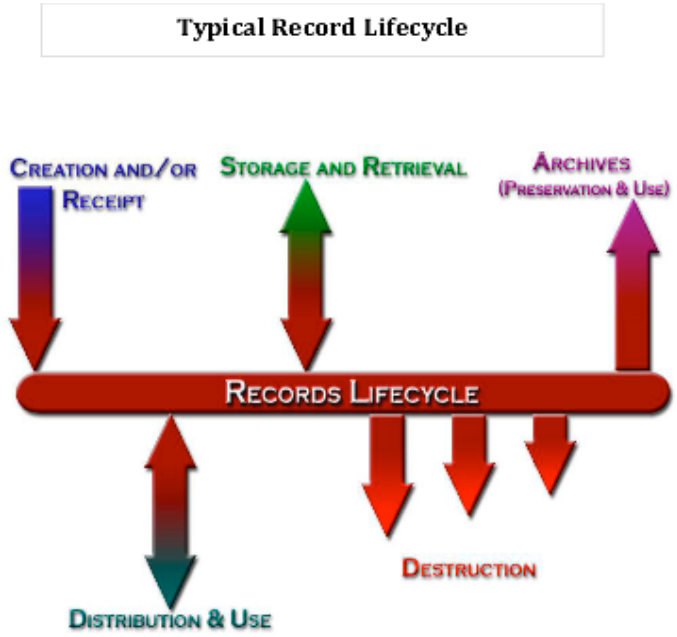
Appendix 4: DRAFT Guide to Establishing an Effective Records/Document Management System

This is a **DRAFT** guide, with best practices and expressions for desired future state, for anyone considering implementing a new document management system, or refreshing an existing one. This "business" checklist covers questions and topics related to documents' and records' entire lifecycle, from creation (or acquisition) through final disposition; it does not address any IT issues.

We recommend that there be a follow-up activity that would refine/amplify/vet this guide, and make it generally available to the MIT community. Additionally, we recommend that the MIT Policies be reviewed and updated to make more operationally useful.

- *MIT-wide Printing & Digital Archiving Team, February 7, 2011*



Appendix 4: DRAFT Guide to Establishing an Effective Records/Document Management System

Overarching best practice/recommendation:

In a perfect world, there would be only one copy that could be accessed from anywhere by any authorized person.

However, since the perfect world is not here, individual records management systems will need to address multiple issues.

TOPIC: What records and/or documents are included; why are they collected/retained; who needs to access them?

Current State

Many records management 'systems' consist of mass scanning of all paper files; there may be little or no assessment of the document lifecycle or the purpose for the documents.

Best Practice/Desired Future State

Any records management project should first consider the basic questions related to records and document lifecycle: who, what, where, why and how. Until these questions are discussed, and common understanding is reached, it will be difficult to address the other topics, or to select a technology to support the business needs.

Examples of questions to discuss:

What kinds of documents/records do we have? Are they:

- Transactional? (e.g. travel expense reports, requests for payment, etc. - generally well structured.)
- Less structured items, such as
  - Documents? (e.g. contracts, presentations, reports, project plans, budget, etc, where there are likely to be iterative versions, with multiple inputs, culminating with a final/official version)
  - References? (e.g. departmental policy/procedures, etc, which, once finalized, are generally static)
  - Other? (e.g. transitory items such as meeting arrangement logistics, or items that may have historical value, such as meeting notes)

How sensitive is the information?

- Regulated personal data (aka PIRN)?

Student information?
MIT confidential (e.g. HR data, business operations, contract negotiations)?
Intellectual property/research data?
Other sensitivity?

What processes the items are part of, and who (individual or department) is responsible for that process?
What are the process flow, and media? (e.g. all digital? Paper with data entry? etc.)
Who will need access (by name or role) and any time restrictions (e.g. only for 1 year)?

TOPIC: What are the relevant standards for protecting information?

Current State

In many cases there are Federal or state regulations, or industry norms that should guide the decisions regarding handling, storage and destruction of certain personal information or business data. Business Process Owners are in the best position to understand the relevant compliance landscape and to make recommendations or set policy for the users of those processes.

MIT has overarching information policies:
MIT Policy 11.0 addresses Privacy and Disclosure of information http://web.mit.edu/policies/11/index.html
MIT Policy 13.0 addresses Information Policies http://web.mit.edu/policies/13/index.html
including Archival Policy and Records Management Program, which have some internal inconsistency.

For regulated personal information (aka PIRN) see MIT's information security program
http://web.mit.edu/infoprotect/wisp/index.html

Best Practice/Desired Future State

Departments should ensure that records/documents are protected as per regulations and MIT policy. In addition to access controls, there may need to be logs of who has accessed what, as well as ability to ensure records are properly disposed of when no longer needed.

The MIT Policies should be clarified, to address the internal inconsistencies as well as contemporary business needs.

Appendix 4: DRAFT Guide to Establishing an Effective Records/Document Management System

TOPIC: Who can access the information and how will access be managed?

