Best Value toolkit: Information management

AUDIT SCOTLAND

Contents

Introduction

The Audit of Best Value

"Achieving Best Value is about ensuring sound governance, good management, public reporting on performance and a focus on improvement"

The duty of Best Value applies to all public bodies in Scotland. It is a statutory duty in local government, and in the rest of the public sector it is a formal duty on Accountable Officers.

Best Value has already been a powerful force for improved performance and accountability in local government, and it will play an important role in supporting the Concordat and the development of Single Outcome Agreements between the Scottish Government, councils and their partners, and in streamlining and coordinating the scrutiny of public services. It also has the potential to underpin the National Performance Framework and the 'management scorecard' elements of Scotland Performs.

On behalf of the Auditor General and the Accounts Commission, Audit Scotland has identified a set of principles that form the basis for a consistent approach to the audit of Best Value across the public sector, although its application will differ to reflect factors such as the different accountability regimes and reporting arrangements in place in different sectors. This will enable us to apply a consistent set of expectations across all the bodies that we audit, and to reflect and support the reality of partnership working between organisations.

The Best Value toolkits are a key part of the practical application of the BV audit. They provide an evaluation framework that will help auditors to reach robust judgements on how public bodies are delivering Best Value**.** However, they cannot generate Best Value judgements on their own. They cover only part of the process. Judgements about Best Value also involve consideration of service standards and performance, outcomes and how effectively continuous improvement is being achieved. The framework through which the various elements of the Best Value audit are brought together to arrive at an overall conclusion on the extent to which an organisation is achieving Best Value is outlined below:

Exhibit 1

Framework for a BV audit of a public body
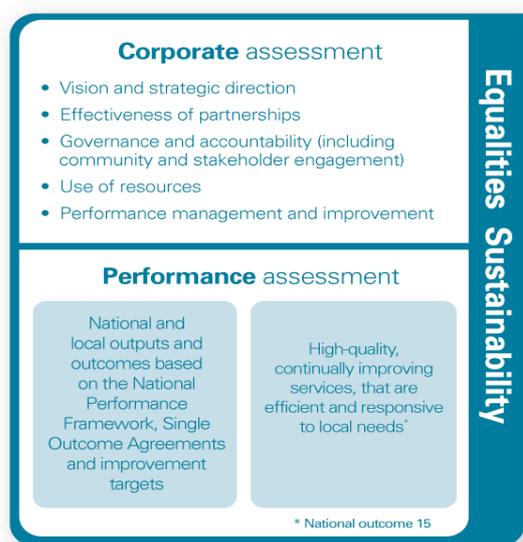
Source: Audit Scotland

As the diagram demonstrates, Audit Scotland's approach to the audit of Best Value entails both corporate assessment and performance assessment elements. The former focuses on how an organisation plans and conducts its business and manages its resources while the latter looks at the quality of those services and the outcomes for service users.

Audit Scotland is committed to ensuring that Best Value auditing across the public sector adds value to existing arrangements, is risk-based and builds on our existing knowledge of individual public bodies, and that of our scrutiny partners. Specifically we aim to:

- report on the delivery of outcomes for people who use services

- protect taxpayers' interests by examining use of resources

- put an increasing emphasis on self assessment by public bodies with audit support and validation

- work collaboratively with other scrutiny bodies to ensure our work is aligned and prevent duplication.

The Best Value toolkits

The Best Value toolkits are a series of audit diagnostics, which will help reviewers to establish the extent to which public bodies' arrangements are designed to achieve, and are actually delivering, Best Value. They have been developed to support the corporate assessment process around the five corporate assessment areas noted in Exhibit 1, and the two cross-cutting themes of equalities and sustainability. However, as each toolkit also incorporates a series of questions on the impact of the area under review, they will also provide some evidence to support the assessment of service performance and outcomes.

The Best Value toolkits have been developed as audit tools in consultation with specialist practitioners, and representatives of public bodies and professional groups.

The toolkits take the form of structured key questions, with a matrix of possible levels of performance, ranging from basic to advanced practice. The matrices cannot of course capture all of the ways in which a public body may address the requirements of Best Value, so there is clearly scope for auditors to exercise balanced judgement and for public bodies to respond flexibly in demonstrating how the key areas of challenge are addressed. Individual evaluations are made about the level a public body has attained in each question or area. However, these have not been weighted and it is not intended that these be used to determine an overall scoring for any toolkit. They are designed to contribute to sound professional judgements, not to replace them.

Using the toolkits

The toolkits are designed for application by Audit Scotland's auditors when carrying out Best Value audits of public bodies. In practice, the toolkits will be applied as part of an audit process, whereby the auditor makes enquiries, seeks supporting information and forms conclusions based on the evidence obtained.

