



WALES **AUDIT** OFFICE

SWYDDFA **ARCHWILIO** CYMRU

Information Management Review Feedback

North Wales Fire and Rescue Authority

Audit year: Annual Improvement Assessment 2011

Issued: September 2011

Document reference: 488A2011

Status of report

The person who delivered the work was Jeremy Evans.

This document has been prepared for the internal use of North Wales Fire and Rescue Authority as part of work performed in accordance with statutory functions, the Code of Audit Practice and the Statement of Responsibilities issued by the Auditor General for Wales.

No responsibility is taken by the Wales Audit Office (the Auditor General and his staff) and, where applicable, the appointed auditor in relation to any member, director, officer or other employee in their individual capacity, or to any third party.

In the event of receiving a request for information to which this document may be relevant, attention is drawn to the Code of Practice issued under section 45 of the Freedom of Information Act 2000. The section 45 Code sets out the practice in the handling of requests that is expected of public authorities, including consultation with relevant third parties. In relation to this document, the Auditor General for Wales (and, where applicable, his appointed auditor) is a relevant third party. Any enquiries regarding disclosure or re-use of this document should be sent to the Wales Audit Office at infoofficer@wao.gov.uk.

Summary report

1. There are concerns about the management and quality of information and records within the public sector following widely publicised failures, and a perception that improvements in public services are being hampered by inefficient management of information. Government-commissioned reports such as the *Bichard Report*¹ have indicated a ‘systemic and corporate failure’ in relation to information management.
2. More recently, two reports² by the Audit Commission reflect little progress in local government in England and reinforce the need for appropriately managed information to support operational service delivery and effective decision making.
3. With increasing financial pressure on the public sector there is a need to maximise and exploit the information held to deliver and plan for quality services effectively, taking decisions with all the available information to support and protect vulnerable people.
4. In 2010 the Wales Audit Office identified through its Improvement Assessment work that many authorities were grappling with using information effectively to support service transformation and efficiency savings; as a result, reviews of information management are being undertaken at all fire and rescue authorities in Wales.
5. This review sought to answer the question:
‘Is North Wales Fire and Rescue Authority’s (the Authority) approach to information management positively supporting improvement?’
6. Our review of the Authority concluded that:
‘The Authority’s approach to information management is supporting improvement and it is generally aware of the issues it needs to address, but there are some weaknesses in governance arrangements that pose a risk to the Authority.’
Our findings, conclusions, and proposals for improvement are outlined in the table below.

¹ *The Bichard Inquiry Report*, Parliamentary Publication June 2004

² Audit Commission, *Is there something I should know?* 2009 and Audit Commission, *Nothing but the Truth*, 2009

High level question	Is the Authority's approach to information management positively supporting improvement?
High level answer: We have concluded that:	The Authority's approach to information management is supporting improvement and it is generally aware of the issues it needs to address, but there are some weaknesses in governance and performance that pose a risk to the Authority.
Assessment of current arrangements	'Some concerns' – There are weaknesses in arrangements which need to be addressed but other aspects of the arrangements are acceptable with signs of improvement.
Assessment of performance	'Proactive' – Performance is broadly sound. There is scope for improvements but these are either already in hand or are not significant enough to warrant urgent action.
Proposals for improvement	<ol style="list-style-type: none"> 1. The Authority should revise the ICT/Information Strategy to bring it up to date with national and local initiatives, ensuring comprehensive coverage of information management issues. 2. Deliver the function of an Information Security Forum, chaired/attended by the Senior Information Risk Owner (SIRO), that meets regularly and has corporate responsibility for information issues, in particular: <ul style="list-style-type: none"> • establishing standards and policies; • monitoring compliance with standards and policies; • information management training; • learning from and addressing information incidents and issues; and • management of information risk. 3. Develop a comprehensive training programme for all staff to ensure that the Authority can demonstrate that responsibility for information issues has been cascaded throughout the Authority. 4. Address the issues raised by the recent Internal Audit review of IT Security; these recommendations are wholly supported by this review. 5. Establish robust arrangements for whole life cycle management of electronic information including e-mail. 6. Bring administrative information governance in line with the effective arrangements for operational information governance. 7. Ensure that sufficient data is held outside the recommended nine-mile limit to enable a full restoration of service information in the event of a disaster.

