AMQ International

Strategic Asset Management

Issue 99, October 18, 2002

KNOWLEDGE REQUIREMENTS FOR INFORMATION SYSTEMS

It's not the system—it's the usable data you have within it.

NEW!

Take advantage of the Virtual Community's pre-publication web serialisation of "Maintenance and Asset Management Information Systems" by the Founding Director of the Institute of Asset Management in the UK, Norman Eason. Not only will you have the opportunity to access each weekly issue for free on the Members site but…

You will have the opportunity to discuss your asset information systems issues with leading specialists, other interested users—and the author of our web serialisation, Norm Eason.

Norm has been involved in computerised aided management systems since they began about 30 years ago. His pioneering work, Rapier, won a major European Award. For more about the author see p.374. For more about the book, see p.380.

Simply go to "Members Profiles" on the Virtual Community site (www.amqi.com) and enter your user name and password.

If you are not yet a member, go to **www.amqi.com** , click on "new member" and follow the instructions. You will then have access to the rapidly growing members database and—from October 28th—to the first issue of the web serialisation.

Join now and you will be reminded of the starting date for the web serialisation, so that you don't miss a single episode. And to see just how useful this serialisation is, see a brief chapter synopsis on the back page.

Researched and written by Dr Penny Burns, AMQ International.
Published fortnightly. Subscription, Comment, or Inquiries to

AMQ International
PO Box 75 Salisbury South Australia
Tel: 618 8281 5795 email: info@amqi.com

Issues Arising from the Step by Step Program:

SHOULD YOU BORROW TO FUND ASSET RENEWAL?

A number of agencies have a policy of not borrowing to fund asset renewal. This is generally prudent as unlike some new investment, reinvestment by way of asset renewal does not generate any additional cash-flow to support repayment of the loan.

However, as with all 'rules of thumb' this policy needs to be applied with commonsense.

There are two situations when it may pay to break the rule.

(1) Where reinvestment can be justified in terms of maintenance savings. If the maintenance savings are sufficient to repay the debt, with interest, then the renewal may be treated as an ordinary investment and it is worth breaking the 'no borrowing' rule.

(2) Where it can be clearly demonstrated that the agency is at a peak in its renewal profile with diminished need for renewal funds in future years. In this case, loans are a sound way of avoiding over-charging and the reduced call on renewal in the future will free up resources to pay off the loan.

But how do you know where your portfolio is in terms of asset life cycles?

Assuming you know is dangerous. If borrowing is introduced when agencies first start to feel the effects of deferred maintenance or renewal demands, it is almost certainly far too soon! Such borrowing severely worsens the situations by

- adding loan repayments to future renewal requirements, and
- postponing the hard decisions on what is affordable

To know whether it is safe to borrow, the agency needs to know the age profile, economic life and remaining life/condition of its total asset stock. In other words it needs a long term renewal plan. It is a good addition to the rule to say "no plan, no renewal borrowing'

About the author of "Maintenance & Asset Management Systems"

Norman Eason has been involved in maintenance and computer technology since 'forever'. In the early 1970s he was approached to see IF the new computer technology could be applied to maintenance! It seems strange to say this now but this WAS over 25 years ago! Norm developed computer aided maintenance management packages and one of them, Rapier, won a major European Award.

He founded the Institute of Asset Management in 1995. In an interview in 1999 he said

'Companies often buy computer maintenance packages without a maintenance strategy and without linking their information requirements to the business. It seemed about time that we addressed this issue and, incidentally, raised the profile of maintenance and asset management generally.'

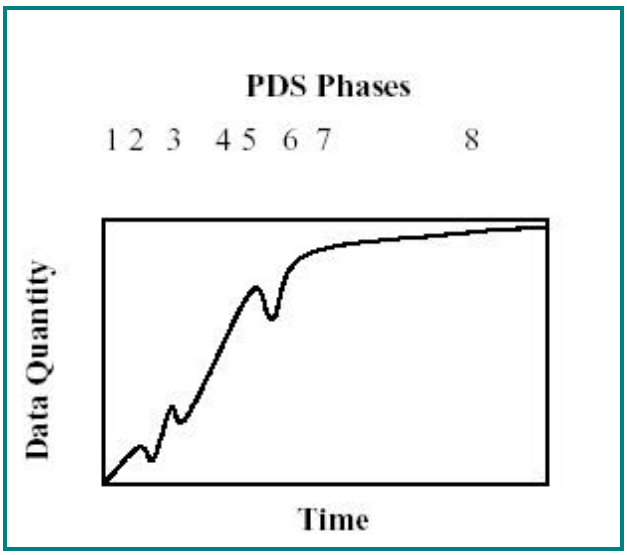
Planning	Definition	Implementation	Commissioning	Operations	Evaluation	In-Service	Deconstruction
1	2	3	4	5	6	7	8

WILL YOUR DATA LAST AS LONG AS YOUR ASSETS?

Long term assets require long term data handling.
Are your data systems are to the job? Can they handle, for example,

- Lengthy maintenance/operations phases?
- Changes in asset performance (deterioration, maintenance, repair, and renewal?
- Changes in functional requirements of assets?
- Decisions that are dependent upon data collected in programming, design, construction and commissioning phases? and where
- Relevance of data collected is not evident until the 'in-service' phase?

Much of your asset data is acquired in the first four project delivery phases. (Note the incidence of data *losses)*



But data loss is only one of the problems……..

Project Delivery Phases

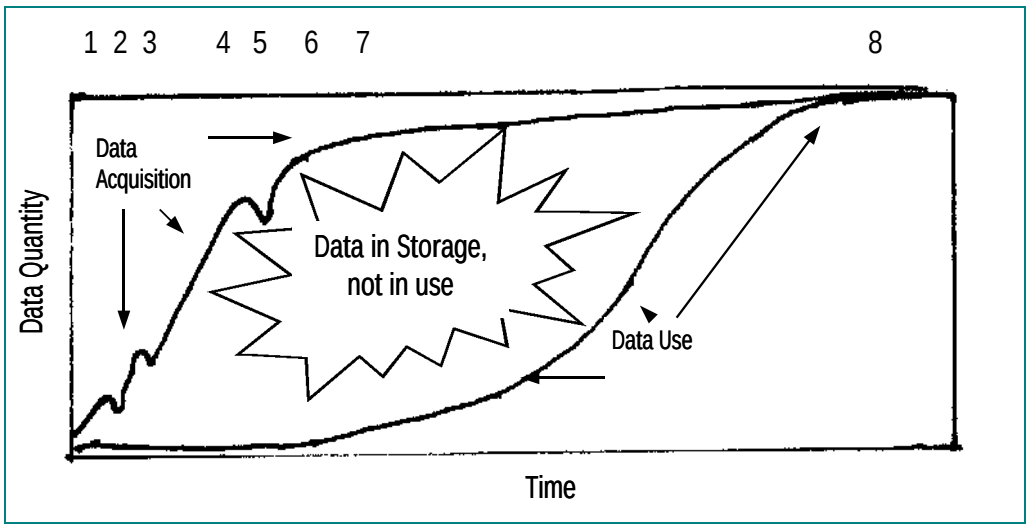
1. **Planning**—opportunity, objectives, options, a recommendation with preliminary schedule/ estimates.
2. **Definition**—planning document translated into technical language suitable for design instructions.
3. **Implementation**—design, preparation of working documents, contracting and construction.
4. **Commissioning**—confirmation that technical requirements in design instructions are satisfied.
5. **Operations**—fine-tune facility operations, with consideration to commissioning results.
6. **Evaluation**—following client/ user acceptance, conducts 'Evaluation' relative to variances between objectives and finished product.
7. **In Service**—all actions during normal operations and maintenance phase of a facility's service life.
8. **Deconstruction**—declaring facility to be 'surplus' to needs and commencing dismantling.

… For much of your data may remain unused for decades, yet needs to be usable 'on demand'.

In practice, the in-service period can be very long. Throughout this period there will be increasing need to call on data stored in earlier periods. When this happens will you find that the right data was stored?

Ensure that you do as much as you can to maintain data integrity and usefulness by reading the Asset Management Community's new web serialisation "Maintenance and Asset Management Information Systems" and taking part in the ongoing discussion forums.

The future of asset management may well lie with the future of systems support!

