Management Topics

Records Management

Records Management is the practice of identifying, classifying, archiving, preserving, and destroying records. There is an International Standard on records management, ISO 15489: 2001. This defines records management as, "The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records".

The ISO defines **records** as "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business". The International Council on Archives (ICA) Committee on Electronic Records defines a **record** as, "a specific piece of recorded information generated, collected or received in the initiation, conduct or completion of an activity and that comprises sufficient content, context and structure to provide proof or evidence of that activity". While the definition of a record is often identified strongly with a document, a record can be either a tangible object or digital information which has value to an organization. For example, birth certificates, medical x-rays, office documents, databases, application data, and e-mail are all examples of records.

Practicing Records Management

The practice of records management involves all of the following activities:

- Creating, approving, and enforcing records policies, including a classification system and a records retention policy

- Developing a records storage plan, which includes the short and long-term housing of physical records and digital information

- Identifying existing and newly created records, classifying them, and then storing them according to standard operating procedures

- Coordinate the access and circulation of records within and even outside of an organization

- Executing a retention policy to archive and destroy records according to operational needs, operating procedures, statutes, and regulations

Often, a records management system helps to aid in the capture, classification, and ongoing management of records throughout their lifecycle. Such a system may be paper based (such as index cards as used in a library), or may be a computer system, such as an electronic records management application.

ISO 15489:2001 States that Records Management Includes:

- setting policies and standards;

- assigning responsibilities and authorities;

- establishing and promulgating procedures and guidelines;

- providing a range of services relating to the management and use of records;

- designing, implementing and administering specialized systems for managing records; and
- integrating records management into business systems and processes.

Managing Physical Records

Managing physical records involves a variety of diverse disciplines. At the simplest, physical records must be organized and indexed. In more complex environments, records management demands expertise in forensics, history, engineering, and law. Records management then resolves to be a coordination of many experts to build and maintain the system.

Records must be identified and authenticated. In a business environment, this is usually a matter of filing business documents and making them available for retrieval. However, in many environments, records must be identified and handled much more carefully.

- **Identifying records.** If an item is presented as a record, it must be first examined as to its relevance, and it must be authenticated. Forensic experts may need to examine a document or artifact to determine that it is not a forgery, or if it is genuine, that any damage, alterations, or missing content is documented. In extreme cases, items may be subjected to a microscope, x-ray, radiocarbon dating or chemical analysis to determine their authenticity and prior history. This level of authentication is rare, but requires that special care be taken in the creation and retention of the records of an organization.
- **Storing records.** Records must be stored in such a way that they are both sufficiently accessible and are safeguarded against environmental damage. A typical contract or

agreement may be stored on ordinary paper in a file cabinet in an office. However, many records file rooms employ specialized environmental controls including temperature and humidity. Vital records may need to be stored in a disaster-resistant safe or vault to protect against fire, flood, earthquakes and even war. In extreme cases, the item may require both disaster-proofing and public access, which is the case with the original, signed US Constitution. Even civil engineers must be consulted to determine that the file room can effectively withstand the weight of shelves and file cabinets filled with paper; historically, some military vessels were designed to take into account the weight of their operating procedures on paper as part of their ballast equation (modern record-keeping technologies have transferred much of that information to electronic storage). In addition to on-site storage of records, many organizations operate their own off-site records centers or contract with commercial records centers.

- **Circulating records.** Records are stored because they may need to be retrieved at some point. Retrieving, tracking the record while it is away from the file room, and then returning the record, is referred to as circulation. At its simplest, circulation is handled by manual methods such as simply writing down who has a particular record, and when they should return it. However, most modern records environments use a computerized records management system that includes the ability to employ bar code scanners for better accuracy, or radio-frequency identification technology (RFID) to track movement of the records from office to office, or even out of the office. Bar code and RFID scanners can also be used for periodic auditing to ensure that unauthorized movement of the record is tracked.

- **Dispositioning of records.** Disposition of records does not always mean destruction. Disposition can also include transfer of records to a historical archive, to a museum, or even

to a private party. When physical records are destroyed, the records must be authorized for destruction by law, statute, regulation, and operating procedure. Once approved, the record must be disposed of with care to avoid inadvertent disclosure of information to unauthorized parties. The process to dispose of records needs to be well-documented, starting with a records retention schedule and policies and procedures that have been approved at the highest level of an organization. An inventory of the types of records that have been disposed of must be maintained, including certification that the records have been destroyed. Records should never simply be discarded as any other refuse. Most organizations use some form of records destruction including pulverization, paper shredding or incineration.

