
Use and Control of Electronic Records for Statutory Compliance Self Audit Checklist

This Self Audit Checklist provides a method to determine your organisations level of compliance to the requirements necessary for Electronic Records Systems that provide compliance evidence in the form of records for statutory authorities.

Issue Date: 5th May 2004

Version: Draft 00.1

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

Self Audit Checklist

The purpose of the Self audit Checklist is to help organisations to determine their respective levels of readiness for using electronic systems 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 self audit checklist is part of a series that is made up of the following 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

Each document is intended to provide assistance at a different level of a company.

The first document, “Quick Guide for Use and Control of Electronic Records for Statutory Compliance” is the current document you are reading. The document is a short document that outlines the principles and issues that must be followed.

The second document, “Guidelines on the Use and Control of Electronic Records for Statutory Compliance” is a detailed comprehensive explanation of the issues that must be addressed.

The third document, “Use and Control of Electronic Records for Statutory Compliance Self Audit Checklist”, is a check list that can be used by companies to measure their respective level of compliance to the guidelines.

Organisation: _____ Site: _____

Audit Date: ___ / ___ / ___ Audit Conducted By: _____

Section	Description	Non-Compliance	Action Required	Comment Only
1	Is there a defined, documented, approved and implemented Risk Assessment and Management Plan for Statutory Compliance Records ?			
1.1	Has the context (What records are for statutory compliance and what records are not) for statutory compliance recording systems been defined?			
1.2	Have applicable risks in reference to the context been defined and documented? Is there an Audit Program to check for changes in risks or additional risks?			
1.2.1	Do the identified risks include natural risks (fire, tempest, flood, etc)?			
1.2.2	Do the identified risks include human or machine made error risks (incorrect information, incorrect entry, inadvertent changes, accidental deletion, etc)?			
1.2.3	Do the identified risks include equipment failure risks (data collection equipment failure, calibration/ accuracy errors, electronic storage failures, network failure, etc)?			
1.2.4	Do the identified risks include risks associated with deliberate acts (personnel sabotage, external sabotage, management acts of fraud, hackers, etc)?			
1.3	Has the organisation determined and documented their critical needs for statutory compliance records and relevant equipment, buildings, personnel and systems?			

Section	Description	Non-Compliance	Action Required	Comment Only
1.4	Has an analysis of risks in terms of probability and effect been conducted and documented? Is it current and relevant?			
1.5	Has there been a risk assessment conducted and documented, involving assessing the acceptability of the risk and priorities for treatment to be undertaken?			
1.6	Is there a documented and approved Risk Management Plan that outlines the responsibilities, authority, activities, controls, monitoring and reporting against the identified risks?			
1.7	Has there been on going and documented monitoring and review of the risk management programs?			
2	Is there a defined, documented, approved and implemented Management Responsibility system related to statutory compliance records ?			
2.1	Has the organisation defined, documented and approved a policy that addresses statutory compliance records management? Is there evidence of the implementation of this policy?			
2.2	Has the organisation defined the authorities and responsibilities of all personnel involved in statutory compliance records management? Does this include senior management ultimately being responsible for statutory compliance records?			

Section	Description	Non-Compliance	Action Required	Comment Only
3.	Has the organisation documented and approved management and operational systems for the creation, maintenance, availability, access, archive, retrieval and destruction of statutory compliance electronic records?			
3.1	Is there a clearly documented and approved system that defines non-statutory compliance records from statutory compliance records for the purpose of creating the electronic records?			
3.1.1	Is there clearly documented, approved and implemented control systems to limit the creation of statutory compliance records to authorised personnel?			
3.1.2	Does the equipment used for the creation of statutory compliance electronic records have suitable controls to stop un-authorized creation?			
3.1.3	Are the statutory compliance electronic records created in a timely and logical manner? Is there clear linkage back to the source information that went in to creating the records?			
3.1.4	If the information captured to create the electronic records is from an electronic source, is there suitable calibration and related information to prove the accuracy of the information in the records?			
3.2	Is there a clearly document and approved system for the maintenance of Statutory Compliance Electronic Records?			
3.2.1	Once Statutory Compliance Electronic Records have been created is there a method to check and verify or validate the records? Such as management reviewing and authorising summary reports?			