Current State

Access rules will vary based on business process/system, and whether records are digital or physical.
The Roles application maintained by IS&T manages access to several central systems (e.g. Data Warehouse). While there are good processes in place for updating access when an employee leaves, there are less consistent methods of ensuring updates if an employee changes roles, or for non-employee access (e.g. contractor).
Departments manage access to local file systems, shared servers etc.
Depending on the software, the type of access may also vary – read only, read/write, download, share with others, etc.

Best Practice/Desired Future State

The ideal would be a holistic/integrated access management system, to help ensure the right people have type of access (based on rules), and access is automatically removed when role changes (e.g. termination)

In the interim, departments should understand existing access rules, and integrate with existing systems (e.g. Roles) where possible. For locally managed system, access management should be linked to HR, so as personnel change roles, (e.g. termination), their access can be updated as appropriate. Rules and processes for non-employee access should also be defined. There should also be a mechanism for periodic (minimally, annual) reviews of access lists.

TOPIC: When is it a 'document of record', vs copy or early version?

Current State

There is a lack of clarity who (DLC, central Admin) is responsible for the official system of record for transactional records, such as RFPs, HR forms, etc. There is also difficulty knowing whether a document (e.g. contract) is the final/official version

Appendix 4: DRAFT Guide to Establishing an Effective Records/Document Management System

Best Practice/Desired Future State

Choose records management products with good version control for documents, so it is clear which version is the final/official version (a la a contract), as well as ability to track who made what changes (some may be useful for historical purposes); digital signatures may also be used to facilitate document authenticity
For transactional processes, clarify re: who has the official copy – DLC or central?
Note: although documents may be in an electronic system, IT is not considered the 'owner' – the department/person responsible for the content or the business process remains the owner.

TOPIC: How long does a record or document need to be kept?

Current State

A set of some retention schedules exists at http://libraries.mit.edu/records/. However, retention schedules do not exist for many records and document types, and, where schedules exist, they may not be consistent with the current processes (e.g. schedule discusses paper retention, when the current process is fully digital).

There may also be different retention needs for DLCS (where access to a local copy for reference purposes may be desirable), central admin (which may be the official record for audit/compliance purposes), Legal (which may require a litigation hold which supersedes any records management policy), Archivist (which may have interest from historical perspective).

Best Practice/Desired Future State

Each business process owner should maintain publically [MIT only] available retention schedules for the processes they are responsible for. The schedules should consider regulatory requirements as well as business needs. However, the default should not be to keep information indefinitely, simply because storage cost is low. Schedules should be reviewed and updated when business processes change.

In the event that schedules do not exist, DLCs should consult with business process owners early in the process, and establish schedules for records under their stewardship.

Appendix 4: DRAFT Guide to Establishing an Effective Records/Document Management System

Assuming schedules exist, look for records management software which will enforce the schedules (as well as the ability to suspend the rules, in the event of a litigation hold) Holders of information need to be aware of the risks to MIT if data is not kept long enough, as well as the risks if kept longer than needed. (e.g., implications for e-discovery).

TOPIC: When should record/document be transferred (e.g. from local storage to offsite; from departmental files to Institute Archives)?

Current State

Although MIT Policy 13.0 http://web.mit.edu/policies/13/index.html discusses the role of the Institute Archives and MIT's records management policy, it may not provide sufficient guidance for specific implementations. There is also no central facility for the archival of digital records.

Best Practice/Desired Future State

Contact the Institute Archivist early in the records management process to understand which, if any, of the records being considered would have Institutional archival value, and document the understanding of when/how records will be transferred.

DLC's should also contact relevant central admin groups, to determine which, if any, of the records need to be retained locally, and how local archives will be managed/maintained.

In the future, it would be desirable to have a digital repository for permanent records.

TOPIC: how should records/documents be disposed of, when no longer needed?

Current State

Departments use a wide range of approaches – office shredders of various types, recycling services, locked shredding bins, annual cleanups, which may or may not ensure that records are properly disposed of.

Appendix 4: DRAFT Guide to Establishing an Effective Records/Document Management System

Best Practice/Desired Future State

For paper: unless sensitive information is consistently kept separate from non-sensitive information, it is prudent to treat all paper as sensitive. See xxx for more detail on shredders and shredding services.

For digital records/documents: records management software typically will include options to automatically securely delete documents/records based on user defined rules. In the absence of such tool, departments should outline a process for manual purges.

For digital devices: most digital devices, including computers, smart phones, copiers, printers, fax machines, USB drives etc. should be 'sanitized' prior to disposal. This process ensures that any files on the device are removed. See xxx for more information.

For digital media such as CDs, DVDs, flash drives, physical destruction is often the preferred approach.
NOTE: Whatever process is established for disposal should have mechanisms to suspend the rules, in the event of a litigation hold

TOPIC: What does a 'signature' or 'approval' mean and how are they handled in the workflow processing?