Managing Electronic Records

The general principles of records management apply to records in any format. Digital records (almost always referred to as electronic records) raise specific issues however. It is more difficult to ensure that the content, context and structure of records is preserved and protected when the records do not have a physical existence. Guidance on the management of electronic records can be found on the websites of National and State Archives authorities listed below.

Unlike physical records electronic records cannot be managed without a computer or other machine. Functional requirements for computer systems that can be used to manage electronic records have been produced by the US Department of Defense DoD 5015.2, the National Archives of England & Wales and the European Commission MoREQ. It is noteworthy that the

Moreq specification has been translated into at least twelve languages and is used beyond the borders of Europe. Development of MoReq was initiated by the DLM Forum, funded by the [MoReq European Commission].

Particular concerns exist about the ability to retain and still be able to access and read electronic records over time. Electronic records require appropriate combinations of software versions and operating systems to be accessed, and so are at risk because of the rate at which technological changes occur. A considerable amount of research is being undertaken to address this issue, under the heading of digital preservation.

Current Issues in Records Management

As of 2005, records management has increased interest among corporations due to new compliance regulations and statutes. While government, legal, and healthcare entities have a strong, historical records management discipline, general record-keeping of corporate records has been poorly standardized and implemented. In addition, scandals such as the Enron/Andersen scandal, and more recently records-related mishaps at Morgan Stanley, have renewed interest in corporate records compliance, litigation preparedness, and issues. Statutes such as the US Sarbanes-Oxley Act have created new concerns among corporate "compliance officers" that result in more standardization of records management practices within an organization. Most of the 90s has seen discussions between records managers and IT managers, and the emphasis has expanded to include the legal aspects, as it is now focused on compliance and risk.

Privacy, data protection, and identity theft have become issues of interest for records managers. The role of the records manager to aid in the protection of an organization's records has often grown to include attention to these concerns. The need to ensure that certain information about individuals is not retained has brought greater focus to records retention schedules and records destruction.

Related topics of current note include: information lifecycle management and enterprise content management.

Education and Certification

Records management, being a complex practice, involves many years of education and practice for full mastery. Many colleges and universities offer degree programs in library and information sciences. Furthermore, there are professional organizations such as the Records Management Association of Australasia (RMAA) (RMAA) Association of Records Managers and Administrators (ARMA International) and the Institute of Certified Records Managers which provides a separate, non-degreed, professional certification for practitioners, the Certified Records Manager designation or CRM. Additional educational opportunities are also available from AIIM International and from the Records Management Society of the UK and Ireland. Education and training courses and workshops on scientific and technical records full lifecycle management and the Quality Electronic Records Practices Standards (Q-ERPS) are available from CENSA, the Collaborative Electronic Notebook Systems Association.

Records Management Systems

A **records management system** is a computer program (or set of programs) used to track and store records. The term is distinguished from imaging and document management systems that specialize in paper capture and document management respectively. Records management systems commonly provide specialized security and auditing functionalities tailored to the needs of records managers.

The National Archives and Records Administration (NARA) has endorsed the U.S. Department of Defense 5015.2-STD as an "adequate and appropriate basis for addressing the basic challenges of managing records in the automated environment that increasingly characterizes the creation and use of records." Records Management Vendors can be certified as compliant with the DoD 5015.2-STD after verification from the Joint Interoperability Test Command (JITC) which builds test case procedures, writes detailed and summary final reports on 5015.2-certified products, and performs on-site inspection of software.

The National Archives (UK) has published two sets of functional requirements to promote the development of the electronic records management software market (1999 and 2002). It ran a program to evaluate products against the 2002 requirements. Whilst these requirements were initially formulated in collaboration with central government, they have been taken up with enthusiasm by many parts of the wider public sector in the UK and in other parts of the world. The testing program has now closed; The National Archives is no longer accepting applications for testing. The National Archives 2002 requirements remain current.

A European Commission project to develop MoReq2 has started. This is due to be completed at the end of 2007, and the National Archives will need to make a judgement as to whether MoReq2 is an appropriate successor.

Commercial Records Centers

Commercial records centers are facilities which specialize in the storage of paper and electronic records for organizations. Commercial records centers provide high density, secure storage for paper records and can provide climate controlled storage for sensitive non-paper media. The trade organization for commercial records centers is PRISM International.