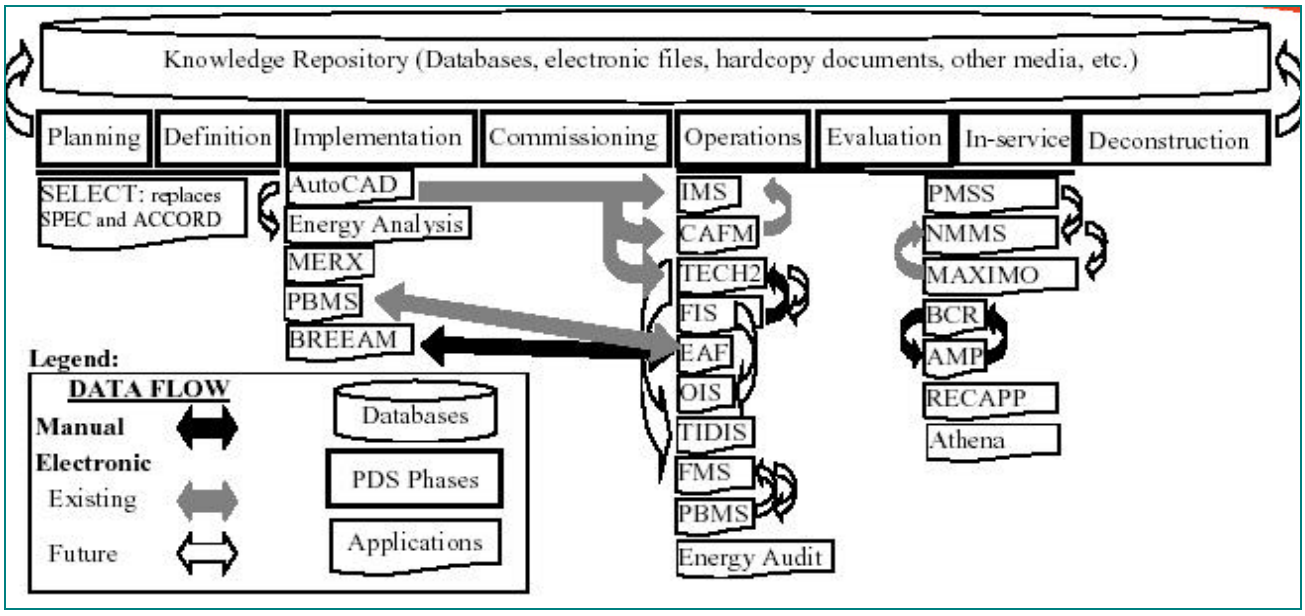


DATA DEGRADATION

Remember when 'floppy discs' were really floppy? What machine today can read them? And with their rate of degradation, how many would still be readable? What of today's data storage tomorrow?

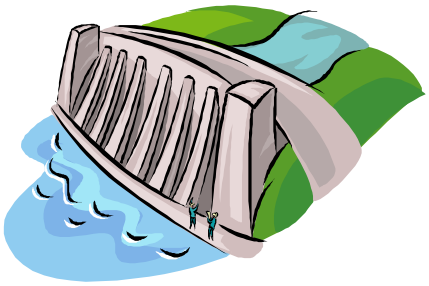
DATA INTEROPERABILITY

The diagram below is merely illustrative of a general problem. However, it you would really like to know what all of the acronyms for the various databases and applications stand for, you can access Dana Vanier's article on "PWGSC Case Study: Technical Information Needs of Public Works Managers " at www.nrc.ca/irc/uir/apwa



ASSET SECURITY

How safe is your water service?



Water agencies have generally held the view that water supply systems are unlikely targets for sabotage. However, recent events have highlighted the potential for deliberate attacks to be made on major public infrastructure.

An increasing number of news reports from around the world have highlighted how major water service providers have been the targets of deliberate attack.

Even within Queensland, electronic attack on a water service providers telemetry system by a disgruntled contractor resulted in raw sewerage being discharged into parklands and creeks. Evidence points to the fact that water supply and sewerage infrastructure is highly vulnerable to vandalism.

The subject of security became even more prominent within Queensland with the recent hosting of the Goodwill Games in Brisbane and the CHOGM meeting in the Sunshine Coast. Such events bring masses of people to the region and consequently there is a necessity to ensure facilities are adequately protected.

