

WHITE PAPER



PRESENTED BY:



KNOWLEDGE MANAGEMENT:

**HOW KNOWLEDGE MANAGEMENT AS APPLIED TO INFOSEC
REDUCES CHAOS AND ENSURES SMOOTHER OPERATION OF
COMPLIANCE SYSTEMS**

James D. Heimberg, ABC, Ph.D., ISSO

March 23, 2006

INTRODUCTION

Federal Network Services, Inc., Information Security (INFOSEC) Services practice is pleased to present this white paper that describes how knowledge management in support of INFOSEC reduces administrative overhead associated with systems maintenance and increases the value of the enterprise by identifying intangible assets.

Intangible assets consist of the tacit knowledge and intellectual property of an organization. Those assets are used to provide a basis from which the organization can make decisions, excel, and prosper. The science of collecting this knowledge and making it explicit is the practice of knowledge management. Little of the discussion of knowledge management has focused on what to do with the information as it is being brought from the tacit stage to the explicit stage or what to do with it once it is explicit. This white paper addresses the practical side of knowledge management with a focus on what it means to an enterprise. Its value is based on gaining an understanding of the intellectual assets.

Most businesses with a knowledge management practice are learning how knowledge management adds to the bottom-line value of the organization. Many of the buzzwords of the past related to knowledge management have come and gone. For some, this is due to an inability to understand why, for some because of the cost of implementation, and for some due to the inability of an organization to capitalize on the concept.

If owners, chief executives, and an executive management team are not to be forced into the role of micro-management, the people involved must trust, trust the people who take the data of business, combine it into meaningful information, and manipulate it into business know-how, in other words, knowledge. But that is not enough; the knowledge must be gathered into a consistent format and shared among those who need it to make valid business decisions in order for the organization to perform at a high level.

At the same time, the practice of knowledge management requires pursuit of sufficient knowledge to manage the organization and all of its parts, even in an ever-changing business environment where loyalty to the organization, or even to the management team, is at best based on meeting the needs and expectations of employees who hold that knowledge in their heads. Thus, it is logical for the managers at the top of an organization to desire, even feel the need, for control of the knowledge of the organization with the ability to use that knowledge to increase performance, profitability, and personal standing in the organization. The only methods of acquiring the knowledge and using it for the good of the organization are for management either to micro-manage or to put in place a workable knowledge management plan that brings the knowledge to those who can best make use of it for the continued health of the organization. This is truly a business crossroad, one that this white paper addresses.

Glaring questions result from this line of thinking. The three major questions are readily apparent using even minimal management logic. They are:

- Who is gathering the data, turning it into information, and ultimately into knowledge and intellectual property that is usable throughout the enterprise; intellectual assets?
- What form should the gathered knowledge and intellectual property take?
- How should the knowledge and intellectual property be disseminated and used throughout the organization?

For those questions to be answered, an organizational structure must exist that allows implementation efforts to gather, disseminate, and use knowledge throughout the organization. Deciding how to pursue knowledge management, as a way of gathering intangible assets and determining how best to disseminate the gathered information so that it has the greatest availability to those in need of it, is the challenge of knowledge management.

A Chief Knowledge Officer must be assigned to define the first steps of a methodology that will work for the enterprise. The methodology includes a way to gather, assess, and distribute knowledge to customers and throughout the enterprise to those who work on issues in a manner that serves the needs for business decision making, for relevant learning from experience, and for understanding products (e.g., how products and services are being applied and evaluated in the field).

A full suite of quality metrics can be put into place to gather the information about how products and services are being evaluated in the field, but without an implemented knowledge management process, the root cause of the results of gathering quality statistics might not be revealed and the decision-making that results would be skewed.

Knowledge Management Methodology

OVERVIEW

Data, at first there was too little. Methods were put into place to identify the type of data needed and soon, there was more data than a person could handle. As data was evaluated, it became information, but various interpretations caused decision making to be somewhat hit and miss. What was really needed in the first place was knowledge, the type of knowledge on which decision making could be based and that could be flexible enough to withstand changes in the working environment or to be modified by those changes that improved the knowledge and decision making so that the enterprise could flourish.

So, it's the 21st Century and still, there are many organizations that do not take advantage of the proven methods for acquiring data, analyzing data and identifying information, and then turning the information into knowledge that can be used to improve the enterprise. This is what makes knowledge management a critical part of every enterprise.

