Roadmap on Legal Requirements for IDMS implementation by Government Departments

SITA

Deloitte.

July 2004

DEFINITIONS

Addressee*	In respect of a data message, means a person who is intended by the originator to receive the data message, but not a person acting as an intermediary in respect of that data message;
Advanced Electronic Signature*	An electronic signature which results from a process which has been accredited by the Authority as provided for in section 37 [of the ECT Act];
Data*	Electronic representations of information in any form;
Data Message*	Data generated, sent, received or stored by electronic means and includes— (a) voice, where the voice is used in an automated transaction; and (b) a stored record;
Department	A department of state in the National sphere of Government ;
DPSA	Department for Public Services and Administration;
ECT Act	Electronic Communications and Transactions Act No 25 of 2002;
E-Government Services*	Any public service provided by electronic means by any public body in the Republic;
Electronic Signature*	data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature;
Hyperlink*	A reference or link from some point in one data message directing a browser or other technology or functionality to another data message or point therein or to another place in the same data message;
IDMS	Integrated document management system means a document management system that is seamlessly integrated with the electronic records management application in such a way that it is not possible to ascertain what functionality belongs to the document management system and which to the records management system.
Information System*	A system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet;
Intermediary*	A person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular data message or provides other services with respect to that data message;
ISO 15489	The ISO International Standard: Information and Documentation – Records Management;
NARS	National Archives and Records Service of South Africa;
NARS IDMS Functional Specs	Functional specification for integrated document and records management solutions (April 2004) published by NARS as a discussion document;
Originator*	A person by whom, or on whose behalf, a data message purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that data message;
PSA	Public Services Act;

IDMS LEGAL ISSUES CHECKLIST

This IDMS Legal Issues Checklist identifies the legal requirements for and legal impact of an IDMS that should be addressed during any IDMS design, implementation and operation. The guidelines provided are of a high level nature and should not be treated as exhaustive of the issues to be considered. The review is confined to the intra and some inter-Departmental legal issues and does not include e-Government services with the citizenry.

1 NEED FOR GUIDELINES AND STANDARDISATION

1.1 *Description*

1.1.1 Most existing inter and intra Departmental processes and procedures are conducted within a physical, paper based environment. Existing guidelines or standards governing such processes and procedures had been developed over the years contemplating a physical, paper based environment.

1.1.2 IDMS will have a substantial impact on these existing processes and procedures, ultimately replacing various physical activities and paper based records.

1.1.3 Without clear guidelines or standards (albeit at a high level), each Department's approach to IDMS may vary, culminating in costly duplication, lack of inter-operability, inconsistent processes and procedures, etc.

1.2 *Risk*

1.2.1 The aforegoing may translate into legal risk when it impacts on service delivery to the citizenry or improper application of taxpayer monies. In extreme cases, this may cause inefficient corporate governance and risk management challenges for Departments.

1.2.2 Legal liability may arise if erroneous or insufficient services can be attributed to negligence in design and implementation of IDMS.

1.2.3 It must be remembered that Government is a single legal entity and a chink in the armour of one Department's IDMS could expose another Department to liability.

1.3 *Recommendation*

There is an indivisible interplay between three IDMS stakeholders:

1.3.1 The ***efficiency and effectiveness*** of an IDMS is the ultimate responsibility of a Department. It forms part of each Departments' business planning, procurement and operational responsibility.

1.3.2 ***Interoperability and integration*** with other systems and Departments, while a shared responsibility of a Department, ultimately falls within the domain of the DPSA. IDMS forms an integral part of e-Government[1] and for which DPSA ultimately assumes

[1] The Gartner Group defines e-Government as: "the continuous optimisation of government service delivery, constituency participation, and governance by transforming internal and external relationships through technology, the Internet and new media." (our emphasis)

responsibility.[2] It is submitted that DPSA is the ultimate custodian for IDMS integration and inter-operability.

1.3.3 NARS has the statutory mandate to regulate the ***management of records systems***.[3] This refers to the management and retention of information generated, processed and stored within an IDMS. In this regard, NARS has released the NARS IDMS discussion document.

1.3.4 We recommend that DPSA considers a review, amendment and possibly joint publication of the NARS IDMS Functional Specs to incorporate aspects in respect of ensuring interoperability and integration. Alternatively, DPSA could develop separate guidelines or regulations which could refer to the NARS IDMS Functional Specs in terms of section 41(1) of the PSA[4]. Consideration could also be given on how to utilise the Public Finance Management Act (regulations) to require governance structures around IDMS.

1.3.5 It is advisable to consider establishing an ***inter-Departmental IDMS committee*** to provide a monitoring and oversight role in respect of IDMS co-ordination, harmonisation and standardisation. This committee could also provide feedback on "lessons learned" in specific IDMS implementation initiatives. Permanent members must include DPSA, SITA, NARS and possibly Treasury and the Office of the Auditor General.

1.3.6 As this would constitute good governance and alignment with good practice, it is submitted that ISO 15489 be used as a basis for all IDMS design, implementation and operation. See next section.

1.3.7 Extracts from this IDMS Legal Issues report could be referred to or incorporated into both DPSA and NARS initiatives, should this be required or deemed prudent.

1.3.8 The recommendations made in this paragraph should be considered in conjunction with those made in paragraph 2 below.

2 E-GOVERNMENT REGULATORY FRAMEWORK

2.1 *Description*

The challenges identified in the current project around IDMS and the lack of inter-Departmental harmonisation accentuates the need to consider establishing a regulatory framework around E-Government in general (which should include IDMS).

In many respects, IDMS constitutes the building blocks or foundation for any Department's initiatives around e-Government.

There is a perception that a great deal of duplication and re-invention of the wheel is occurring in respect of current initiatives and projects such as HANIS, e-Deeds, e-Justice, Tax filing, CIPRO, e-Gateway, etc. These projects extend far beyond the notion of IDMS but it becomes almost impossible to divorce such projects from IDMS underlying it or forming a component part thereof.

[2] The South African Government's e-Government Policy (Second Draft 2001 version 3.2) published by the DPSA includes the Government-to-Government (G2G) environment within the concept of e-Government. The other sectors are: Government-to-Citizen (G2C), and Government-to-Business (G2B). The e-Government Policy specifies the need for co-ordination of acquisition of information technologies and places a premium on interoperability.

[3] Section 13(b)(ii)-(iii) of the NARS Act.

[4] Specifically subsection (3)(iv) and (v).

2.2 ***Recommendation***

In environments where there is a history of "going at it alone" or where there are considerable challenges to create a culture of co-ordination, regulatory intervention may be preferable as opposed to a policy approach.

A regulatory regime in the form of an E-Government Act need not be punitive or prohibitive but can be structured to facilitate and enable E-Government initiatives (including IDMS).

It is recommended that the Minister for Public Service and Administration be consulted on the need to consider e-Government regulation, whether as part of the PSA or by way of a new Act. Regulation will be of no practical application unless a Member of Cabinet is formally tasked with the administration thereof. In any country where the concept of e-Government is novel and challenging, there is a need to appoint an e-Government champion and, in this regard, consideration could be given to the UK Government initiatives around the office of an "e-envoy".

Care must be taken in ensuring continuity of current IDMS initiatives pending finalisation of such regulatory framework. DPSA and/or SITA is currently in possession of recommendations from consultants on the need for e-Government regulation which had been produced as part of the e-Gateway Project (Phase 1).

3 ALIGNMENT WITH BEST PRACTICE

3.1 ***Description***

3.1.1 It is a common misconception that the ECT Act creates "rules" for electronic records management, it merely sets certain broad parameters, primarily around the need to take reasonable steps to retain the integrity or trustworthiness of records.

3.1.2 The ECT Act facilitates the electronic enablement of forms, authorities, approvals and retention. However, the ECT Act does not prescribe which processes are to be followed.

3.1.3 The ECT Act accordingly leaves it up to the industry to determine the nature, scope and technologies for (in this case) IDMS. It leaves it to the industry to set their own rules, provided these can be accommodated within the parameters set in the ECT Act.

3.2 ***Risk***

3.2.1 IDMS will form an integral part of a Department's overall records management processes. As such, records management should conform to the same principles, irrespective of the fact that it is in paper or electronic form.

3.2.2 To follow separate regimes for paper versus electronic records would be contrary to good practice and create disparity and confusion.

3.2.3 To manage legal risk, records management within an IDMS must be aligned with best practice principles.

3.3 ***Recommendation***

3.3.1 IDMS implies by its very name the integrated management of records, which is a technology neutral concept.

3.3.2 In the absence of any other guidelines or standards applicable to Departments, it is recommended that IDMS design, implementation and operation should conform to ISO 15489, alternatively the NARS Functional Specs.

3.3.3 The ISO 15489 standard has now been adopted as a South African National Standard SANS/ISO 15489. The standard is divided into two parts:

3.3.4 *Records Management - Part 1*: *General* provides a high level framework for recordkeeping and specifically addresses the benefits of records management, regulatory considerations affecting its operation and the importance of assigning of responsibilities for recordkeeping. It also discusses high level records management requirements, the design of recordkeeping systems and actual processes involved in records management, such as record capture, retention, storage, access etc. It concludes with a discussion of records management audit operations and training requirements for all staff of an organisation.

3.3.5 *Records Management - Part 2: Guidelines* provides practical and more detailed guidance about how to implement the framework outlined in Part 1. For example it provides specific detail about the development of records management policy and responsibility statements and outlines the process for developing recordkeeping systems. Part 2 also provides practical guidance about the development of records processes and controls and specifically addresses the development of key recordkeeping instruments, disposal authorities and security and access classification schemes. It then discusses the use of these tools to capture, register, classify, store, provide access to and otherwise manage records. Part 2 also provides specific guidance about the establishment of monitoring, auditing and training programs to promote and effectively implement records management within an organisation.

3.3.6 The legal issues / considerations discussed in the remainder of this "Roadmap" document could directly or indirectly be brought within the ambit of ISO 15489. However, they merit specific discussion with reference to South African Law.

4 'PROCESS OWNERS' TO ACTIVELY PARTICIPATE IN IDMS DESIGN, IMPLEMENTATION, OPERATION AND GOVERNANCE

4.1 *Description*

4.1.1 Form a legal and regulatory perspective, an IDMS is merely a tool to support a Department's internal operations. IDMS therefore automatically falls within existing processes, procedures and governance.

4.1.2 Some officials within a Department who bear responsibility for existing processes and procedures ("Process Owners") could perceive IDMS as merely an "IT" issue. This mentality may cause those responsible for design and implementation of an IDMS to depart (in good faith) from existing processes and procedures.

4.1.3 The end result may be an IDMS which, because of its technical set-up, causes substantial disparity between the same process or procedure performed in a physical or paper-based manner.

4.2 *Risk*

4.2.1 Process Owners who fail to provide adequate input during the design phase and remain involved in implementation, operation and governance of an IDMS may introduce legal risk to the Department if the disparity between physical vs IDMS processes lead to errors or undue delays.

4.2.2 Legal risk arises where such errors or delays impacts on service delivery to the citizenry or improper application of taxpayer monies. In extreme cases, Departments may become exposed to inefficient corporate governance and risk management challenges.

4.2.3 Legal liability may arise if erroneous or insufficient services can be attributed to negligence in design of an IDMS.

4.3 ***Example***

4.3.1 A Process Owner has always required a certain application form to be approved by two authorised officials, the relevant paper form providing for two physical signatures. The same application, now processed by the Department through the IDMS, requires only one official to approve the electronic form. Applications (whether for internal or external approval purposes) are approved faster in the IDMS as opposed to paper forms. Applicants whose applications go through IDMS "catch up and overtake" those processed physically. As a result, applicants who were "first in time" suffer a prejudice as a result of the disparity in paper vs electronic processing (assuming this can be translated into monetary loss) and sue the Department.

4.4 ***Recommendation***

4.4.1 Process Owners must be consulted and remain involved throughout the design, implementation, operation and governance of an IDMS.

4.4.2 Process Owners must ensure harmonisation with concurrent paper processes. However, this must not be taken to the extreme, i.e. slowing down IDMS approvals. Each case must be addressed on its own merits.

5 REVIEW OF "VESTED RIGHTS" OF THIRD PARTY SUPPLIERS/VENDORS

5.1 ***Description***

5.1.1 Although various reviews are likely to be performed as part of a business requirement analysis for an IDMS, these reviews are usually aimed at determining the scope and functional specifications of an IDMS for purposes of its design and implementation.

5.1.2 What is required is a review of the potential effect of IDMS on existing legal relationships.

5.2 ***Risk***

5.2.1 The IDMS causes existing processes and procedures to be altered drastically, thereby affecting existing legal relationships with third parties.

5.2.2 Such third parties may have long term agreements to continue servicing the (now redundant) physical processes and procedures.

5.2.3 A Department may be legally obliged to continue with the third party relationship or, where such relationship is terminated, pay damages as a result of breach of contract.

5.3 ***Example***

5.3.1 Supplier X has an agreement to supply the Department with 100 batches of paper clips per annum.

5.3.2 As a result of IDMS there is less usage of paper and, consequently, paper clips.

5.3.3 Assuming the Department need only 50 batches after IDMS, the Department would still be legally obliged to procure the redundant 50 batches per annum.

5.4 ***Recommendation***

5.4.1 A Department must conduct a review of how an IDMS will affect existing processes and procedures within the Department ("Existing Processes") by comparing it to the processes and procedures envisaged after full implementation of an IDMS ("New Processes"). The review must indicate the following:

5.4.1.1 Does an Existing Process involve a third party, such as another Department, company or organisation ("External Party")?

5.4.1.2 What is the nature of such External Party involvement?

5.4.1.3 Would the New Process still require the External Party involvement?

5.4.1.4 If so, does the New Process require a change in the relationship with the External Party?

5.4.1.5 If such relationship is likely to be affected, what is the legal nature of the relationship with the External Party?

5.4.1.6 If the relationship is governed by an agreement, would the New Process require a change to the terms of such agreement?

5.4.1.7 If yes, enter into negotiations with the External Party and determine whether such amendments would be easy/difficult to achieve (once the IDMS becomes operational).

5.4.1.8 If difficult, the IDMS Project Manager must consult its legal advisors and determine next steps.

6 REVIEW OF EFFECT OF IDMS ON INTERNAL STAFF

6.1 ***Description***

The job functions of various existing staff may be impacted by the IDMS. This could result in amendments to terms of employment, transfers or even redundancies.

6.2 ***Risk***

Breach of labour laws, employment terms and trade union action.

6.3 ***Example***

Archival staff may have to be reduced or reassigned to other divisions.

6.4 ***Recommendation***

6.4.1 A Department must conduct a review of how an IDMS will affect Existing Processes by comparing it to the New Processes. The review must indicate the following:

6.4.1.1 the nature of an Existing Process;

6.4.1.2 the documents or records that are subject to such Existing Process;

6.4.1.3 the Departmental staff involved in the administration or facilitation of such activity and a short description of such Staff's job function ("Affected Staff");

6.4.1.4 how the New Process will affect / change the Existing Process;

6.4.1.5 will the New Process impact on or change the job function of Affected Staff? If so, are any lay-offs or amendments to terms of employment envisaged? (this must be completed by a Department's HR division)

7 LEGALLY SOUND PROCUREMENT PROCESS

At the risk of stating the obvious, the acquisition and implementation of an IDMS must conform to prescribed procurement principles and procedures.

8 CONTINUITY OF IDMS MAINTENANCE & SUPPORT

8.1 *Description*

It is acknowledged that SITA will play an integral role in the procurement of an IDMS. This section does not draw a distinction between a Department's role or that of SITA nor does it prescribe what the agreement between SITA and a Department should provide for. It merely outlines certain generic but fundamental principles in respect of the relationship between a Department/SITA and third party service providers/suppliers.