Section	Description	Non-Compliance	Action Required	Comment Only
3.2.3	Is there an automated electronic system in place to check the status of the Statutory Compliance Electronic Records? Such as software that scans the records for viruses, faulty media (hard disk drives, etc) and fragmented or corrupted data?			
3.2.4	Is there a documented and approved system implemented for maintaining mirrored or multi-system operational copies of Statutory Compliance Electronic Records?			
3.3	Is there a clearly documented and approved system that controls the Availability of Statutory Compliance Electronic Records?			
3.3.1	Is the availability of Statutory Compliance Electronic Records limited to authorised personnel for approved purposes?			
3.3.2	Are the Statutory Compliance Electronic Records readily available in a timely and logical retrieval manner?			
3.4	Is there a clearly documented and approved system for controlling access to Statutory Compliance Electronic Records?			
3.4.1	Has the physical and virtual access to Statutory Compliance Electronic Records been identified, documented and a system implemented for control of the access?			
3.4.2	Is there a documented and approved operational instruction(s) for the use of Workstations or other electronic equipment related to Statutory Compliance Records?			

Section	Description	Non-Compliance	Action Required	Comment Only
3.4.3	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)?			
3.4.4	Has the organisation documented and approved systems for personnel security (user authenticity, access levels, maintenance and identification) related to Statutory Compliance Records?			
3.5	Is there a clearly documented and approved system for Archiving of Statutory Compliance Electronic Records ?			
3.5.1	Are the archived Statutory Compliance Electronic Records held by a third party or some other independent process to ensure segregation from current operational records?			
3.5.2	Is the method for codification or identification of archived Statutory Compliance Electronic Records suitable to allow for timely and reliable retrieval from archive should this be required?			
3.5.3	Is the archiving of Statutory Compliance Electronic Records limited to authorised personnel and only to those records that require archiving?			
3.6	Is there a clearly documented and approved system for the Retrieval of Statutory Compliance Electronic Records?			
3.6.1	Are Statutory Compliance Electronic Records logically and readily able to be retrieved?			

Section	Description	Non-Compliance	Action Required	Comment Only
3.6.2	Are Statutory Compliance Electronic Records clearly able to be distinguished from non-Statutory Compliance Electronic Records ?			
3.6.3	Are the indexing and searching methods logical and consistent with the likely requirements for retrieving Statutory Compliance Electronic Records ?			
3.6.4	Is the retrieval of Statutory Compliance Electronic Records limited to authorised personnel for approved purposes?			
3.7	Is there a clearly documented and approved system for the Destruction of Statutory Compliance Electronic Records?			
3.7.1	Are those Statutory Compliance Electronic Records to be destroyed clearly identifiable from those records that are to be retained?			
3.7.2	Is the destruction of Statutory Compliance Electronic Records limited to authorised personnel and only to those records that are to be destroyed?			
3.7.3	Is there a management or secondary review process conducted, documented and authorised for records that are to be destroyed?			
4	Has the organisation documented and approved a system for Disaster planning, management and recovery related to Statutory Compliance Records?			

Section	Description	Non-Compliance	Action Required	Comment Only
4.1	Does the system specifically identify disasters affecting Statutory Compliance Records both paper and electronic?			
4.2	Is there a documented and approved disaster recovery plan? Does this specifically address Statutory Compliance Records both paper and electronic?			
4.3	Have vital Statutory Compliance Records both paper and electronic been identified and documented?			
4.4	Is there a specific documented method for protecting vital Statutory Compliance Records both paper and electronic?			
5	Has the organisation documented and approved a program for personnel training in Statutory Compliance Records management?			
5.1	Is there a documented program for identification of the specific training needs?			
5.2	Is there a documented and approved program for the identification of the personnel that must be trained?			
5.3	Is there a current list of trained personnel and details of the training?			

Section	Description	Non-Compliance	Action Required	Comment Only
5.4	Is there a documented review process for the training requirements and the personnel to be trained?			
6	Has the organisation documented and approved an incident identification, reporting and response program related to Statutory Compliance Records?			
6.1	Is there evidence of incidents being logged?			
6.2	Is there evidence of a continual improvement program based on the incidents that have been logged?			
6.3	Is there a specific corrective action system for Statutory Compliance Record incidents?			
6.4	Is there a specific preventive action system for Statutory Compliance Record incidents?			
7	Has the organisation documented and approved an internal and external audit program for Statutory Compliance Records?			
7.1	Are there records of Statutory Compliance Records audits that have been undertaken?			

Section	Description	Non-Compliance	Action Required	Comment Only
7.2	Are there records of the actions taken as a result of the audits?			
7.3	Are there records that the actions taken were effective?			

General Audit Comments:
