erpa tool

Information Society Technologies


# Risk Communication Tool

September 2003

ELECTRONIC RESOURCE PRESERVATION AND ACCESS NETWORK

## Risk Communication Tool

*Risk is a combination of the probability of an event (usually adverse) and the nature and severity of the event. The main aim in understanding and communicating risk is to identify and impose priorities, and take appropriate actions to minimize risks.*
*The uncertainty of digital preservation in the constantly evolving technological environment means that there is an ever-present risk that digital assets will be orphaned when formats and technology becomes obsolete. Digital preservation is still an immature process from both an economic as well as a technical standpoint, and the lack of sufficient experience and evidence can be problematic.*

This tool is designed be used to:

- Highlight what digital resources are at risk in an organisation
- Highlight the risks to these digital resources
- Highlight the risks to organisations posed by threats to digital resources
- Categorise and prioritise risk in order to manage it
- Enable communication within the organisation about areas of risk
- Stimulate risk management strategy development

Three stages to consider in assessing and managing risk:

- **Risk identification** ► *For example:* resources at risk, type of threats, value of resources, organisational vulnerabilities. Identifying risk scenarios should begin with an understanding of how the system *should* work.
- **Risk analysis** ► *For example:* levels of acceptable risk, likelihood of risk materialising, direct and indirect costs, consequences of risk materialising, safeguards in place.
- **Risk management** ► *For example:* mitigation options and responses, risk prioritisation, management strategies, risk reduction, tradeoffs

*Risk Categorisation*
Risks should be categorised in accordance with the goals of the organisation. Questions must be asked of the organisation in order to determine priorities and goals:

- What is the organisational and legal status of this agency? (e.g. profit, non-profit, public, private, cooperative)
- Who is the organisation accountable to?
- What is the scope and value of the organisation's assets?
- What digital assets does this organisation need to preserve?

Risk can be divided into categories, and the risks within each category can then be prioritised/ranked in terms of probability of occurrence and impact in relation to the organisation's needs and operations.

*Categories and Ranking*
As many sources of information and evidence should be gathered in the ranking process to assess the significance of the risk sources. Such evidence includes common sense, professional experience, expert knowledge, and statistical data.

*Risk Process*
This generalised risk process begins with human or natural activities which give rise to loadings or accident initiating events. These, in turn, lead to exposures and effects, which are then perceived and valued by people. Within each stage of the process categories of risk can be established and risks within these can then be ranked (see severity scale matrix below). Some examples of possible digital preservation risk categories are provided in the table.

**Risk Process and Categorisation Table**

| Human Activity | Loading/Initiator | Exposure and Effects | Perception and Value |
|---|---|---|---|
| Can include:<br>By Information creation risks, Information management risks, Information systems risks | Can include:<br>Technology risks, organisational failures | Can include:<br>inability to retrieve information, litigation, damage/loss of corporate assets, corporate liability, legal retention requirements not met | e.g. loss of value loss of trust, delivery of services |

Alternative risk categorisations can prove useful to an organisation. Possible subsequent interventions might focus on, for example, modifying human activities or lessening exposure.

*Qualitative Severity Scale Matrix*[1]
Each of the risks in each of the categories can be mapped onto this table. Risk sources falling into the darkest boxes are judged to be the ones requiring priority attention.

**Qualitative Severity Scale Matrix**

| Likelihood / Effect | Unlikely | Seldom | Occasional | Likely | Frequent |
|---|---|---|---|---|---|
| Loss of Asset (catastrophic event) | | | | | |
| Loss of Function/operational ability) | | | | | |
| Loss of capacity with compromise of some function | | | | | |
| Loss of some capability with no effect on function | | | | | |
| Minor or no effect | | | | | |


*Management*
A number of scenarios are therefore identified, constituting most of the risk to the digital assets and the organisation. Attention should be then turned to managing these. Decisions should be made about the best course of action (and whether it would actually reduce risk without creating any new risks), and finding the most cost-effective manner in which to do so.

Mitigation options/responses should be generated and evaluated in terms of cost, benefit, and risk tradeoffs, and then a decision on which options to implement and in what order should be made. An implemented risk management programme should balance the value of the assets and the direct and indirect costs of preventing or recovering from damage or loss. Risk

[1] Taken from Haimes, Kaplan, & Lambert, *Risk Filtering, Ranking, and Management Framework*, Risk Analysis, Vol. 22, No. 2 , 2002.

assessment and management should never be considered finished: new sources of risk and information about risk should be added as they arise and are identified.