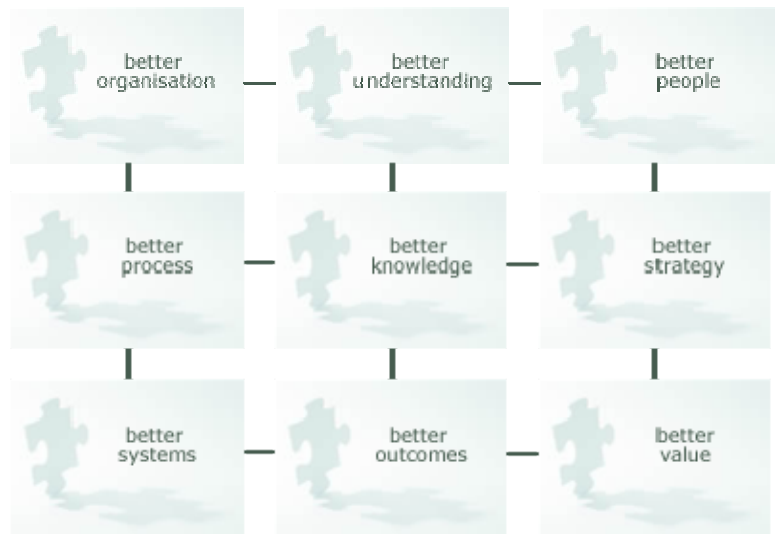


Joined-up management for a joined-up world™

(UK only) 0800 3277 934
+44 (0)207 870 9506
<http://www.colin-beveridge.com>



Information Governance

Measures for preserving
stakeholder confidence

by Colin Beveridge

*MSc FRSA FIMIS FBCS CITP
The Better Practice Forum*

October 2008

Abstract

The frequency and scale of personal and commercial information leakage, through accidental loss and deliberate theft, has seriously weakened stakeholder confidence in the Information Governance capabilities of organizations, in both private and public sectors. Such losses are often beyond the realms of inconvenience and embarrassment, carrying real risks to personal welfare, organizational integrity and National security.

However, despite the diversity of the compromised information and the points of failure, it is not difficult to discern a common theme – absence or weakness in basic housekeeping principles. The casual observer may think that, while no expense is spared in the routine capture and creation of information, poor operational processes around the use and handling of information so easily undermine the very integrity of the enterprise.

And yet important as it may be, information governance is not just about security.

For example, the broader scope of information governance encompasses the need to ensure that the organization fulfils statutory, regulatory and contractual obligations for the creation, retention, dissemination and management of information. Furthermore, stakeholders reasonably expect information governance practices to ensure that the organization is properly vested with timely information for effective management.

This paper sets out a summary of straightforward measures that should help organizations preserve stakeholder confidence in their information governance.

Key Points

The author challenges the presumption that changes to the political and regulatory process will help to identify and encourage best practice; because such [legal] changes could only realistically follow, rather than lead, suitably effective practice.

Well-considered legislation/ regulation is unlikely to fit the necessary timeframe so the most plausible solution to the problem of diminished stakeholder confidence in information governance must be a concerted, sustained and timely effort to prevent further high-profile incidents, by direct improvement to process.

Stakeholder confidence devolves from a diverse base of stakeholder groups [internal and external]; even in the simplest enterprise the stakeholder group extends well beyond the immediately apparent data subjects, providers and customers. Notwithstanding the requisite variety of stakeholders, measures for preserving stakeholder confidence in information governance can be developed and usefully related to four key zones: *Compliance; Design and Access; Connectivity and Handling; Care and Control*. Such measures could support an Information Governance Capability Maturity Model.

The self-discovery and improvement process associated with the implementation of a maturity model is also thought to be a quicker, more effective and sustainable path to improving the general level of stakeholder confidence.

Information governance failures are almost always expressed through incidents in the “lower reaches” (below the waterline of senior management’s perception) so assessment of governance capability should not be simply aggregated to the enterprise level, as this could imbue a false sense of confidence; therefore a consistent, coherent cascade of expectation and accountability needs to be maintained throughout the organization.

Information leakage

Figure 1 shows a high level interpretation of the nature and location of some well-publicized information leakages:

The examples shown are not exhaustive but are representative of the most frequent categories of the highest-profile data losses.