Audit Scotland recognises that bodies may find the toolkits helpful in carrying out general organisational reviews or specific service reviews and are therefore available in the Audit Scotland website www.audit-scotland.gov.uk. It should be stressed however that public bodies using the toolkits do so at their own discretion. The toolkits are designed principally as audit tools that are part of

Audit Scotland's overall Best Value audit methodology and are not expressly produced for self-assessment purposes.

Any organisation using the toolkits to inform their own corporate or service-based self-evaluation processes will need to consider the local context when applying them, and also the indicative rather than conclusive nature of the findings when interpreting the results. The toolkits were designed to elicit contextual information and provide evidence for arriving at professional audit judgements. They are not intended to be, and cannot be, used in a "tick-box" fashion.

The Best Value toolkits are generic in nature, in that they are not specific to any one type of public body or to any one sector and are designed so that they can be applied to all public bodies. Auditors will require to be sensitive to the differences between organisations both in terms of different sectors and varying scales of operation.
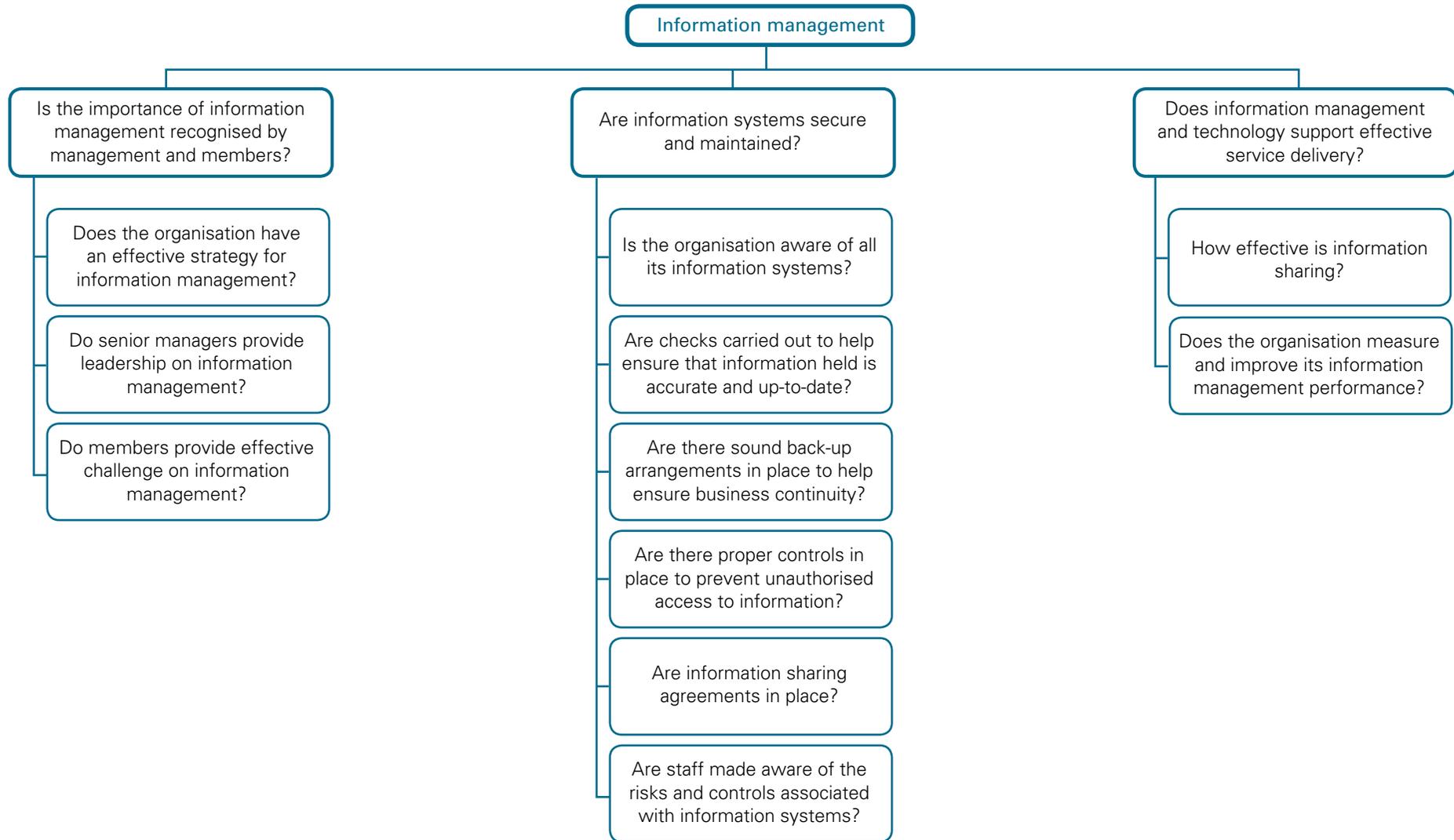
This toolkit forms part of a suite of audit products that will be applied, over time, to support a structured, evidenced based, judgment on an organisation's approach to the use of the resources with which it has been provided and its achievement of Best Value.

