to the location of each and every piece of equipment that is to create, store or access statutory compliance records. This should also include the location of authenticity systems for personnel that create, store or access statutory compliance records.

Methods for physical security include suitable building access, storage facilities and access control systems for the location of each and every piece of equipment that is to create, store or access statutory compliance records.

The level of security and the choice of security methods are dependent on the level of risk and the likelihood of occurrence.

6.4.4 Personnel Security

Personnel security (user authenticity, access levels, maintenance and identification) is an important element of any system that included statutory compliance records. The ability to control the physical and virtual access to only those personnel that are suitability and currently authorised is a critical element of systems for statutory compliance records.

The use of access control photo identification cards, that log all access both physically and virtually is a typical method for achieving personnel security. This approach is used along with a system for ensuring the currency of the access control photo identification cards. When a person has their access rights changed then the access control systems and methods should instantly and automatically reflect these changes.

6.5 Archiving of Statutory Compliance Records

At certain times due to general house keeping, specific archiving plans or due to storage limitation statutory compliance records will need to be archived.

The specific archiving process must clearly differentiate non-statutory compliance records from statutory compliance records.

Archiving processes and policies must take into account the possible requirements of future access, availability and maintenance should for an audit or legal reason archived statutory compliance records need to be retrieved. The methods for retrieving must be definable, selectable, timely and reliable.

The use of contracted third parties that provide a level of independence for the purpose of archiving for statutory compliance records is an acceptable method.

The documented archiving plan and policies must have clear authority rights defined, authorisation and be current.

The following questions are useful to determine the suitability of the implemented policies and methods for archiving of statutory compliance records:

- Is there a clearly documented and approved system for archiving of statutory compliance records?
- Are the archived statutory compliance records held by a third party or some other independent process to ensure segregation from current operational records?
- Is the method for codification or identification of archived statutory compliance records suitable to allow for timely and reliable retrieval from archive should this be required?
- Is the archiving of statutory compliance records limited to authorised personnel and only to those records that require archiving?

6.6 *The Retrieval of Statutory Compliance Records*

The retrieval of statutory compliance records occurs due to a number of reasons, including the following:

- External audit or other legal requirement to obtain old statutory compliance records.
- Disaster recovery to replace lost or damaged data.
- Internal auditing activities.
- Un-expected operational requirement.

The following questions are useful to determine the suitability of the implemented policies and methods for retrieval of statutory compliance records:

- Is there a clearly documented and approved system for the retrieval of statutory compliance records?
- Are statutory compliance records logically and readily able to be retrieved?
- Are statutory compliance records clearly able to be distinguished from non-statutory compliance records?
- Are the indexing and searching methods logical and consistent with the likely requirements for retrieving statutory compliance records?
- Is the retrieval of statutory compliance records limited to authorised personnel for approved purposes?

6.7 *The Destruction of Statutory Compliance Records*

Due to space or time requirements, statutory compliance records will at some point in time need to be destroyed. The process of the destruction means that the records can never again be used for the purpose of external audit, other legal or internal organisational requirements. The decision making process for destruction must be such as to ensure destruction is appropriate. Inappropriate destruction of statutory compliance records may breach legal, statutory and/or contractual requirements.

The policies and principles of appropriate destruction of statutory compliance records apply equally to electronic and non-electronic records.

The following questions are useful to determine the suitability of the implemented policies and methods for the destruction of statutory compliance records:

- Is there a clearly documented and approved system for the destruction of statutory compliance records?
- Are there methods for determining what statutory compliance records are to be destroyed and what records are to be maintained?
- Are those statutory compliance records to be destroyed clearly identifiable from those records that are to be retained?
- Is the destruction of statutory compliance records limited to authorised personnel and only to those records that are to be destroyed?
- Is there a management or secondary review process conducted, documented and authorised for records that are to be destroyed?

7 Disaster Planning, Management and Recovery Related to Statutory Compliance Records

7.1 Records and disasters

There are a number of definitions for 'disasters'. Some sources define them as unexpected events with destructive consequences, including small and large-scale events. Others distinguish disasters from emergencies, seeing emergencies as adverse events that require action, but not significant expenditure of effort to control, and disasters as emergency events that require resources beyond the organisation's means.