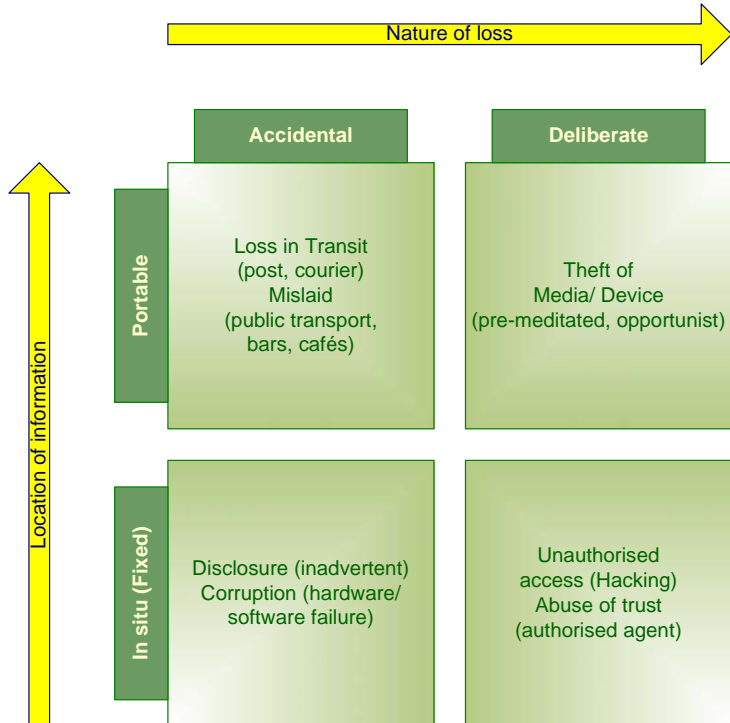


Figure 1 - Information Leakages

Governance process failures

Figure 2 shows how the information losses relate to failure in Information Governance process:

Three key zones of process illustrate the most likely causes of information/ data losses.

Care and Control

Particular care must be afforded to "Portable" information because it is highly vulnerable when removed from its "fixed home."

Connectivity and Handling

Huge amounts of sensitive information can be compromised by transfer to removable media and devices, which often facilitate the by-passing of protective design features of the "fixed home"

Design and Access

Hardware and software design should routinely not only protect access but also structure information to mitigate the effects of leakage from "fixed home" storage.

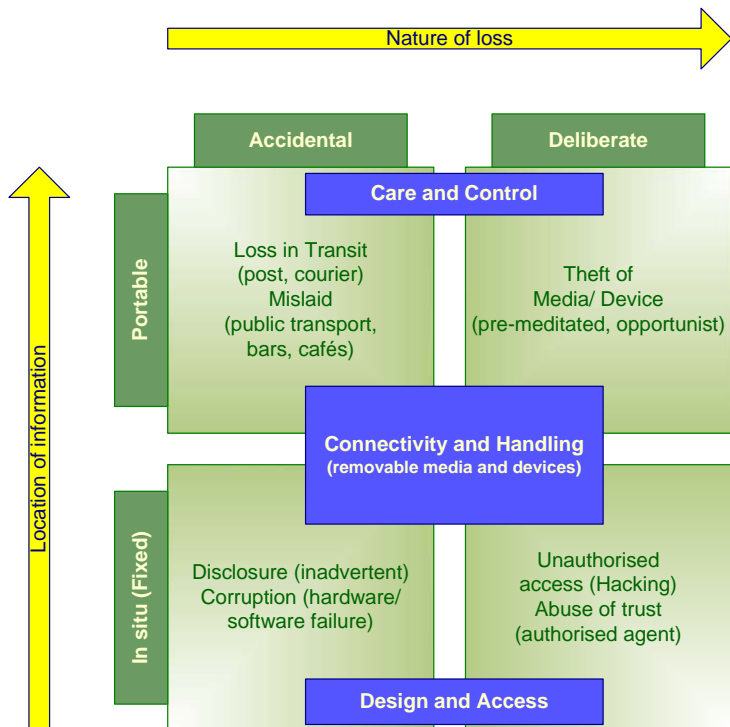


Figure 2 Governance Process Failures

Zones of stakeholder confidence

Figure 3 shows how the different aspects of Information Governance process combine to influence Stakeholder Confidence:

Weakness in any of these zones (as evidenced by a failure leading to information loss) is likely to damage/destroy overall stakeholder confidence (aka trust), regardless of the resilience and robustness of the other (uncompromised) governance processes.

For effective Information Governance, enterprise capability in each of these zones should be properly covered, from an individual systems/ service perspective and from a [recursive] organizational perspective.

Sensitivity of the information under management will determine the proportionality of Information Governance measures required.

Stakeholder confidence can be pro-actively improved by maintaining evidence of effective Information Governance capability.

The alternative is to persist with the present approach of apology, investigation and process remediation, following a governance failure.



Figure 3 - Zones of Stakeholder Confidence

Measuring Information Governance Capability

Despite the diversity of organizations and their Information Governance requirements, it is possible to create a standardized approach to measuring governance capability.