In order to take the greatest advantage of knowledge management, the following products should be developed or re-developed at a minimum for use by various functions:

- Staff knowledge map
- Lessons learned database
- Developmental database
- Help desk-trouble ticket system
- Supporting documentation
- Customer and employee training

The most important task is to gather the information once and disseminate it to the correct place for placement in the appropriate dissemination vehicle (e.g., those listed as products above). Thus, the rest of this plan will discuss the processes of gathering, documenting, and disseminating data and information with a view towards the various channels that need to be controlled to make this happen in a way that is not redundant and that does not waste company resources.

INFORMATION GATHERING

Scope

Information gathering will be performed through ongoing research between individuals as a result of their normal job duties and will be supplemented by development of a lessons-learned database, a development database, and the help desk-trouble ticket system. Each of these is further described below.

Research

All of the information being gathered for various products and services is based on the personal information and knowledge held by members of the enterprise staff. The staff members are gathering information for very different reasons, but some of the efforts are redundant. Planned sharing of the information gathered into a very organized methodology will reduce redundancy and ensure that information is accurate.

The first phase of this effort should be to create a knowledge map of the enterprise, which will allow for any staff member to know where to go to get information that is being sought.

The second phase is to create a library of attributed research in the form of white papers, some of which may be published on the enterprise's Website. This library must be searchable by keywords, topics, sources, and dates, so that conflicts can be resolved as information is added and further researched. This effort lends itself to the use of a relational database with key individuals having author rights, management having editorial rights, and all enterprise staff members having read rights to nonproprietary or nonsensitive data. Any search of the database should reveal the string of entries on a given topic and indicate who was the last one to put an entry in that is considered the most valid. Thus, any search will find the most recent instance of the same information. This may be accomplished by having everyone report on their efforts or experiences to a mailbox (e.g., the mailbox could be named km@"enterprise-name".com (or .gov or .mil, etc.)). This should at least be the initial part of the effort. For the most part, this will be an additional addressee to already occurring reporting within the company. The knowledge officers (those with authoring and editorial rights) should filter and compile the information, which saves research time, and the filtered information can be stored in the database collaborative Website for publishing to whoever expresses an interest.

The third phase is for the knowledge managers to review information at some regular interval. Senior knowledge managers will have the ability to eliminate records that are false or grossly inaccurate, which in their opinion might mislead; however, such deletion shall result in the record being modified to show that the information is no longer available based on inaccuracy or being outdated. In such cases, the deleted records should be saved in a separate space for at least one year in case there is any overlooked value to the information.

Lessons-Learned Database

A lessons-learned database should be created. This may be included in an existing application, such as a trouble ticket system or a customer relationship management system. In that regard, a mailbox should be created under the name lessonslearned@"enterprise-name".com so that any staff member can add the mailbox as an additional addressee on information being passed throughout the e-mail system. The mailbox should be a group mail address for the knowledge managers, so that staff members are apprised of every submitted e-mail. Knowledge managers will be vested with the task of checking e-mails that fall into their area of responsibility and moving the information into a record on the network and notifying the other knowledge managers of the movement into a record and the location.

All staff members will ultimately have read access to the lessons-learned database and knowledge managers will have modify access in order to correct any inaccuracies within the database that are pointed out verbally or via e-mail. This database will be particularly useful to personnel working the help desk or providing customer support at higher tiers as well as pre- and post-sales personnel, who are tasked with scanning the database in order to help find answers for customer questions.

Topics must be locatable by keyword searches of various fields.

Development Database

Development notes for the enterprises' engineered products and complex services should be gathered for use throughout the enterprise. The need to capture this data should ensure that any development effort undertaken is well documented throughout the development portion of the lifecycle in order to feed the developmental database. The notes should be made available to all knowledge workers.

Help Desk Trouble Ticket System

A help desk-trouble ticket system must have the ability to output trouble tickets as e-mail to the lessons-learned mailbox. Thus, when a lesson is learned from a customer query, the information can be made rapidly available to knowledge workers. The trouble ticket system also must gather information about how resolutions are achieved and the relative importance of a problem, based on whether the system is down as a result of the customer report. This information is critical to problem resolution and escalation as required, so it should be readily available.

Documentation

By gathering information in this form, it will be readily available to all knowledge workers. Some part of the enterprise, perhaps a communications department should take the lead in preparing documentation templates and the information that is in the databases must be readily available for cut-and-paste into documents as the documents are created.

That same communications department also should take the lead for producing a content management plan that ultimately will enhance the use of technical documents and allow for dynamically placing copies of release masters under configuration control.

INFORMATION DISSEMINATION

Documentation that is produced will be identified based on usage.