Perhaps the most realistic interpretation of 'disasters' is to view them as dependent, not on the *scale* of damage, but on the *effect* that the incidents create. For example, a water leak affecting one shelf of an organisation's records may only be a small-scale emergency, but can be considered a disaster if the material affected is of significant value and will result in financial loss or legal action. Whether damage is considered a disaster will also depend on who values that material. For example, if the material on the shelf was uncopied, vital for the purpose of statutory compliance records and cannot be salvaged, it is disastrous *for that organisation* but perhaps not for the general community.

7.2 Disasters Affecting Statutory Compliance Records

Records are always potentially at risk of disaster. Due to the importance of statutory compliance records, their loss in a disaster can be crippling for the organisation. Disasters affecting records may include:

- natural events such as earthquakes, cyclones, bushfires, floods, vermin.
- structural or building failure such as malfunctioning sprinklers, heating or air conditioning systems, leaks in roofs, poor wiring.
- industrial accidents such as chemical spills.
- technological disasters such as viruses and computer equipment failures.
- criminal behaviour such as theft, arson, vandalism, and
- accidental loss through human error.

Disasters may also be caused by storage conditions that are unsuitable for the media stored, and by the natural decay of materials.

7.3 Counter Disaster Management for Statutory Compliance Records

Counter disaster management is the term given to strategies for the prevention, preparedness and response to disasters, and the recovery of operations following disasters. There are 4 clear steps required:

1. Assessment of risks affecting statutory compliance records and related systems, and the subsequent activities to reduce the probability of a disaster and reducing the probability of loss should a disaster occur.
2. Planning activities to establish a counter disaster plan to assist the Organisations to respond to an emergency event.

-
3. The activities to identify and protect vital statutory compliance records of the organisation, and response and recovery from a disaster.
 4. The activities involved in implementing the plan and initiating resources to protect or secure the organisation from loss, and restoring records and operations, so that normal business operations can resume.

7.4 Counter Disaster Plan for Statutory Compliance Records

The counter disaster plan for statutory compliance records should be sufficient to address all logical and likely risks. The plan should easily updateable, current and authorised.

It is important to plan for the most likely disasters identified in the risk assessment. For example, organisations can reasonably expect to treat the effects of fire and water. However, in a disaster, staff will be under pressure so the plans should be as concise and easy to follow as possible.

If organisations wish to reduce the time and effort expended in preparing response and recovery plans, they may use generic plans. They could also draw on existing plans from similar organisations. If generic or other plans are used as a basis they must be adapted to the specific needs of the organisation's statutory compliance records.

Where a generic package is used, the package should only be seen as the first step in developing a comprehensive plan. Identification and consideration of specific risks to the organisations is still required.

7.4.1 Content of the Plan

The basic components of the plan may vary according to organisational needs, but should include the following as noted in the Australian Standard on records management (AS 4390—1996, Part 6, *Storage*, Appendix B):

- List of vital statutory compliance records, particularly significant or vulnerable holdings, and location and control documentation.
- List of equipment and materials available for use in disaster salvage and recovery.
- The function, composition and chain of command of the salvage and recovery team and their contact information.
- Procedures for identification and declaration of a disaster situation and initiation of the disaster response chain of command by the normal business operation.
- Provisions for the training and current awareness of the team.
- List of sources of back-up resources, including expertise, tradespeople, materials, equipment, vehicles and accommodation.
- Procedures for updating and testing plan.
- Simple technical information on the handling of damaged material, directed towards establishing priorities for early action.

The counter disaster plan should be supported by:

- A clear policy statement which mandates the plan and defines responsibilities.
- Vital statutory compliance records lists and risk management procedures.
- Results of the risk assessment and analysis.

-
- Arrangements for reviewing risks and statutory compliance records lists, and revising procedures.