Risk Management

Risk management is the process of measuring, or assessing, risk and developing strategies to manage it. Strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk. Traditional risk management focuses on risks stemming from physical or legal causes (e.g. natural disasters or fires, accidents, death, and lawsuits). Financial risk management, on the other hand, focuses on risks that can be managed using traded financial instruments.

Explanation

In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled later. In practice the process can be very difficult, and balancing between risks with a high probability of occurrence but lower loss vs. a risk with high loss but lower probability of occurrence can often be mishandled.

Intangible risk management identifies a new type of risk - a risk that has a 100% probability of occurring but is ignored by the organization due to a lack of identification ability. For example, knowledge risk occurs when deficient knowledge is applied. Relationship risk occurs when collaboration ineffectiveness occurs. Process-engagement risk occurs when operational ineffectiveness occurs. These risks directly reduce the productivity of knowledge workers, decrease cost effectiveness, profitability, service, quality, reputation, brand value, and earnings quality. Intangible risk management allows risk management to create immediate value from the identification and reduction of risks that reduce productivity.

Risk management also faces difficulties allocating resources. This is the idea of opportunity cost. Resources spent on risk management could have been spent on more profitable activities. Again, ideal risk management minimizes spending while maximizing the reduction of the negative effects of risks.

Steps in the Risk Management Process

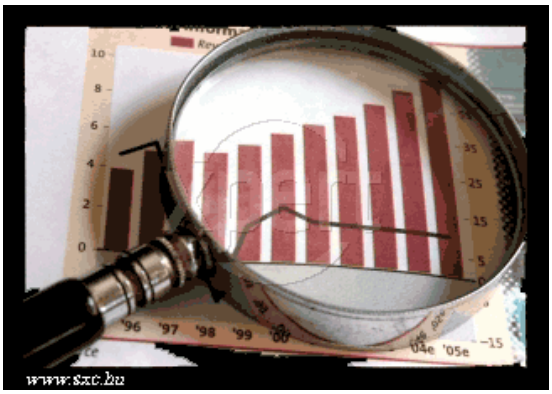
Establish the Context

Establishing the context involves

1. **Planning** the remainder of the process.
2. **Mapping out** the following: the scope of the exercise, the identity and objectives of stakeholders, and the basis upon which risks will be evaluated.
3. **Defining a framework** for the process and an agenda for identification.
4. **Developing an analysis** of risk involved in the process.

Identification

After establishing the context, the next step in the process of managing risk is to identify potential risks. Risks are about events that, when triggered, cause problems. Hence, risk identification can start with the source of problems,
or with the problem itself.



- **Source analysis** Risk sources may be internal or external to the system that is the target of risk management. Examples of risk sources are: stakeholders of a project, employees of a company or the weather over an airport.

- **Problem analysis** Risks are related to identified threats. For example: the threat of losing money, the threat of abuse of privacy information or the threat of accidents and casualties. The threats may exist with various entities, most important with shareholder, customers and legislative bodies such as the government.

When either source or problem is known, the events that a source may trigger or the events that can lead to a problem can be investigated. For example: stakeholders withdrawing during a project may endanger funding of the project; privacy information may be stolen by employees even within a closed network; lightning striking a Boeing 747 during takeoff may make all people onboard immediate casualties.

The chosen method of identifying risks may depend on culture, industry practice and compliance. The identification methods are formed by templates or the development of templates for identifying source, problem or event. Common risk identification methods are:

- **Objectives-based risk identification** Organizations and project teams have objectives. Any event that may endanger achieving an objective partly or completely is identified as risk. Objective-based risk identification is at the basis of COSO's Enterprise Risk Management - Integrated Framework

- **Scenario-based risk identification** In scenario analysis different scenarios are created. The scenarios may be the alternative ways to achieve an objective, or an analysis of the interaction of forces in, for example, a market or battle. Any event that triggers an undesired scenario alternative is identified as risk.

- **Taxonomy-based risk identification** The taxonomy in taxonomy-based risk identification is a breakdown of possible risk sources. Based on the taxonomy and knowledge of best practices, a questionnaire is compiled. The answers to the questions reveal risks.

- **Common-risk Checking** In several industries lists with known risks are available. Each risk in the list can be checked for application to a particular situation.