Findings	Yes or No	Because:
<p>Are the Authority's plans for information management likely to secure continuous improvement?</p>	<p>In part</p>	<ul style="list-style-type: none"> • There is no overarching information strategy in place. However there is an ICT Strategy; this is dated March 2007. The ICT Strategy document covers a number of key information initiatives, such as security, document management and customer relationship management but this is in need of a refresh to reflect the current national and local aspirations and direction and cover the medium and longer term. • The Authority's code of corporate governance includes in principle 4, the need for 'good quality information, advice and support to ensure that services are delivered effectively and meet the needs of the community'. However, there are no detailed plans aimed at specifically achieving this principle. • There is a range of policies and guidance – Service Administrative Policy & Procedure Order (SAPPOs) in place. Policies are developed to meet a need and cover most aspects of information management. All policies that are in place have been approved. • There are no plans directly focused or overarching in relation to information management. Specific information issues are integrated within the individual project plans, for example those that related to the Fire Records Management System (RMS). • There is limited training on information management issues available to staff.

Findings	Yes or No	Because:
<p>Are the Authority's arrangements for information management likely to secure continuous improvement?</p>	<p>In part</p>	<ul style="list-style-type: none"> • There are no formal dedicated information management posts in place, but the functions are included in the roles of officers. The SIRO responsibilities were held by the Deputy Chief Fire Officer whilst the Authority was creating its submission for the code of connection. The SIRO responsibilities were re-affirmed early in May 2011 to the Deputy Chief Fire Officer. • The Information Steering Group (ISG) is chaired by an Assistant Chief Fire Officer and membership ensures that all aspects of the service are represented. The prime focus of ISG is project governance. • The ICT section develop, implement and monitor policy and guidance; this could lead to potential conflicts of interest. • The two senior officers (assistant chief fire officers) interviewed during this review had a clear understanding of information issues as they impacted on their departments. Information issues are considered a low priority at the present time (economic climate etc) and there has not been any overarching review of information issues. So there is the possibility that both threats and opportunities could be invisible to the Authority. • The Authority focuses on operational risks which promotes the importance of information management and demonstrates an understanding that information is a key element of effective service delivery. However, as operational information has had a higher focus than administrative information there is a need to bring administrative information governance in line with the arrangement in place for operational information. • A corporate risk register is in place. The limited amount of personal information held by the Authority encourages the view that information issues such as reputational damage brought about by personal information loss are sufficiently controlled and represent a low risk. (Note – this statement excludes operational information and operational risks.) However there is a need, as noted above, to bring administrative information governance in line with the arrangements in place for operation information. • Projects are managed using recognised project management models and are subject to ICT Steering Group challenge. Project plans are robust and the Authority has a track record of effective delivery, for example Fire RMS.

Findings	Yes or No	Because:
<p>Is the Authority's information management performance supporting it in providing efficient, effective and economical services?</p>	<p>In part</p>	<ul style="list-style-type: none"> • The Authority uses a Windows Explorer style file structure which is not controlled or effectively structured. Access controls are applied to the shared drive providing individual, function, department and Authority groupings. • The Authority makes effective use of a single gazetteer, which is used in the command and control system, representing good practice. • Key systems are covered by data quality processes, for example Fire RMS. • The Data Retention Policy lists current data holdings (July 2010). The retention policy was drawn up following a request to departments for a list of information they held. However, individual departments are responsible for archiving and disposal of information in accordance with Data Retention Policy, but compliance with these responsibilities is not monitored and it is likely that little if any electronic information is deleted, data volumes are increasing annually which supports this view. • Information provision to operational firefighters is a key issue and information for fire safety and community safety is in place using an effective model suited to the geographical region and its infrastructure. • The Authority does not have a dedicated information security officer, however a recent Internal Audit report on IT Security was broadly positive, we support the report's recommendation that the information security function should be vested in a single officer. The Authority has a range of security measures in place such as password controls and there is an IT Security Policy. Employment contracts include the need to be mindful of the organisation's information in terms of use and security. • The Authority has signed data-sharing protocols with a range of partner organisations (local councils, police, health board, ambulance service etc) and receives information as well as shares information within this group. Data is shared using a range of available media including electronic and paper as well as by word-of-mouth.