7.4.2 How to Prepare the Response and Recovery Plan

The response and recovery plan forms an important part of the counter disaster plan. If internal personnel are allocated the responsibility, members should represent personnel from all areas of the organisation. The response and recovery team need to:

a. Determine the preparedness strategy

By employing methods like research, brainstorming and simulations, the team can determine what the organisation has to do to prepare for the most likely disasters.

b. Determine a response strategy

The team should also consider what initial action the organisation should take when a disaster occurs, who should be called and in what order, and what further action is required. Response strategies may be determined by function if that is useful. Remember that there will be priorities in responding and recovering statutory compliance records affected by the disaster.

c. Determine a recovery strategy

Simulations and brainstorming sessions should also be used to consider the action needed to ensure that recovery is facilitated.

d. Collect data

The other major task for the team is to collect information that relates to all the phases of counter disaster management. This process may also be done through a critical needs determination with data gathered from within and outside of the organisation involving a set of inventories and checklists. This method could be chosen if a organisation has not continually maintained or updated its counter disaster plan with the consequent rise in vulnerability or it is has just been established.

7.4.3 Lists and Supplies

A vital part of planning involves compiling and frequently updating lists of materials and contacts that can be used in a disaster. Having these lists available both on and offsite enables the fast and efficient procurement of services and equipment. The lists to include will depend on the needs of the organisations and the resources available to them.

7.4.4 Implementing the Plan

Implementation of the plan involves:

- Personnel training to prevent unsafe practices or carelessness.
- Regular building and equipment inspections and maintenance to avoid building and equipment malfunctions.

-
- Installation of fire, water and movement alarms.
 - Establishment of an information security program to protect information.
 - Establishment of prevention, response and recovery contracts so that vendors can be on hand in an emergency.

For the plan to be implemented successfully, the organisation will also need to:

- Assign responsibility for the implementation and ongoing maintenance of the plan.
- Involve staff in the process of implementing the plan.
- Place a priority on vital statutory compliance records and critical data recovery.
- Regularly practice and test the plan through training exercises.

7.4.5 Training and Testing

Plans must be tested and maintained to accommodate change. If these two principles are not acted upon then the value of the human and financial investment by the organisation in its counter disaster plan (no matter how large) will dwindle as time passes. If an organisation has been fortunate enough not to experience a disaster event for a prolonged time then there is often an unwillingness to renew the disaster plan.

The objectives of counter disaster plan testing include:

- Revealing any flaws in the plan.
- Gaining feedback on any problems while implementing the plan.
- Gauging organisational responses to the suggested recovery procedures.
- Training the disaster management team.
- Practising debriefing of staff.
- Preparing for post disaster analysis.

7.4.6 Recovery and Restoration

To facilitate systematic vital statutory compliance records recovery, the vital statutory compliance records recovery plan, i.e. the list of all vital statutory compliance records, their locations, and the procedures for the recovery of these records should be included in the counter disaster plan for records and recordkeeping systems. The listing of all vital statutory compliance records should include the location of buildings and room locations, and floor plans. The vital recovery procedures should be written in a clear and concise language, easily understandable by non-technical staff. Backup copies of the vital records recovery plan should be stored off-site.

The vital statutory compliance records recovery strategy is founded on a detailed knowledge of the organisation's records holdings including every storage area in use, and of its contents and their nature, the location of vital records, and the level of information contained in finding aids or indexes.

8 Training of Personnel Related to Statutory Compliance Records Management

A training programme should ensure that the functions and benefits of managing statutory compliance records are widely understood in an organisation. It should explain policies and place procedures and processes in a context that gives staff an appreciation of why they are required. It will be most effective when it is tailored to the needs of particular groups of staff or, in some cases, individual staff members.

8.1 Training programme requirements

It is important for an organisation to assign responsibility for implementing and managing its statutory compliance records management training programme to a manager at a suitable level and to resource the programme adequately.

8.2 Personnel to be Trained in Relation to Statutory Compliance Electronic Records

It is important that appropriate training be provided for all personnel with any kind of responsibility for statutory compliance records. This includes

- a) Managers, including senior managers,
- b) Personnel,
- c) Contractors,
- d) Any other personnel who have a responsibility to create or use statutory compliance records

Organisations need to ensure that all staff identified through the risk analysis processes are trained so that they can fulfil those responsibilities.