A broad range of individual capability elements can be profiled, using appropriate dimensions for each element, to create a series of capability profiles. Figure 4 shows an example of how such a capability profile might look:

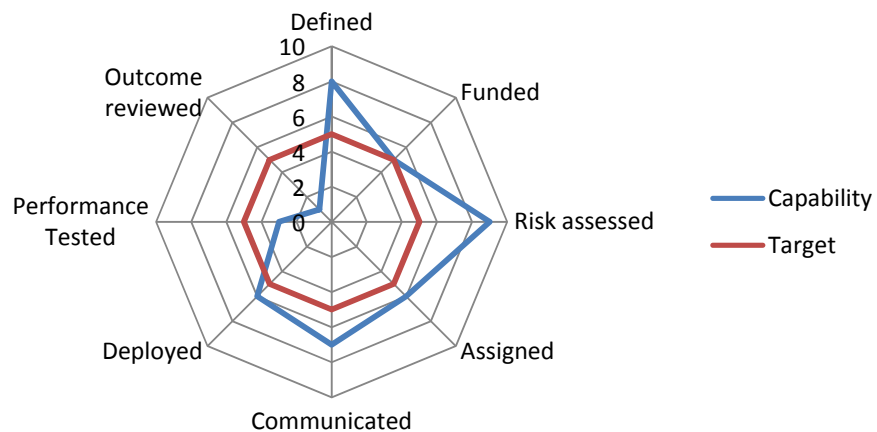


Figure 4 - Example Capability Profile (Care and Control: Personnel Database)

This approach not only forms the basis of an effective method of maintaining a consistent and coherent means of communicating governance capability to stakeholders but also very useful management information for governance process improvement.

An Information Governance Capability Maturity Model

Detailed capability information is a sound basis for stakeholder confidence and process management. However, some sort of high-level “kite-mark” accreditation model is useful at the divisional and enterprise levels. For such purpose the author recommends the introduction of an Information Governance Capability Maturity Model, as a standardised means of assessing governance capability.

Figure 5 shows an example of such a Capability Maturity Model:

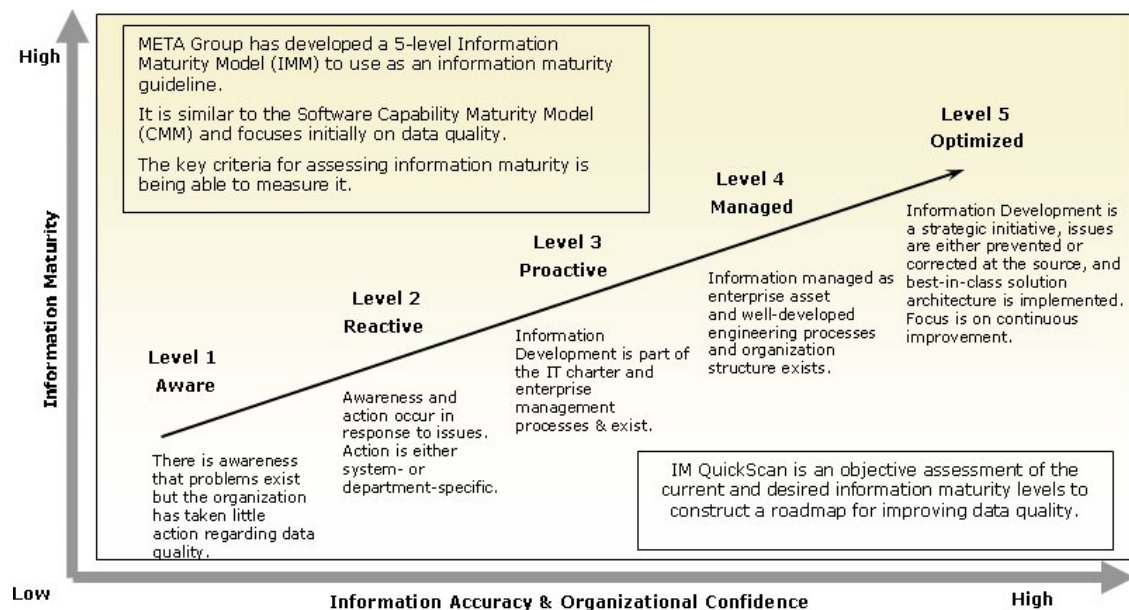


Figure 5 – Example of a Capability Maturity Model

(The diagram at Figure 5 is used under license from the Information Maturity project, part of the MIKE2.0 Methodology <http://www.openmethodology.org>, which is made available under the Creative Commons Attribution License.)

An Information Governance Maturity Model would take a similar format, with appropriate underlying terminology and methodology. The above example is given to provide sufficient flavour of this type of approach, which has been applied successfully in many other fields. A key principle of maturity models is that organizations seek systematic improvement to attain higher levels of demonstrable capability.

Next Steps

The approach outlined in this paper can be developed into a fuller discussion paper, incorporating further guidance on matters of detail precluded by the short-form of this document.

In conjunction/ parallel, a working group of interested parties could be established to prepare a “straw-man” model of an Information Governance Capability Model.

It is hoped that representatives of HMG would participate in the development and review process, in alliance with Eurim and experts from the vendor and user communities.

Conclusion

Information Governance is undoubtedly a complex challenge, with potentially huge costs of failure and little or no concomitant return on investment in the event of successful provision. Nevertheless, it is not a discretionary choice for most undertakings; apart from the scale of effort and cost involved. A systematic, standardized approach to the challenge will facilitate better understanding of the issues and a general improvement in Information Governance process.

The key attributes of a governance regime will inevitably include: sensitivity, resilience, sustainability, affordability, practicality, proportionality and comprehensibility. But above all, governance must be effective, if we truly wish to preserve stakeholder confidence and trust.