Findings	Yes or No	Because:
		<ul style="list-style-type: none"> • Current disaster recovery and business continuity processes are in place; these include auto failover mechanisms which are in place but within two offices on the same site. PSBA will enable greater flexibility in offsite location choice and taking advantage of this facility will resolve current limitations in this respect. Offsite tape storage is less than the recommended nine-mile limit (Rhyl, seven miles), although it is acknowledged that some tapes are 15 miles away but it is unclear whether these would be sufficient for full system rebuild. The ICT section tests the business continuity arrangements. The learning from these exercises together with the lessons learned from adapting the ICT service during periods of staff absence due to weather and sickness has enabled a robust approach to business continuity, for example, the ICT helpdesk can be delivered from alternative locations or home working. • The Authority is compliant with the Data Protection Act and the Freedom of Information Act (FoIA) legislation with appropriate publication schemes in place. The Authority meets the expected response times for both subject access and freedom of information requests.
<p>Is the Authority effectively monitoring and evaluating improvement and performance?</p>	<p>Yes</p>	<ul style="list-style-type: none"> • Although the Authority has a number of operational performance measures in place there are no specific measures to assess information management performance. • Detailed incident data is entered onto the web-enabled Incident Recording System (IRS) by Control staff and is analysed by the Performance Analyst and submitted to CLG. Home Fire Safety Check (HFSC) and fire safety/prevention data is entered onto Fire RMS by relevant staff and is reviewed by the Fire RMS Administrator. The Performance Analyst develops and delivers reports to managers as required. For example, papers produced and provided on request to committees and groups at both department and Authority level eg, Executive Group, Fire Authority Risk Reduction Plan Working Group and Executive Panel meetings. Reports include key performance data in regular monitoring report form and an annual presentation of previous years' PIs and annual returns.

Findings	Yes or No	Because:
		<ul style="list-style-type: none"> Information is used by professional and technical groups eg, specific Chief Fire Officers Association groups, both within Wales and at a UK level, through collaborative activity between the three Welsh FRSs; inter-agency incident debriefs, exercises and internal/external audits. As part of the Operational Assurance of Service Delivery there is an annual self-assessment and reciprocal peer assessment with the other two Welsh authorities (observed by the Wales Audit Office and Welsh Government). Comparisons are made against other FRAs from published data eg, in compiling improvement and risk reduction plans. The Authority does not currently have GCSX Code of Connection approval. The submission was made at the end of July 2011 and the outcome is not yet known. However, the Authority has two 'Airwave Service Code of Connection' approvals for different system connections to Airwave. There is some alignment with ISO27001, for example the ISG act as the Information Security Management Forum, although the ISG prime focus is project governance. Data protection and FoIA audits have been carried out recently by the Internal Audit service; the Authority has taken action to address the recommendations. IT Security has recently been audited by Internal Audit. The report is currently in draft but it is understood that it concludes that in general IT Security is working well, however a few weaknesses need addressing. These relate to access controls, documentation, and the disposal of photocopier hard drives. The report also notes the lack of an IT Security Officer.



WALES **AUDIT** OFFICE

SWYDDFA **ARCHWILIO** CYMRU

Wales Audit Office
24 Cathedral Road
Cardiff CF11 9LJ

Tel: 029 2032 0500

Fax: 029 2032 0600

Textphone: 029 2032 0660

E-mail: info@wao.gov.uk

Website: www.wao.gov.uk