- **Risk Charting** This method combines the above approaches by listing Resources at risk, Threats to those resources Modifying Factors which may increase or reduce the risk and Consequences it is wished to avoid. Creating a matrix under these headings enables a variety of approaches. One can begin with resources and consider the threats they are exposed to and the consequences of each. Alternatively one can start with the threats and examine which

resources they would affect, or one can begin with the consequences and determine which combination of threats and resources would be involved to bring them about (Crockford 1986)

Assessment

Once risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of the probability of an unlikely event occurring. Therefore, in the assessment process it is critical to make the best educated guesses possible in order to properly prioritize the implementation of the risk management plan.

The fundamental difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kinds of past incidents. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for immaterial assets. Asset valuation is another question that needs to be addressed. Thus, best educated opinions and available statistics are the primary sources of information. Nevertheless, risk assessment should produce such information for the management of the organization that the primary risks are easy to understand and that the risk management decisions may be prioritized. Thus, there have been several theories and attempts to quantify risks. Numerous different risk formulae exist, but perhaps the most widely accepted formula for risk quantification is:

Rate of Occurrence Multiplied by the Impact of the Event Equals Risk

Later research has shown that the financial benefits of risk management are less dependent on the formula used but are more dependent on the frequency and how risk assessment is performed.

In business it is imperative to be able to present the findings of risk assessments in financial terms. Robert Courtney Jr. (IBM, 1970) proposed a formula for presenting risks in financial terms. The Courtney formula was accepted as the official risk analysis method for the US governmental agencies. The formula proposes calculation of ALE (annualized loss expectancy) and compares the expected loss value to the security control implementation costs (cost-benefit analysis).

Potential Risk Treatments

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories: (Dorfman, 1997) (remember as 4 T's)

- **Tolerate** (aka **retention**)
- **Treat** (aka **mitigation**)
- **Terminate** (aka **elimination**)
- **Transfer** (aka **buying insurance**)

Ideal use of these strategies may not be possible. Some of them may involve trade-offs that are not acceptable to the organization or person making the risk management decisions.

Risk Avoidance

Includes not performing an activity that could carry risk. An example would be not buying a property or business in order to not take on the liability that comes with it. Another would be not flying in order to not take the risk that the airplane were to be hijacked. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits.

Risk Reduction

Involves methods that reduce the severity of the loss. Examples include sprinklers designed to put out a fire to reduce the risk of loss by fire. This method may cause a greater loss by water damage and therefore may not be suitable. Halon fire suppression systems may mitigate that risk, but the cost may be prohibitive as a strategy.

Modern software development methodologies reduce risk by developing and delivering software incrementally. Early methodologies suffered from the fact that they only delivered software in the final phase of development; any problems encountered in earlier phases meant costly rework and often jeopardized the whole project. By developing in iterations, software projects can limit effort wasted to a single iteration. A current trend in software development, spearheaded by the Extreme Programming community, is to reduce the size of iterations to the smallest size possible, sometimes as little as one week is allocated to an iteration.

Risk Retention

Involves accepting the loss when it occurs. True self insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

Risk Transfer

Means causing another party to accept the risk, typically by contract or by hedging. Insurance is one type of risk transfer that uses contracts. Other times it may involve contract language that transfers a risk to another party without the payment of an insurance premium. Liability among construction or other contractors is very often transferred this way. On the other hand, taking offsetting positions in derivatives is typically how firms use hedging to financially manage risk.

Some ways of managing risk fall into multiple categories. Risk retention pools are technically retaining the risk for the group, but spreading it over the whole group involves transfer among individual members of the group. This is different from traditional insurance, in that no premium is exchanged between members of the group up front, but instead losses are assessed to all members of the group.

Create the Plan

Decide on the combination of methods to be used for each risk. Each risk management decision should be recorded and approved by the appropriate level of management. For example, a risk concerning the image of the organization should have top management decision behind it whereas IT management would have the authority to decide on computer virus risks.

The risk management plan should propose applicable and effective security controls for managing the risks. For example, an observed high risk of computer viruses could be mitigated by acquiring and implementing antivirus software. A good risk management plan should contain a schedule for control implementation and responsible persons for those actions. The risk management concept is old but is still not very effectively measured

Implementation

Follow all of the planned methods for mitigating the effect of the risks. Purchase insurance policies for the risks that have been decided to be transferred to an insurer, avoid all risks that can be avoided without sacrificing the entity's goals, reduce others, and retain the rest.

Review and Evaluation of the Plan

Initial risk management plans will never be perfect. Practice, experience, and actual loss results will necessitate changes in the plan and contribute information to allow possible different decisions to be made in dealing with the risks being faced.