Under the rough category of product and service manuals, documents for customer use should be available to all needed users and the enterprises' knowledge workers without limitations via the enterprise's Website. Documentation in this category should include student training manuals, product manuals and descriptions, marketing materials, etc. These documents should be available in an unchangeable format that does not lend itself to being cut-and-pasted into other documents. These documents should be available via the enterprise intranet without limitation.

NOTE: It is critical that the enterprise intranet HTML pages are available to remote users just as easily as they are available to users throughout the enterprise.

Under the rough category of guides (e.g., scripts for professional services, training lesson plans, installation guides, presentation materials, internal specifications, etc.), the documents should be made available to knowledge workers via the intranet Website. These documents should be available via the enterprise intranet without limitation, but should not be disseminated by staff members to any location beyond the enterprise without management approval.

Under the rough category of proprietary materials, those materials that are deemed to be of great importance to the enterprise keeping its competitive or core competence edge should be maintained. These materials may be available with proper release of enterprise leadership via the organization's Website, but access shall be limited on a need-to-know basis (refer to the applicable enterprise Security Standard Practice Procedures with any further specific questions to the applicable security officer). Some method of protecting this type of information should be developed and may include the use of Public Key technology or other encryption schemes. For example, signature and encryption keys may be required to gain access and documents. In such a case, the documents should not be available over the enterprise's intranet to anyone other than the management team.

Under the rough category of organizationally sensitive materials, those items deemed to be of significant importance to the enterprise's ability to continue in business will be maintained. Such materials might include business plans, financial documents, etc. These documents should be available to the personnel listed as having need to know only on specific access lists that are

part of the document and are created with it (refer to the applicable enterprise Security Standard Practice Procedures with any further specific questions to the applicable security officer). These documents should be available to the executive management team, also on a need-to-know basis. They should not be available via the company intranet and should only be sent electronically via properly signed and encrypted e-mail. Any staff member who receives a copy of this type of material from any other staff member who is not a member of the executive management team shall report such occurrence to their direct manager.

Process Components

STAFF KNOWLEDGE MAP

The best method for doing this quickly and efficiently may be to have every member of the staff log on to Microsoft Outlook® (if that is the e-mail application being used) and in the listing contained in the Global Address Book to add their specialty, current assignments, and subject matters of expertise to their personal information. If Microsoft Outlook is not the e-mail application being used, there are other applications that can be obtained that will perform similar functions, but it may be necessary to have knowledge workers within the enterprise gather the information and enter it into the application either via another office productivity application. From that, a knowledge map in a single file can be published and maintained.

LESSONS LEARNED DATABASE

A lessons-learned database is a holding location for realizations about any phase of operations. For example, a lessons-learned database might include lessons that are learned by deployment teams during deployments at various sites. It also might include information from individual sites about application behavior based on issues such as bandwidth, machine class, or any other unique or nonunique factor. Gathering and reviewing this information also will contribute to quality management as trends can be gathered from lessons learned to more quickly identify issues that are occurring throughout a system.

The role of knowledge worker will be able to review incoming issues and determine how the issues apply to the role that they perform for their line organization. Knowledge managers will be placed in a unique position by ensuring the accuracy of inputs via the inputs of the knowledge workers, and this is the point where trend analysis will become automatic throughout the enterprise.

The availability of the lessons learned database represents one of the most valuable research tools and should be reviewed by every development team or management team with regard to the specific topics that are part of their enterprise endeavors.

Metrics can be gathered based on the items covered in the lessons learned database and the efforts of line organizations and development teams that are impacted by the information so that management acquires a better view of how effective and efficient tasks are being performed when directed. In addition, management will be better able to direct the workflow of the enterprise based on the information contained in the lessons learned database, which should result in less redundancy and more focused directions through the chain of command. Each organization will have different requirements for the information to be gathered and contained in their own lessons learned database, but as a baseline, the following information should be included in every record in the lessons learned database.

- Date of entry
- Time of entry
- Submitter's identity

- Submitter's telephone contact number
- Submitter's e-mail address
- System impacted
- Type of issue being reported
- Description of issue
- Solution implemented
- Indication of whether solution was permanent or temporary
- Revealed vulnerabilities, if any

DEVELOPMENTAL DATABASE

A developmental database should be put into effect that captures all design notes and specifically follows the notes that are placed in code on software development efforts, so that at any point, a researcher can go back and identify the reasons for making decisions. It would be most beneficial if the data could be pulled electronically from those programs where it is developed. For instance, the java (or any other language) code used to develop a new application should be readable so that notes (depending on the nature of how the code is noted) could be automatically pulled from the code to be put into the developmental database.