8.2 *Risk*

8.2.1 IDMS maintenance and support may require long-term involvement by the relevant vendor/s providing maintenance and support.

8.2.2 As we have seen, various IT companies have been liquidated, sold or dissolved over the last few years.

8.2.3 This requires each Department to provide for contingencies by way of appropriate agreements (Development, Maintenance & Support).

8.3 *Example*

Vendor X is an approved distributor and service provider in South Africa for a US software product. The US Licensor cuts ties with Vendor X. The affected Department does not have a back-to-back service & support agreement with the US Licensor. No vendor is licensed by the US Licensor to provide maintenance, support or upgrades.

8.4 *Recommendation*

Provision should be made for the following core principles to be incorporated in all agreements concluded with service providers and suppliers of an IDMS (please note that these principles are confined to IDMS specific issues and are in addition to a variety of other principles):

8.4.1 Comprehensive on-site acceptance testing

8.4.2 Service levels & milestones

8.4.3 Skills transfer (to Department and/or SITA)

8.4.4 Maintenance, support, right to upgrades & new versions

8.4.5 Access to source code (subject to an Escrow arrangement)

8.4.6 Authority to commission a third party vendor to provide maintenance & support where the primary vendor is in breach of contract, commits an act of insolvency or undergoes a change of control which may have adverse consequences.

9 MAKE EXISTING POLICIES & PROCEDURES TECHNOLOGY NEUTRAL

9.1 *Description*

Many existing policies and procedures contemplate physical, paper based activity.

9.2 ***Risk***

Creating separate regimes for paper based and IDMS processes would introduce disparity and therefore risk (including legal risk).

9.3 ***Recommendation***

As opposed to creating separate governance structures, policies and procedures for IDMS, existing ones should be revisited and adapted to make them apply equally to IDMS.

10 THE NOTION OF A 'TRANSACTION' FOR IDMS PURPOSES

10.1 ***Description***

10.1.1 In an IDMS environment, the term or concept of a "transaction" should be afforded a wide meaning. It should extend to any electronic approval or authority that is logically linked with a particular record. It should not be restricted to the traditional notion of 'buying or selling' something. For instance, the electronic approval of a leave application would constitute a transaction.

10.1.2 A distinction must be drawn between the following:

10.1.2.1 A paper document is signed and is imaged purely for archival purposes. In this case, the electronic record evidences a transaction by and of itself (its contents). There is no additional data necessary to prove that a transaction occurred.

10.1.2.2 A record is authorised, accepted or approved by electronic means (e.g. a digital certificate). In this case, the data evidencing such approval, acceptance or authority is not always determinable form the record itself, but from associated data or metadata.

10.2 ***Risk***

10.2.1 If no logical association or audit trail is maintained between the record and its approval, it may be difficult to prove that a transaction had occurred.

10.2.2 This could lead to unforeseen consequences and legal risk.

10.3 ***Recommendation***

10.3.1 IDMS design must ensure that all transactional data associated with a record is maintained and retained for as long as such record is kept.

10.3.2 There is no legal obligation to embody the transactional data within the relevant record and it is permissible to retain such data separately, provided an audit trail exists linking the two data sets.

11 Z-FORMS

11.1 ***Description***

DPSA has and continues to administer the issuing of all Z-forms.[5] Departments may be concerned that by e-enabling the Z-forms ("e-Forms") onto an IDMS, such e-Forms may be at risk of being invalid. DPSA indicated that while it may be tasked with the issuing of the Z-Forms, it has always been and remains the responsibility of each Government department to properly execute and process them and put control checks and policies in place in this regard.

[5] See also Government Gazette Notice No R1 of 5 January 2001 (as amended) published in terms of the Public Services Act.

11.2 ***Recommendation***

11.2.1 Most (if not all) Z-Forms can be generated, approved, transmitted, processed and stored electronically, subject to such requirements set by DPSA from time to time.

11.2.2 DPSA is considering publishing regulations, alternatively guidelines under the Public Services Act dealing with the electronic enablement of Z-Forms. Depending on the nature and scope thereof.

11.2.3 The setting of standards is to avoid disparity between Departments, which could ultimately translate into legal risk.

11.2.4 Stakeholders for consultation include the Office of the Auditor General, SITA and NARS.

12 FORMS OTHER THAN Z-FORMS

12.1 Any forms (other than Z-Forms) to be generated, approved, transmitted, processed or stored electronically must be recorded on an "IDMS Forms Approval List" by the Departments IDMS project manager.

12.2 The Department's legal department must review whether any of the forms on such list fall within the ambit of statute or regulation.

12.3 If a form is not subject to statute or regulations, such form may be generated, approved, transmitted, processed or stored electronically.

12.4 If a form is subject to statute or regulation, the legal department must determine whether such law prescribes any formalities in respect of such form (such as writing or signature).

12.5 To ensure standardisation and covering all relevant issues, it is suggested that the legal division of a Department complete the questionnaire attached as Schedule 1. In performing this review, the Department's legal division must take due notice of the provisions of Part 1 of Chapter 3 of the ECT Act. The following provisions of the ECT Act would have to be considered:

12.5.1 ***Statutory requirement for document or record to be "in writing"***

Where a law (statute or regulation) requires a form or information to be in writing, section 12 of the ECT Act permits this requirement to be met electronically, provided the information or form is "accessible in a manner usable for subsequent reference".

12.5.2 ***Statutory requirement for a form to be signed***

12.5.2.1 Very few laws require the application of a signature. Examples of laws that do require the application of a signature are the Credit Agreements Act and Alienation of Land Act. However, in an IDMS environment one is unlikely to find such requirements where forms are required to be signed by statute or regulation. However, this cannot be excluded and a Department's legal division must perform a review to determine whether any form is prescribed by statute or regulation and, if so, whether such law 'requires' a signature.

12.5.2.2 If it is found that a form is required by statute or regulation to be signed, then the legal division must have regard to the provisions of section 13(1) of the ECT Act to determine whether such form can only be signed by way of an "advanced electronic signature". See definition in ECT Act of advanced electronic signature.

12.5.2.3 NB: it doesn't automatically mean that if such signature requirement is encountered, that an "advanced electronic signature" MUST be used. One must have regard to the consequences of not using a signature: does it lead to invalidity of the form or not? If not, there should be no reason for using an advanced electronic signature.

12.5.3 ***Statutory requirement to retain the "original" document***

12.5.3.1 Even where a statute or regulation requires a Department to retain the "original" of a paper based document, it is permissible to image such document and to destroy the original subject to the following:

> "…the integrity of the information from the time when it was first generated in its final form as a data message remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display."[6]

12.5.3.2 Although not an express requirement of the ECT Act, it is advisable that the imaging must be conducted in terms of a standardised process which is aligned with best practice and governed by a policy and procedures manual.

12.5.3.3 See section on imaging.

13 APPROVALS AND AUTHORITIES: MUST AN ELECTRONIC "SIGNATURE" BE USED?

13.1 There are a variety of authentication tools and methodologies Departments can use to authenticate employees. These include the use of passwords and personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards or other types of "tokens," database comparisons, and biometric identifiers.

13.2 In short, a Department is not required by law to use what is commonly known as an 'electronic signature' to 'sign' e-Forms for such forms to be valid or official within an IDMS.

13.3 The validity of an e-Form can be determined from the process by which it was generated. If a technical process is set up so that an e-Form can only be processed if it had been approved by an authorised person, such evidence would be sufficient for legal purposes.

13.4 In terms of section 13(5) of the ECT Act, unless a "signature" is required by a Statute or Regulation or unless the parties (in an IDMS) expressly require the use of an "electronic signature":

> …. an expression of intent or other statement is not without legal force and effect merely on the grounds that ….it is not evidenced by an electronic signature but is evidenced by other means from which such person's intent or other statement can be inferred." (our emphasis)

13.5 The ECT Act makes it clear that the law would look at the process whereby approval, acceptance or authority had been given, rather than to the manifestation of such approval, acceptance or authority.

13.6 For instance, if the access levels in an IDMS is set up in such a way that only a person with requisite authority (hereinafter referred to as the "Approval Authority") would have been able to approve a form, then, just as in the case of a paper based signed form, such approval is likely to be deemed to have been properly granted. It would suffice to lead

[6] Section 14 of the ECT Act.

evidence on the soundness of the process of setting access levels and the security of the system.

13.7 One should not confuse the concept of approval or authorisation with the traditional notion of "signing" a document. In an IDMS one should prefer the term "affirmation" in stead of the term "signature". ***Affirmation*** means some action or activity is affirmed, whether the fact that a person:

13.7.1 completed an application (I affirm this is me having submitted this form);

13.7.2 submitted an application (I affirm I am the line manager of the applicant);

13.7.3 approved an application (I, duly authorised, hereby approve the application);

13.7.4 received an approved application (I confirm having received and executed a duly authorised application); or

13.7.5 acknowledges having read, understood and agreed to the terms of a contract or a policy.

13.8 The affirmation must be capable of identifying the individual who performed the action of affirmation. However, the manifestation of such affirmation need not be apparent from the record itself, provided there is a logical, traceable link or "audit trail" evidencing the fact that the requisite affirmations have been obtained.

13.9 By way of example, an Approval Authority (e.g. line manager with requisite authority) approves leave applications of her staff in the ordinary course of business. With the introduction of IDMS, the relevant completed Z-Form leave application is located on the Intranet and the Approval Authority is notified of the need to approve it by email. The Approval Authority accesses the relevant form on the Intranet by way of applying her unique User ID and PIN. The IDMS permits only the Approval Authority's User ID and PIN to give access to the Z-Form. The Approval Authority reviews the Z-Form and then clicks "approved" on the relevant Intranet page. This "click" constitutes the instance and moment of affirmation (the equivalent of a signature). The IDMS notifies the applicant and the Approval Authority of such acceptance by email. Such notification by email is merely the notification of an event (approval), and not the approval itself.

13.10 This means that at no point was a digital certificate really needed – it was sufficient for the IDMS to be set-up in such a way that there is clear evidence or proof that the approval could not have been given had the User ID and PIN of the Approval Authority not been applied. If an unauthorised person somehow obtains knowledge of the Approval Authority's User ID and PIN, the email notification to the true Approval Authority may serve as a means to prevent the fraud from being executed.

13.11 ***Principles to be applied in selecting the technologies:***

13.11.1 In all instances, it is imperative for the IDMS design to consider the technologies and means of producing adequate and sufficient evidence of the fact that an affirmation had been given.

13.11.2 The affirmation need not be evidenced in the relevant record which required affirmation, provided there is an audit trail linking the record to the act of affirmation.

13.11.3 The affirmation must be linked to the individual having performed such affirmation. Where technically possible and feasible, the date of affirmation should form part of such audit trail.

13.11.4 In most IDMS "transactions" as discussed in paragraph 10, the process of affirmation (the ability to link an activity to the relevant person) is more important that the manifestation of the affirmation (e.g. a digital certificate or digitally imaged signature). Of course, these can be combined and this may contribute to the reliability or proof of affirmation.

13.11.5 However, take care in falling foul of two extremes:

13.11.5.1 Insufficient processes and technologies;

13.11.5.2 "overkill" or too complex technologies having regard to the nature of the record or activity.

13.11.6 Avoid using "scanned" copies of a physical signature as this is one of the most unreliable means of "signing" or affirmation. It is also one of the most risky activities for a Department to tolerate. If a person's signature is stored on a publicly accessible network, almost anyone can perpetrate a fraud merely by having access to a letterhead and such imaged signature.

13.11.7 This is not to say that a scanned signature cannot serve as a reliable means of affirmation. If the IDMS access levels are set up in such a manner that the scanned signature image is accessible only to the signatory and that only such signatory or her secretary could have applied it to a record, such "process" would provide reasonably reliable evidence of affirmation. This implies of course that the applied imaged signature is not reasonably capable of being copied (e.g. do not send out a Word document, rather convert to pdf).

13.11.8 Each case must be evaluated on its own facts. However, it is suggested that the NARS IDMS Functional Spec set out certain guidelines or criteria. In this regard, see the guidelines issued by the Office for the Controller of Currency in the USA and also the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce.

14 PROOF OF HAVING SENT AN EMAIL

As a general rule, the law would deem an email to have been sent by the purported originator unless such purported originator can prove otherwise on a balance of probabilities. The IDMS must be set up in a manner that requires log-on through a User ID and PIN (collectively referred to as "Password") for the authorised person to access and send email from his/her email. This can be achieved either during initial log-on to the network and/or when accessing email. It is however not legally necessary to require a Password in <u>both</u> instances.

Email usage must be governed by a policy. The policy should be user friendly and readily accessible. Email usage need not be covered by a separate policy (e.g. email usage policy) but could form part of a broader policy (e.g. communication systems usage policy).

15 PRIVACY & DATA PROTECTION

15.1 *Description*

Personal information can broadly be defined as any information capable of identifying and individual. As a guideline, the definition of personal information in the Promotion of Access to Information Act can be used.

The SA Law Reform Commission ("Commission") released an Issue paper on the need for legislation governing privacy and data protection. Some of the important concepts, terms and words which are defined include: biometrics; cookies, cryptography; data processing;

data subject; hacking; personal data; profiling etc. It is apparent from the Issue Paper that the investigation into the protection of personal information should include:

a) Automatic and manual files;

b) Information pertaining to both natural and juristic persons;

c) Information kept by both the public and the private sector; and

d) Sound and image data.

E-Government is also cited as a specific example of data sharing in practice and outlining benefits and problems flowing from this, including problems with regard to perceptions.

15.2 ***Risk***

Breach of privacy could lead to interdicts, civil damages claims and, once data protection legislation is enacted, could result in criminal offences.

In terms of our common law the right to privacy is protected under the law of delict. It is also entrenched as a fundamental right in the Constitution of the Republic of South Africa[7]. There is no all-encompassing privacy or data protection legislation in South Africa. The ECT Act contains a voluntary section on protecting personal information collected by electronic means. The right to privacy is not absolute. However, the privacy of the individual has been awarded recognition in several cases.

The wrongfulness of a factual infringement of privacy is determined by means of the so-called boni mores or reasonableness criterion. This criterion considers the infringement of the right in light of the legal convictions of the community by assessing whether the infringement was reasonable or not. The presence of a ground of justification may exclude the wrongfulness of an invasion of privacy. For instance the public interest in information as a ground of justification plays an important role in respect of the publication of private facts by the mass media.

The constitutional right to privacy includes the right of a person not to have their person, home or property searched, their possessions seized, or the privacy of their communication infringed. When developing the common law, the courts must promote the spirit, purport and objects of the Bill of Rights.

15.3 ***Recommendation***

15.3.1 The IDMS must afford no lesser protection of personal information than that used in respect of the Department's existing records management system.

15.3.2 This implies more stringent security and access level requirements for an IDMS by virtue of the ease of access and dissemination of electronic records. The concepts of security and privacy are so closely related that they are often a source of confusion. The two are not separate, and for purposes of protecting individual information cannot be separated. Without strong security, personal information cannot be properly protected from misuse or abuse. Security policies must take breach of privacy risks into account.

15.3.3 The IDMS and the policies and procedures supporting it must make provision for an information classification system. An information management policy should record the information classification and indicate which records are e.g. restricted, classified or unrestricted.

[7] In section 14 of Chapter II of the Bill of Rights

16 CONFIDENTIALITY

16.1 *Description*

Various records are subject to express or implied confidentiality restrictions. As a general rule, records denoted on the face of it as confidential may only be accessed by the addressee.

16.2 *Risk*

If an unauthorised person obtains access to a record denoted as confidential, the originator of the record may have recourse to an interdict and claim for damages.

16.3 *Recommendation*

The same principles as discussed in paragraph 15 should be applied.