Risk analysis results and management plans should be updated periodically. There are two primary reasons for this:

1. to evaluate whether the previously selected security controls are still applicable and effective, and

2. to evaluate the possible risk level changes in the business environment. For example, information risks are a good example of rapidly changing business environment.

Limitations

If risks are improperly assessed and prioritized, time can be wasted in dealing with risk of losses that are not likely to occur. Spending too much time assessing and managing unlikely risks can divert resources that could be used more profitably. Unlikely events do occur but if the risk is unlikely enough to occur it may be better to simply retain the risk and deal with the result if the loss does in fact occur.

Prioritizing too highly the *risk management processes* could keep an organization from ever completing a project or even getting started. This is especially true if other work is suspended until the risk management process is considered complete.

It is also important to keep in mind the distinction between risk and uncertainty. Risk can be measured by impacts x probability.

Areas of Risk Management

As applied to corporate finance, **risk management** is a technique for measuring, monitoring and controlling the financial or operational risk on a firm's balance sheet. See value at risk.

The Basel II framework breaks risks into market risk (price risk), credit risk and operational risk and also specifies methods for calculating capital requirements for each of these components.

Enterprise Risk Management

In enterprise risk management, a risk is defined as a possible event or circumstance that can have negative influences on the Enterprise in question. Its impact can be on the very existence, the resources (human and capital), the products and services, or the customers of the enterprise, as well as external impacts on society, markets, or the environment.

In addition, every probable risk can have a pre-formulated plan to deal with its possible consequences (to ensure *contingency* if the risk becomes a *liability*).

From the information above and the average cost per employee over time, or cost accrual ratio, a project manager can estimate

- the cost associated with the risk if it arises, estimated by multiplying employee costs per unit time by the estimated time lost (*cost impact, C* where *C = cost accrual ratio * S*).
- the probable increase in time associated with a risk (*schedule variance due to risk, Rs* where Rs = P * S):
    - Sorting on this value puts the highest risks to the schedule first. This is intended to cause the greatest risks to the project to be attempted first so that risk is minimized as quickly as possible.

    - This is slightly misleading as *schedule variances* with a large P and small S and vice versa are not equivalent. (The risk of the RMS *Titanic* sinking vs. the passengers' meals being served at slightly the wrong time).

- the probable increase in cost associated with a risk (*cost variance due to risk, Rc* where Rc = P*C = P*CAR*S = P*S*CAR)

    - sorting on this value puts the highest risks to the budget first.

    - see concerns about *schedule variance* as this is a function of it, as illustrated in the equation above.

Risk in a project or process can be due either to Special Cause Variation or Common Cause Variation and requires appropriate treatment. That is to re-iterate the concern about extreme cases not being equivalent in the list immediately above.

Risk Management Activities as Applied to Project Management

In project management, risk management includes the following activities

- Planning how risk management will be held in the particular project. Plan should include risk management tasks, responsibilities, activities and budget.

- Assigning a risk officer - a team member other than a project manager who is responsible for foreseeing potential project problems. Typical characteristic of risk officer is a healthy skepticism.

- Maintaining live project risk database. Each risk should have the following attributes: opening date, title, short description, probability and importance. Optionally a risk may have an assigned person responsible for its resolution and a date by which the risk must be resolved.

- Creating anonymous risk reporting channel. Each team member should have possibility to report risk that he foresees in the project.

- Preparing mitigation plans for risks that are chosen to be mitigated. The purpose of the mitigation plan is to describe how this particular risk will be handled – what, when, by who and how will it be done to avoid it or minimize consequences if it becomes a liability.

- Summarizing planned and faced risks, effectiveness of mitigation activities and effort spend for the risk management

Risk Management and Business Continuity

Risk management is simply a practice of systematically selecting cost effective approaches for minimizing the effect of threat realization to the organization. All risks can never be fully avoided or mitigated simply because of financial and practical limitations. Therefore all organizations have to accept some level of residual risks.

Whereas risk management tends to be pre-emptive, business continuity planning (BCP) was invented to deal with the consequences of realized residual risks. The necessity to have BCP in place arises because even very unlikely events will occur if given enough time. Risk

management and BCP are often mistakenly seen as rivals or overlapping practices. In fact these processes are so tightly tied together that such separation seems artificial. For example, the risk management process creates important inputs for the BCP (assets, impact assessments, cost estimates etc). Risk management also proposes applicable controls for the observed risks. Therefore, risk management covers several areas that are vital for the BCP process. However, the BCP process goes beyond risk management's pre-emptive approach and moves on from the assumption that the disaster **will** realize at some point.