Auditors' evaluations

The toolkit takes the form of a series of questions based on identified good practice. It then offers four sets of descriptors, these being:

Does not meet basic requirements	An organisation may not yet demonstrate the basic practice level in any particular category.
Basic practices	Minimum acceptable standards, which would be sufficient to allow an organisation to demonstrate sound performance.
Better practices	As basic, with some elements of good or even best practice, but not on a consistent basis.
Advanced practices	Consistently demonstrating good or best practice and contributing to innovation.

Best Value toolkit: Information management

```
                          ┌─────────────────────────┐
                          │  Information management │
                          └─────────────────────────┘
```

Information management

Is the importance of information management recognised by management and members?

- Does the organisation have an effective strategy for information management?
- Do senior managers provide leadership on information management?
- Do members provide effective challenge on information management?

Are information systems secure and maintained?

- Is the organisation aware of all its information systems?
- Are checks carried out to help ensure that information held is accurate and up-to-date?
- Are there sound back-up arrangements in place to help ensure business continuity?
- Are there proper controls in place to prevent unauthorised access to information?
- Are information sharing agreements in place?
- Are staff made aware of the risks and controls associated with information systems?

Does information management and technology support effective service delivery?

- How effective is information sharing?
- Does the organisation measure and improve its information management performance?

	Basic Practice	**Better Practice**	**Advanced Practice**
Part 1 Is the importance of information management recognised by management and members?			
1.1 Does the organisation have an effective strategy for information management?	Some planning of information needs is occurring on an ad-hoc, departmental, basis. But there is no co-ordinated, corporate information strategy. Strategic planning tends to focus on ICT matters, such as hardware and software issues and data security, rather than the wider concerns of information management.	The importance of an information management strategy is understood and accepted, and responsibility for its development is assigned and clearly communicated. Key elements of a corporate information management strategy are in place or are being developed. An ICT strategy is in place to help deliver the wider objectives of the information management strategy. .	An information management strategy is in place, setting out a corporate vision of: • information sharing within the organisation • information sharing with external partners; • matching information collected and held with business needs; • security measures, informed by a risk assessment, to protect the information held. The strategy sets out measurable targets. The information management strategy has been approved by members and been widely communicated to staff. There is a co-ordinated approach to ICT procurement, maintenance and development throughout the organisation and with external partners.

	Basic Practice	Better Practice	Advanced Practice
1.2 Do senior managers provide leadership on information management?	A manager has operational responsibility for data processing and ICT, but there is limited evidence of an awareness of wider information management issues at a senior level.	A member of the top management team has responsibility for information management and has been assigned as Senior Information Risk Owner (SIRO) or Chief Information Officer (CIO). There is a general understanding of the information needs of the organisation.	There is regular discussion of information management risks and performance by the whole of the top management team. Top management have a clear view of the organisation's information governance responsibilities. There is evidence through, for example, risk registers, that top management are aware of the wider information / data processing issues and risks.
1.3 Do members provide effective challenge on information management?	Members provide some challenge on information management, but this tends to be ad hoc and limited to ICT projects.	Members are aware of the wider information management issues, but discussion of these matters tends to covered during scrutiny of risk management rather than as part of a structured assessment of information management. Information management issues are considered by members at a departmental level.	Members focus on strategy and key performance issues relating to information management, rather than simply specific points of detail. Information management regularly features in discussions by members about corporate risk management. Information management issues, at corporate and departmental levels, are part of the remit of a committee and are regularly discussed.

	Basic Practice	**Better Practice**	**Advanced Practice**
Part 2 Are information systems secure and maintained?			
2.1 Is the organisation aware of all its information systems?	There are basic inventories of information held, showing what is held and how it is stored. These tend to be maintained at departmental level and are not comprehensive	There is a corporate inventory of information held throughout the organisation. For each item, the inventory includes: • The owner of the information • The location of the information • Staff who have access rights • With whom and how the information can be shared • The risks associated with each asset (such as sensitive personal data, inappropriate disclosure, loss, tampering, deletion etc.) • How information/data will be updated, transferred and disposed of. Risk factors, such as sensitive personal information, are flagged.	A comprehensive inventory of information is in place and is regularly reviewed and kept up-to-date. The inventory is used to manage the organisation's information assets, helping to develop more streamlined processes that avoid, for example: • multiple collection, storage and maintenance of duplicate information • inconsistency in data • information which is no longer needed.
2.2 Are checks carried out to help ensure that information held is accurate and up-to-date?	Some quality control checks are in place to ensure that the information is accurate, reliable and up-to-date.	Quality control checks are in place for all information processes to ensure the accuracy, reliability and currency of the information.	The organisation's quality control process helps ensure that accurate, reliable and up-to-date information is provided. Regular, independent reviews of the information held and the system outputs, perhaps carried out as part of a rolling programme of internal audits, are used to identify areas for improvement.