17 MONITORING & INTERCEPTION

17.1 *Description*

The Interception Act[8] has yet to come into operation but it is envisaged that it will be proclaimed during August/September 2004. It provides that subject to what is in the Act, no person may intentionally intercept or attempt to intercept directly or indirectly, at any place in the Republic, any communication in the course of its occurrence or transmission. There are various exceptions to this general prohibition. These are where the Interception is authorised by certain other Acts or carried out:

- for the purpose of executing an interception direction;
- to prevent serious bodily harm[i];
- for purposes of determining location in case of emergency;
- in circumstances where the interceptor is a party to the communication being intercepted;
- by law enforcement officers under certain circumstances;
- with the prior written consent of one of the parties to the communication;
- in respect of so-called indirect communications (including email), where this is done in connection with carrying on of business subject to certain requirements.

17.2 *Risk*

Email monitoring within an IDMS which does not conform to the Act may open the Department to criminal charges.

17.3 *Recommendation*

The following processes must be complied with:

17.3.1 Head of Department must expressly -

17.3.1.1 authorise interception “in ordinary course of business” and

17.3.1.2 designate person responsible for interception

17.3.2 Create formal monitoring & interception policy forming part of Communication Systems Usage Policy

[8] Regulation of Interception of Communications and Provision of Communicated Related Information Act 70 of 2002.

17.3.2.1 Not just an email policy

17.3.2.2 Policy must inform of interception in ordinary course of business

17.3.2.3 Ensure valid communication of this policy

18 RECORD RETENTION AND DOCUMENT IMAGING LEGAL COMPLIANCE

18.1 One can broadly distinguish between records received from other public or private bodies ("external records") and records generated by the department ("internal records"). Both external and internal records can be paper based or in electronic form.

18.2 Paper based records (internal or external) can be imaged (scanned) into the IDMS. Electronic records generated outside the IDMS can also be processed (saved/converted) into the IDMS. All these records then become part of the IDMS records and will be referred to as "IDMS ***processed*** documents".

18.3 Records generated (not imaged or saved) within the IDMS is referred to as "IDMS ***generated*** records".

18.4 IDMS ***processed*** and ***generated*** records must comply with section 16 of the ECT Act, which states:

> "(1) Where a law [e.g. the NARS Act] requires information to be retained, that requirement is met by retaining such information in the form of a data message, if-
>
> (a) the information contained in the data message is accessible so as to be usable for subsequent reference;
>
> (b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
>
> (c) the origin and destination of that data message and the date and time it was sent or received can be determined.
>
> (2) The obligation to retain information as contemplated in subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received."

18.5 As a general rule, it is permissible to perform document imaging and retain only the imaged document in lieu of the original.[9]

18.6 The following three principles must be complied with for purposes of the ECT Act:[10]

18.6.1 ***The electronic record must be accessible so as to be usable for subsequent reference***.

18.6.1.1 This requirement implies that the imaged record must be capable of being retrieved and read throughout its retention. It implies that the technology to read it must always remain available eg. where such technology is replaced with more modern technologies that do not support retrieval of the specified format.

18.6.2 ***The electronic record is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received***;

[9] Section 16 of the ECT Act, read with sections 11, 14, 15 and 17.
[10] Section 16 of ECT Act.

18.6.3 ***if the document was sent or received electronically the origin and destination of that document and the date and time it was sent or received must be determinable***.

18.7 Although not an express requirement of the ECT Act, it is paramount for any imaging process to be recorded in an information management policy with a procedures manual specifically governing the imaging process.

18.8 The policy must contain a record retention schedule indicating which records must be retained for what period in which form.

18.9 The most optimal way to ensure legal recognition and evidential weight of imaged records is to align the process with ISO/TR 15801. The likelihood is that this ISO standard may be adopted as a SANS standard in the near future.

18.10 Unless authorised by a Department's Legal advisors, the original paper document should not be destroyed if the document itself, as opposed to merely the information it conveys, is important for evidentiary purposes. Examples include:

18.10.1 fingerprints,

18.10.2 stains (e.g. blood stains),

18.10.3 whether it was folded (indicating it was sent by envelope),

18.10.4 special colours that my be lost during imaging,

18.10.5 official seals; or

18.10.6 where the depression marks of an original signature may be important to prove its authenticity.

18.11 As far as documentation which is subject to the VAT Act is concerned, SARS has issued the following guideline on 1 September 2002: Permission has been granted for computer scanning of documents, provided that the following requirements are met:

18.12 A proper audit trail is maintained.

18.13 The necessary equipment to reproduce paper copies of such documents will always be available at the vendor's premises.

18.14 Due to the fact that a copy of the original document is made, a paper copy of the document scanned should be clearly marked "copy".

18.15 An effective index should be maintained in respect of the scanned documents.

18.16 The database does not permit any alteration or manipulation of the scanned documents.

18.17 The scanned and subsequently printed documents should be of a good quality and allow for easy reading.

18.18 The original documents must be retained for a period of 12 months from the beginning of tax period to which they relate [section 55(4)]. However, the documents saved in electronic form must be retained for a period of 5 years as envisaged in section 55(3).

19 ELECTRONIC INVOICING

19.1 *Description*

Electronic invoices, debit and credit notes issued through an IDMS must conform to requirements set by the South African Revenue Services.

19.2 ***Risk***

Non-compliance may lead to penalties in terms of the VAT Act.

19.3 ***Recommendation***

The SARS requirements in respect of electronic tax invoices, as well as credit and debit notes, are as follows:-

19.3.1 The tax invoices, debit or credit notes must contain the mandatory information for tax invoices, credit or debit notes as stipulated in sections 20(4), 21(4)(a) and 21(4)(b) respectively.