Current State

There are 'wet' signatures (handwritten signature on paper), and 'digital signatures' (which may be a digitized version of the wet signature, or, more likely, is some type of digital authentication). For example, some MIT applications use an digital certificate to validate the user, and the user clicks a box or button to signal approval (e.g., e-DACCA). The combination of these factors, along with other items, such as an electronic date stamp, comprise a type of digital signature. As per US Law, a digital signature carries the same legal weight as a wet signature. Wet signatures may still be used when the 'symbolism' of pen-to-paper is preferred, such as a significant contract, or a large donation.

Appendix 4: DRAFT Guide to Establishing an Effective Records/Document Management System

Best Practice/Desired Future State

There needs to be clear understanding of who is responsible for what type of approval. 'Approval' may range from asserting that certain information has been reviewed, to approval for committing resources to an activity, to a collective agreement that a document represents everyone's final position. The type of approval will influence the choice of how that approval is recorded.

As workflows become more automated, it makes sense to incorporate digital signatures – there is little value to having a digital workflow, if paper has to be produced for someone to physically sign. Whether and when to use digital signatures should be a risk-based assessment, including General Counsel.

TOPIC: How many media formats need to be supported – paper, digital, images, voice, etc.?

Current State

Many MIT business processes handle information flows through a mix of paper and electronic media (e.g. depts. can use paper RFP or electronic RFP; those using electronic RFPs may still keep a paper screen print, or other record)

Best Practice/Desired Future State

Having a consistent media format for all uses of a given process improves efficiency and reduces the chances of errors. When updating a process, promote convergence by allowing time for people to adopt the new, but include a firm sunset date for the old process. Avoid building a new system that treats all the existing variations as equally supported ("paving the cow paths").

TOPIC: How should 3rd party service providers/software companies be evaluated?

1. Understand the driver for records management: to improve document workflow? to facilitate document retrieval? To enable more collaborative document creation? To better support distributed workgroup? Simply need to recover floor space? Etc. (Different vendors have strengths in different areas.)

2. Understand what, if any, regulations may apply – e.g. records containing sensitive personal information, such as SSN, or research data, may have some regulatory requirements that any vendor would need to address. For example, there may need to be specific language in the 3rd party contract with regard to roles and responsibilities for protecting data, and reporting breaches.
3. Understand your environment –
    a. Will you need to support both PCs and Macs? (some vendors' products have a less functionality for Mac users);
    b. Where will the data physically reside – will you have your own local server? Or use an IS&T managed server? Or will the data be 'in the cloud'? – this will also link to the question of regulatory requirements for data protection)
    c. Do you have access to IT staff? (some vendors' customization options involve programming; others offer 'drag and drop' customization options that a competent knowledge worker can learn);
4. Understand data flows well enough to know what input/output devices and technologies need to be considered (e.g. fax machines, multifunction devices, bar code readers)
5. What kind of support for document lifecycle is needed (e.g. version control, digital signatures, automated retention rules, archiving, data persistence; support for litigation holds; support for true redaction; support for document annotation; retaining PDFs as both image and text files)
6. Will the system need to be integrated with email? If so, to what degree? (e.g. sending email alerts if there is something new in a workflow inbox; capturing all emails that part of a contract negotiation thread; etc)
7. How does it handle data security? What are the deterrents to/detection of unauthorized access?
8. **How is access granted to those outside the workgroup** and how easy is it to give access? How granular can access be set – file level, document level, parts of documents? (e.g. to support collaboration between MIT and Harvard researchers, or a process with many participants, some of who should not see information created by others) PROCESS Touchstone authentication for MIT Affiliate with local system access vs. Kerberos certificate broad access
9. What kind of searching will need to be supported (e.g. Metadata search and/or content search)?

10. What reporting tools exist, and how easy are they to use? (e.g. reports of how long records are 'in' the workflow; how many documents are older than a certain date, etc.)
11. Scalability – can system grow with dept/usage?
12. Licensing models – concurrent, per seat etc.

Appendix 4: DRAFT Guide to Establishing an Effective Records/Document Management System

Reference document	Summary	Recommendations
11.0 Privacy and Disclosure of Information	Addresses privacy of personal information – staff, and students; includes Student Information Policy (11.3)	Digitizing can make information more broadly accessible. Recommend appropriate use of privacy and access controls.
13.0 Information Policies	Addresses intellectual property (ownership, copyright, tech transfer) , use of IT (security, etc.) (13.2), MIT's Archival Policy (13.3) and Records Management program (13.4)	Some of the policy language is dated and reflects a largely paper-based world. The Archival Policy and Records Management program are somewhat conflicting. Any new process needs to define appropriate records management policy. A review and update is recommended.
Institute Archives & Special Collections Records Management Program at MIT http://libraries.mit.edu/records/index.html	Provides guidance for archiving and retention of records, particularly of Financial and TLO records	Last major update was in 2007. The VPF Digital Archiving Team is conducting a review and update in conjunction with Office of General Counsel, Audit Division and Institute Archivist. The updated document should consider records pertaining to HR and other relevant business processes.