	Basic Practice	Better Practice	Advanced Practice
2.3 Are there sound back-up arrangements in place to help ensure business continuity?	Where possible, all information is held on a secure network, rather than laptops or other portable devices, and regularly backed-up. Business and continuity processes are in place in some parts of the organisation, and there are plans to extend this to other areas to meet disaster recovery requirements.	Business and continuity processes are in place in all significant parts of the organisation, but are not regularly tested. Information is regularly backed up.	Business and continuity plans are in place throughout the organisation to meet disaster recovery requirements. They are regularly tested. Information is regularly backed-up to a remote site.
2.4 Are there proper controls in place to prevent unauthorised access to information?	There are appropriate physical security measures and procedures to control access to business premises. There are controls in place to ensure that user access lists are up-to-date, with rights removed when no longer required. There is a secure network where incoming files are verified by appropriate firewall and anti-virus defences. All staff are regularly reminded of an Acceptable Use Policy. The organisation can demonstrate that it complies with the Payment Card Industry data security standards, if applicable.	There are restrictions on external email services as a means of transferring information out of the organisation. There is an Information Security Policy in place that applies to all staff and partner organisations and is readily available. Guidance has been issued to staff on the security of laptops, other mobile devices, and portable memory devices.	Measures are in place to limit the impact of the loss of a physical device (such as encryption by default). High-risk data handling activities are identified and relevant users are given appropriate training. A programme of penetration testing is carried out in order to test the robustness of controls.

	Basic Practice	Better Practice	Advanced Practice
2.5 Are information sharing agreements in place?	Some departments have established formal information sharing agreements with external partners.	All significant parts of the organisation have established formal information sharing agreements with external partners, but these vary in scope.	A corporate template is used for information sharing agreements across the organisation. Checks are regularly carried out to help ensure these procedures are followed.
2.6 Are staff made aware of the risks and controls associated with information systems?	Staff are required to sign on to an information management code of conduct. Compliance reviews on the organisation's legal, regulatory and standards frameworks are carried out ad-hoc or in response to events.	Staff are encouraged to be pro-active with regard to the organisation's information management policies and procedures. Compliance reviews on the organisation's legal, regulatory and standards frameworks are carried out regularly.	Staff awareness of the organisation's information management policies and procedures is tested using surveys or other tools. Appropriate action is taken on the results of such feedback. Staff actively participate in workshops to discuss new legislation, regulations and standards. Senior management requires routine compliance reports from all business areas. In addition, changes in the regulatory framework trigger compliance reviews.

	Basic Practice	Better Practice	Advanced Practice
Part 3 Does information management and technology support effective service delivery?			
3.1 How effective is information sharing?	Examples of effective information sharing are in place, but are not consistently developed across the organisation or with partners. Information sharing conforms to DPA, FOI and other security / legal requirements; any non-compliances are addressed.	Information-sharing is effective, both across the organisation and in aspects of partnership working. Information-sharing and technology is effectively used to support customer services, shared client/ patient records, website and on-line services. The organisation makes good progress against its information strategy and related plans, and in implementing relevant national information-sharing initiatives.	Information-sharing is effective and well developed across the whole organisation and with partners. Information-sharing and technology is seen as a strong enabler for better service delivery; good practice in information-sharing and technology is shared across the organisation and with partners. The organisation consistently delivers against its information strategy and related plans and demonstrates a strong lead in national information-sharing initiatives.
3.2 Does the organisation measure and improve its information management performance?	A range of measures are in place to assess the quality and cost effectiveness of information management (including monitoring internal and external ICT service standards). The organisation demonstrates generally good and improving performance; and monitors and reports performance regularly. Options appraisal and business cases are used intermittently to demonstrate the costs and benefits of technology and information-sharing applications	Measures have a strong focus on user feedback and customer satisfaction, as well as cost and quality comparisons with other organisations and the marketplace. The organisation has a track record of good and improving performance in information management regarding both service provision, and internal user satisfaction. Options appraisal and business cases are used regularly to clearly demonstrate the costs and benefits of information-sharing applications and technology.	The organisation demonstrates good and improving user and customer/client services and consistently out-performs in benchmarking and commercial market comparisons. Options appraisal and business cases are used systematically for both the organisation's overall information-technology strategy, and individual developments. Options appraisal considers a wide range of delivery options including: shared services, joint working, supplier partnerships and contracting options.

Best Value toolkit:
Information management

If you require this publication in an alternative format
and/or language, please contact us to discuss your needs.

You can also download this document at:
www.audit-scotland.gov.uk

AUDIT SCOTLAND