19.3.2 Documents must be transmitted in encrypted form of at least 128 bytes.

19.3.3 Both the supplier and the recipient of the supply must retain the documents in readable and encrypted form for a period of five years from the date of the supply.

19.3.4 If a service provider is used, he must also retain the documents for a period of five years.

19.3.5 Both the supplier and the recipient of the supply must have the necessary codes or other means available to enable SARS auditors to compare the documents in readable form with those in encrypted form.

19.3.6 The transmitted electronic document will constitute the original tax invoice, credit or debit note. Hard copies extracted from the system must bear the words “computer generated tax invoice”, “computer generated copy credit note” or “computer generated copy debit note” thereon. All further copies must also bear such words.

19.3.7 The recipient of the supply must confirm in writing that he is prepared to accept electronic tax invoices, credit and debit notes under the conditions set out herein. Such authority must be retained by the supplier for a period of five years after the date of the last electronic document issued to the recipient.

19.3.8 No other tax invoice, credit or debit note may be issued in respect of the specific supply, unless such document is marked as a copy of the original document.

Yours faithfully

Wim Mostert

Partner

Deloitte Legal

wmostert@deloitte.co.za

SCHEDULE 1

IDMS Forms Approval List

If the forms to be used in the IDMS are not Z-Forms (see DPSA Regulations / Guidelines), the following **approval process** must be performed before the IDMS Forms Approval List is completed.

1 **APPROVAL PROCESS**

Name of Form	
Form Code	
From which Gov Department is Form received?	
Who completes the Form initially? (Who is the applicant?)	
Which official provides the required authorisation?	
To which official (other than the authorising official) is the Form submitted? Why?	

Is a copy made and, if so, who keeps the original and who keeps the copy?	
Which supporting documents must be provided. Are copies attached to the form?	
Can a person other than the rightful applicant commit a fraud by mere possession of the completed form?	
To which external Department / person or entity must the completed Form be submitted? Why?	

2 **FORMS APPROVED FOR IDMS AND REQUIREMENTS (IF ANY)**

Form name	Owner	Requirements	Date approved
Xyz	Procurement	None / See IDMS Manual	1 June 2004

SCHEDULE 2

RELEVANT EXTRACTS FROM ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 25 OF 2002

The central concept in the ECT Act (a ‘‘data message’’) is defined as:

> “data generated, sent, received or stored by electronic means and includes— (a) voice, where the voice is used in an automated transaction; and (b) a stored record.”

Legal recognition of data messages

11. (1) Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message.

Writing

12. A requirement in law that a document or information must be in writing is met if the document or information is—

(a) in the form of a data message; and

(b) accessible in a manner usable for subsequent reference.

Signature

13. (1) Where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.

(2) Subject to subsection (1), an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form.

(3) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if—

(a) a method is used to identify the person and to indicate the person’s approval of the information communicated; and

(b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.

(4) Where an advanced electronic signature has been used, such signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved.

(5) Where an electronic signature is not required by the parties to an electronic transaction, an expression of intent or other statement is not without legal force and effect merely on the grounds that—

(a) it is in the form of a data message; or

(b) it is not evidenced by an electronic signature but is evidenced by other means from which such person’s intent or other statement can be inferred.

Original

14. (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if—

(a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and

(b) that information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of subsection 1(a), the integrity must be assessed—

(a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;

(b) in the light of the purpose for which the information was generated; and

(c) having regard to all other relevant circumstances.

Admissibility and evidential weight of data messages

15. (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence—

(a) on the mere grounds that it is constituted by a data message; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message must be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard must be had to—

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the integrity of the data message was maintained;

(c) the manner in which its originator was identified; and

(d) any other relevant factor.

(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

Retention

16. (1) Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if—

(a) the information contained in the data message is accessible so as to be usable for subsequent reference;

(b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) the origin and destination of that data message and the date and time it was sent or received can be determined.

(2) The obligation to retain information as contemplated in subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

Production of document or information

17. (1) Subject to section 28, where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, and if—

(a) considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and

(b) at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference.

(2) For the purposes of subsection (1), the integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for—

(a) the addition of any endorsement; or

(b) any immaterial change, which arises in the normal course of communication, storage or display.

Notarisation, acknowledgement and certification

18. (1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message.

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, that requirement is met if the person provides a print-out certified to be a true reproduction of the document or information.

(3) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature.

Other requirements

19. (1) A requirement in a law for multiple copies of a document to be submitted to a single addressee at the same time, is satisfied by the submission of a single data message that is capable of being reproduced by that addressee.

(2) An expression in a law, whether used as a noun or verb, including the terms ‘‘document’’, ‘‘record’’, ‘‘file’’, ‘‘submit’’, ‘‘lodge’’, ‘‘deliver’’, ‘‘issue’’, ‘‘publish’’, ‘‘write in’’, ‘‘print’’ or words or expressions of similar effect, must be interpreted so as to include or permit such form, format or action in relation to a data message unless otherwise provided for in this Act.

(3) Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.

(4) Where any law requires or permits a person to send a document or information by registered or certified post or similar service, that requirement is met if an electronic copy of the document or information is sent to the South African Post Office Limited, is registered by the said Post Office and sent by that Post Office to the electronic address provided by the sender.