8.2.1 Methods of Training

Methods of records management training can include the following:

- a) Incorporation in the organisation's personnel orientation programmes and documentation;
- b) Classroom training for personnel new to particular responsibilities or at times of system change;
- c) On-the-job training and coaching provided as part of a formal programme or informally by knowledgeable supervisors or peers;
- d) Briefing sessions and seminars on specific record issues or initiatives;
- e) Leaflets and booklets providing short "how-to" guides describing aspects of the organisation's record policies or practices;
- f) help text provided within a computer-based system;
- g) training courses provided by educational organisation or professional organisations that may be part of the general offerings of these organisation or may be developed on request to meet an organisation's particular needs.

8.2.2 Evaluation and review of training

Evaluation of the training programme is based on subsequent successful operation of the statutory compliance records system by the personnel. This may require measurement against the level of training undergone, and operational audits of the statutory compliance records system in the organisation. The programme may also monitor and record staff skill levels against the requirements set out in the training programme.

The effectiveness and efficiency of the records training programme will be enhanced if it is regularly reviewed and reports provided to management through the organisation's usual channels.

It is important that evaluation and review of training programmes are followed by any necessary adjustments to the programme, and that updates are provided to those already trained.

It is useful to assess any accountability breakdowns to see whether statutory compliance records management issues were a factor.

9 Incident Identification, Reporting and Response in Relation to Statutory Compliance Records

9.1 *Incident Management Procedures*

Incident management responsibilities and procedures should be established to ensure a quick, effective and orderly response to security incidents. The following controls should be considered.

- a) Procedures should be established to cover all potential types of security incident, including:
 - 1) Information system failures and loss of service;
 - 2) Denial of service;
 - 3) Errors resulting from incomplete or inaccurate statutory compliance records data;
 - 4) Breaches of confidentiality.
- b) In addition to normal contingency plans (designed to recover systems or services as quickly as possible) the procedures should also cover:
 - 1) Analysis and identification of the cause of the incident;
 - 2) Planning and implementation of remedies to prevent recurrence, if necessary;
 - 3) Collection of audit trails and similar evidence;
 - 4) Communication with those affected by or involved with recovery from the incident;
 - 5) Reporting the action to the appropriate authority.
- c) Audit trails and similar evidence should be collected and secured, as appropriate, for:
 - 1) Internal problem analysis;
 - 2) Use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation;
 - 3) Negotiating for compensation from software and service suppliers.
- d) Action to recover from security breaches and correct system failures should be carefully and formally controlled. The procedures should ensure that:
 - 1) Only clearly identified and authorized staff are allowed access to live systems and data;
 - 2) All emergency actions taken are documented in detail;
 - 3) Emergency action is reported to management and reviewed in an orderly manner;
 - 4) The integrity of business systems and controls is confirmed with minimal delay.

9.2 *Fault logging*

Faults related to statutory compliance records systems should be reported and corrective action taken. Faults reported by users regarding problems with information processing or communications systems should be logged. There should be clear rules for handling reported faults including:

- a) Review of fault logs to ensure that faults have been satisfactorily resolved.
- b) Review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized.

9.3 *Continual improvement*

The organisation shall continually improve the effectiveness of the statutory compliance records systems through the use of the information security policy, security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.

9.4 *Corrective action*

The organisation shall take action to eliminate the cause of nonconformities associated with the implementation and operation of the statutory compliance records systems in order to prevent recurrence. The documented procedures for corrective action shall define requirements for:

- a) Identifying nonconformities of the implementation and/or operation of the statutory compliance records systems;
- b) Determining the causes of nonconformities;
- c) Evaluating the need for actions to ensure that nonconformities do not recur;
- d) Determining and implementing the corrective action needed;
- e) Recording results of action taken;
- f) Reviewing of corrective action taken.

9.5 *Preventive action*

The organisation shall determine action to guard against future nonconformities in order to prevent their occurrence. Preventive actions taken shall be appropriate to the impact of the potential problems. The documented procedure for preventive action shall define requirements for:

- a) Identifying potential nonconformities and their causes;
- b) Determining and implementing preventive action needed;

-
- c) Recording results of action taken;
 - d) Reviewing of preventive action taken;
 - e) Identifying changed risks and ensuring that attention is focused on significantly changed risks.

The priority of preventive actions shall be determined based on the results of the risk assessment.

NOTE: Action to prevent non-conformities is often more cost-effective than corrective action.

10 Internal and External Audits Related to Statutory Compliance Records

This Guideline gives direction to organisations in their planning and performing of Information Audits specifically for statutory compliance records.

Information Audit is seen principally as a tool of statutory compliance records system governance within an Information Management context.

As with the audit of other organisation resources and assets, an information audit should aim to evaluate performance and compliance in relation to regulatory, legal, process, economic and efficiency based accountability measures in relation to all information lifecycle activities. The information lifecycle for statutory compliance records within an organisation consists of Collection, Creation, Storage, Access, Use and Disposal.

10.1 Conducting Audits for Statutory Compliance Records

The audit consists of an examination or survey, and an assessment followed by a report and recommendations. Elements of the examination and assessment will be done at the same time, that is: compare each item of information of the Information Inventory against the statutory compliance records audit checklist developed during the planning step, and record an assessment against each checklist item.

The information audit survey or examination step should be *active*, that is, conducted by a team of interviewers using the audit checklist developed during the planning step.

10.2 Audit Reporting for Statutory Compliance Records

The statutory compliance records Audit report should document the findings of the assessment, and contain recommendations to address deficiencies found by the assessment. It may, for example, identify those areas or sections not conforming to information policy and guidelines. It is both inadvisable and unproductive to target the failings of particular individuals. In the majority of cases, statutory compliance records problems will be the result of organisational structure, culture, technology, objectives or other non-personal factors.

The audit report may include recommendations on changes to, or new elements of, the organisations statutory compliance records policy and guidelines.

10.3 Audit Corrective Action for Statutory Compliance Records

Areas of concern identified through the audit and documented in the audit report must have corrective action applied.

Gap analysis is a tool for assisting the organisation to understand what it has and where it needs to improve. An initial information gap analysis should be performed as

part of the audit corrective action process. This is basically a view of “where are we now” and “where should we be” in terms of statutory compliance records.

10.4 *Frequency of Audits and Corrective Action Follow-Up for Statutory Compliance Records*

Audits should be conducted on a regular and documented basis. This audit schedule should be comprehensive and adequate to ensure meeting the legal requirements for statutory compliance records. The audit schedule should be kept current and suitably authorised.

The results of any corrective actions that have occurred may require special or subsequent audits to verify that the corrective action has been successful. These additional audits must be included on the audit schedule.

11 APPENDIX – Reference Material

Australian Acts

Electronic Transaction Act 1999 (Commonwealth)
[Electronic Funds Transfer Code of Conduct \(National Scheme\)](#)
[Electronic Transactions \(Victoria\) Act 2000 \(VIC\)](#)
[Electronic Transactions Act 2000 \(TAS\)](#)
[Electronic Transactions Act 2000 \(NSW\)](#)
[Electronic Transactions Act 2000 \(SA\)](#)
[Electronic Transactions \(Queensland\) Act 2001 \(QLD\)](#)
[Electronic Transactions Act 2001 \(ACT\)](#)
[Privacy Act 1988 \(Cth\)](#)
[Privacy Amendment \(Private Sector\) Act 2000 \(Cth\)](#)

Standards:

AS/NZS 4360:1999 *Risk Management*

AS/NZS 7799.2:2003 Information security management - Specification for information security management systems.

AS/NZS 7799.2:2000 (BS 7799-2:1999), Information security management, Part 2: Specification for information security management systems.

AS ISO 15489.1-2002 Records management - General

AS ISO 15489.2-2002 Records management - Guidelines

AS/NZS ISO/IEC 17799:2001 Information technology - Code of practice for information security management

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

ISO/IEC TR 13335-4:2000, Guidelines for the Management of IT Security, Part 4: Selection of safeguards.

ISO 15489-1, Information and documentation — Records management — Part 1: General

Other publications:

[1] OECD. OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002.
www.oecd.org

Standards Australia HB 171-2003 Guidelines for the management of IT evidence

Commonwealth of Australia Office of Regulation Review, *A Guide to Regulation (Second Edition)*, December 1998

National Archives of Australia PART 1 – THE DIRKS METHODOLOGY: A USERS GUIDE
September 2001 (rev July 2003)