The format of the database is not critical, but the ability to search and find relevant information is the critical aspect. In that regard, two efforts should remain primary. The first is the searchability of the datastore. The data should be stored in a way that key words and phrases can be sought and found with relative ease. The second is the development efforts and determination of what information is to be pulled into the developmental database. For example, it does little good to create a developmental database if application engineers and coders are not going to write notes against code that describe why the code is written the way it is and what the intent of each code line or code group is. Minutes from engineering meetings such as an Engineering Review Board also should be captured.

Finally, the developmental database should be available online to anyone throughout the enterprise who might be working on a system that will require similar engineering planning and decision making efforts. One way of doing this is to have it available through the enterprise's intranet with an HTML search capability and the application of need-to-know parameters based on access to data rather than on the ability to search.

Placing the developmental database under configuration control should be considered. Additions can be grouped for inclusion at each revision level of the controlled version, but each deletion or edit of material in the developmental database would require commensurate action through the enterprise's configuration management system as an impact to a configuration item.

HELP DESK-TROUBLE TICKET SYSTEM

There are many different approaches to creating a help desk trouble ticket system. Some applications have been developed just for that purpose (e.g., a trouble ticket or change request system) and other applications are much broader than just that purpose but include that functionality (e.g., a full-up customer relationship management system). Either case will work depending on the scope of the enterprise and the services it offers.

Regardless of which type of system is used, much of the gathered information will be the same (e.g., name of reporting person, type of problem or change being reported, description of issue, etc.). Often, the solution does not get described in trouble tickets, which means that the information about how the resolution is determined and whether it masks a symptom or truly fixes a root cause is not contained in the individual ticket with the result that workarounds result in other tickets being opened and the lack of knowledge system information about how a problem should be fixed. So it is critical that a solution field be included that describes how the

issue was overcome and fixed. One method of ensuring that this works is to have that field a required field that must be completed by the person implementing the fix with a subsequent requirement that the Tier 1 or 2 person who first opened or worked the ticket be the person to close the ticket. This additionally allows for a teaching tool for Tier 1 or 2 individuals to show the solutions to problems that are identified and passed on for solution development at some point later in the system.

The key issue is to ensure that the help desk trouble ticket system feed the lessons learned database in an attempt to increase future abilities to resolve issues and decrease the time spent on each individual issue.

SUPPORTING DOCUMENTATION

Regardless of the system used, supporting documentation for any system is considered a top priority. Major applications and general support systems often will include purchased systems embedded in the new system. This requirement does not mean that the embedded portions should be re-documented, but that the overall system should be clearly documented with regard to its function and intent. This may include the portions being documented separately or the separate documentation might not be an important part of the supporting documentation as it serves only a function that is described much simpler elsewhere. For example, a new application may use a dashboard that is purchased and embedded in the application. Documentation about the dashboard may not be included separately as the dashboard is designed specifically for information about the new application and how the dashboard functions is not as important as the information being monitored.

Supporting documentation should allow a user or a later researcher to determine what is being accomplished and the means that are used to accomplish the goals of the application. In addition, supporting documentation must include any necessary user and administrator guides, system specifications, and concepts of operations.

All of the supporting documentation should be made available electronically and may be candidates for including in the developmental database.

CUSTOMER AND EMPLOYEE TRAINING

Training materials often provide insight into the intent of a development effort for that system. For that reason, training materials should reside in an online storage of some type. In addition, training materials are often upgraded based on upgrades to the systems or new, inherent ways of using the system. For this reason, the training materials that are hardcopy should be considered as perishable materials and students should be made aware of the changing materials so that they can refer to the online versions rather than to carry away a lot of paper in the form of hardcopy versions that may well become outdated before the end of lifecycle for the users.

Copies of training materials including lesson plans should be included in the developmental database and under configuration control.

Summary

The major focus in implementing a knowledge management system for any enterprise is that the collected information serves a purpose of enhancing future developments and changes throughout the enterprise.

Employees who want to learn new things so that they can enhance their own ability for the benefit of the enterprise are vital to every enterprise. The key of a knowledge management

system is the ability to provide the knowledge to those employees (whether direct or contract employees) in order to enhance the enterprise by the growth of its employee public.

The key to a successful IT security program lies in how well systems are documented and evaluated with regard to security issues. Federal Network Systems' INFOSEC Services Division provides a holistic approach to INFOSEC in general and specifically to C&A efforts for Government and Federally mandated programs to ensure IT systems can be operated safely and securely. In addition, INFOSEC Services provides services that offer Return-On-Investment (ROI) features to increase safe, secure operations of IT systems and to provide for better system protection throughout the life cycle of the system.

For more information, refer to the contact information provided on our Website: www.fnsnet.com and a representative will be happy to provide more information.