So, what can we do? Security Guidelines

Risk reduction strategies can be implemented to improve the security and protection of water supply and sewerage systems. A major challenge is to review procedures and implement security controls in order to protect the livelihood of a water agency's business and consequently, reputation, clients, consumers, and the environment.

Following events of September 11, Cardno MBK undertook a detailed study tour of the US including liaison with some of that country's premier experts on security management. In association with Maroochy Water Services, Pine Water and strategic risk management adviser, Paul Donato (Cardno MBK) developed a comprehensive Security Management Guideline for Water Supply Services. Figure 1 (overpage) illustrates the key security management activities identified in the Security Management Guidelines for Water Service Providers.

The Guidelines specifically address these issues with checklists and proformas to assist with documenting a security management plan. **Security management planning** involves several stages and requires the following processes to be undertaken:

- ***Identifying hazards and threats***
- ***Quantifying risks***
- ***Assessing vulnerability***
- conducting a review of the site to determine where security weaknesses are.
- ***Preparing security management documents***
- Including a Security Policy, Crisis Management Plan and a Risk Reduction/ Mitigation Plan.
- ***Implementing a Security Plan***

Figure 1 broadly outlines these elements of security management.

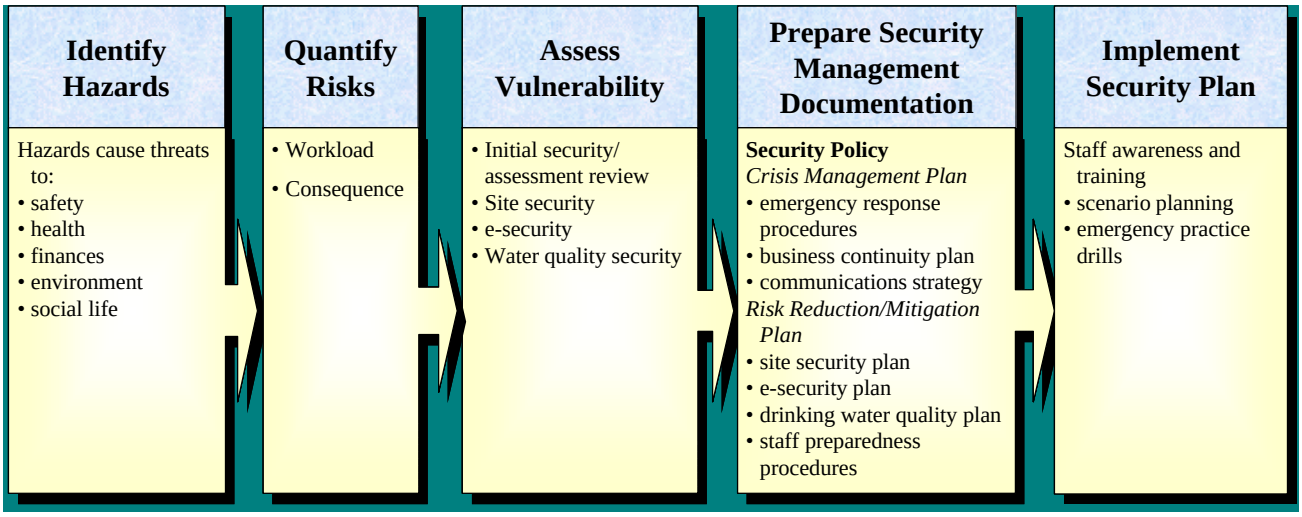


FIGURE 1 : Elements of Security Management

Hazards, Threats & Risks

The first stages of security assessment focuses on defining hazards and risk. These threats are different for each utility.

Threats which may affect an organisation at any time include:

- ***physical***
- vandalism;
- attack on staff (i.e., robbery);
- personal injury; and
- damage to property.

- ***electronic***
- accessing confidential and/or critical information;
- accessing critical controls; and
- unauthorised alteration of control configurations.

- ***biological/chemical***
- contamination by biochemical toxins, microbiological agents, industrial chemicals and weapons of mass destruction.

The hazard (threat) assessment involves:

1. determining who and/or what constitutes a threat;
2. identifying individuals, groups, or events that may attack a particular system; and
3. considering all potential threats, because assuming the worst may result in overlooking more likely events.

Continued on page 379

Open Oct 23 *on the Virtual Asset Management Community Site* ***www.amqi.com***

ONGOING FORUM—WATER ISSUES

This is a moderated discussion forum open to any issues in the management of water and wastewater assets. ***Take part in discussing today's issues in water asset management.***

Moderators: Chris Adam, Cardno MBK, Queensland, AUSTRALIA
Raj Shivalingam, Global Engineering & Management Services, California, USA
Ross Waugh, Ross Waugh & Associates, NEW ZEALAND

Continued from p. 378

Hazard/risk and threat identification enables management and operators to assess and quantify hazards, risks and threats faced by the organisation and develop suitable strategies to control and manage these events, should they occur.

Defining Vulnerability:

A **vulnerability assessment** determines the level of resistance and susceptibility of an element to a hazard and risk. For water utilities, a vulnerability assessment may be used to identify the weaknesses in the water supply system and the outcomes may be used to develop actions to improve on the operation of the systems and reduce the water utility's exposure to risk and hazards.

Vulnerability may be defined as a weakness that can be exploited to cause an organisation/ system to become compromised.

Who can Help?

Cardno MBK's Security Management Guidelines for Water Service Agencies provide a tool to identify the vulnerable facilities within an organization and provide procedures and methodologies to improve the security at these sites.

The Guidelines come in two parts. The first part provides you with an overview of risk and security management for water service providers, with respect to deliberate acts of disruption by physical, electronic and chemical attacks, while the second part provides a comprehensive selection of forms and checklists that may be used by the service provider to develop procedures for improving the security at each site.

Copies of the guidelines can be obtained by contacting Carolyn Parker on (07) 33699822. If you want assistance with implementing the actions outlined in the security guidelines, please contact Kerry Jones (kjones@cardno.com.au) or Chris Adam (cadam@cardno.com.au) or Aneurin Hughes (ahughes@cardno.com.au) of Cardno MBK.

"Maintenance and Asset Management Information Systems"

Web serialisation begins October 23rd

There are very few books on this subject.

This is NOT a book on technology. There is, in fact, little reference to technology itself (although it covers the impact of technology). Instead it covers the fundamental problems of what data and information are required for maintenance and asset management and how requirements vary between different types of user. No other book has approached the subject in such a logical manner or has treated such a technology-based subject in a way that transcends constant technology updates.

Contents:

Chapter 1. Scope of the book—what's here and what's not

Chapter 2. Maintenance and Asset Management—looks at the differences between the two and the consequences for data requirements

Chapter 3. Data and Information—Climbing the Data to Wisdom ladder—data, informatin, knowledge, wisdom. How data and information interact. Concept of data as an asset.

Chapter 4. Objectives of Maintenance and Asset Management Systems—considers the way in which systems evolved to meet the perceived requirements of different types of industry, examines how vendors have addressed conflicting user requirements and explains why users' and vendors' objectives are not necessarily the same.

Chapter 5. The Nature of the Problem—gets down to the major problem of difference. Areas of divergence.

Chapter 6. Codes—examines how the coding system within a user organisation affects the choice and use of an information system.

Chapter 7. Functions—Interrelationships between functions can cause an installed system to be effective or to fail because its designer has assumed a method of operation that is alien to the organisation.

Chapter 8. Technology—is considered with respect to its ability to cause differences in the requirements of organisations; problems of compliance with company standards.

Chapter 9. Culture—one of the most fundamental differentiators between organisations is culture. Organisations may be competitive or complacent, they may be innovative or entrenched, paternalistic or hard-driving. Failure to take culture into account is a serious risk to the success of information systems.

Chapter 10. Evolution– considers the evolution of the project itselfand the need to utilise information and knowledge gained from the use of the system to continually refine.

Chapter 11. Interconnection—relationship between maintenance or asset management department and the rest of the organisation.

For information on remaining chapters, go to "Members Profiles" on www.amgi.com

Chapter 12. Methodologies; Chapter 13. Traditional Approach to Product Development; Chapter 14.Successful Procurement for Through Life Effectiveness; Chapter 15.Objective Assessment of Progress; Chapter 16. Risk Analylsis for System Procurement; and Chapter 17.Ethics.