Audit Together

Collaborating to improve services

An Internal Audit View

Welcome to the fourth edition of 'An Internal Audit View'.
In our last bulletin, we reported that we are a collaboration of seven local government Internal Audit Partnerships from across England and Wales. Taken together we partner with 11 County Councils, 9 Unitary Councils, 24 District or Borough Councils, 4 Police Authorities, 3 Fire Authorities and numerous other public sector bodies. Our ability to share benchmarking and best practice continues to grow for the benefit of our partner organisations. If we can help you in this way, please do not hesitate to contact your Head of Audit.

Contents:

General data protection regulations

These will be the new regulations that used to be covered by the Data Protection Act.

Are you ready?

Brexit doesn't make a difference! It has been decided that this is going to be taken on in English statute and therefore whether we are in the EU, article 50, or anything else, does not make any difference, we must be compliant by May 2018!

As with all regulations, your Authority will need time to implement the necessary controls to ensure compliancy, so they need to be looking at the requirements, the 'as is' position, and the need to achieve this. Your Authorities need to be thinking about and planning this NOW! Do you have it in your 2017-18 Audit Plan?

The main differences between the current DPA and the new GDPR are:

- Increase in levels of fines; removal of fees;
- 'Child' Language – any guidance regarding the rights of children must be understandable by children; ensuring mechanisms remain in place for gathering parental or guardian consent;
- Data Protection Officer – a DPO must be appointed;
- Abolition of the £10 fee as standard; reduction in timescales; greater burden of proof to demonstrate required governance, consent and due diligence by Authority (and third parties); significant increase to the rights of data subjects; expected increase in data subject requests; PIA's and evidencing of due diligence may all increase pressure on resources;
- Processing of data outside of the EU – stricter rules specifically for public authorities;
- New data portability requirements infer that they relate to the private sector, however authorities may wish to review any data sharing to establish any applicability;
- Breach definition and reporting – there will now be a need to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected;

GDPR
EU General Data Protection Regulation

Further guidance

So you now need to support your Authorities in the journey to compliance. The Information Commissioners Office have provided various advice and guidance, the key pieces being:

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

You'll be pleased to see within the ICO guidance that thought has been made around the differences between public and private sector.

How do you start the GDPR project?

These are the first steps in supporting your Authorities;

- Both Members and Officers at the highest level must be committed to the delivery of this by May 2018 and the allocation of necessary resources to both achieve and maintain compliance;
- A Data Protection Officer must be appointed to oversee and actively manage the initial and continued compliance of the regulations for the Authority;
- The organisation must understand their full ‘personal data’ lifecycle - how it’s collected; how it’s stored; where it’s located, including third parties; how it’s transferred/ shared; how it’s secured; how it’s classified; reason for retention whilst being processed by the Authority; and ultimately the method of disposal;
- A project plan identifying critical pathways to ensure the remediation of non-compliant areas by May 2018 should be developed now, this should include consideration of audit activity; Gap analysis.

Further detail on the main differences between the current DPA and the new GDPR

Increase in levels of fines; removal of fees

There are two categories of fines, with differing maximum financial penalties.

Violations of data subjects rights – 20million Euro or 4% global annual turnover;

Infringement of data controller obligations – 10million Euro or 2% of global annual turnover;

A County Council with a £500m turnover could have a fine of up to £20m. This suggests a far greater focus on the data subject’s rights rather than the previous focus of DPA on the controller.

Children’s Personal Data

Where services are offered directly to a child, you must ensure that your privacy notice is written in a clear, plain way that a child will understand.

The GDPR states that parental/guardian consent for access to online services is required for children aged 16. Parental/ guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child.

There are extra requirements when the request for erasure relates to children’s personal data. If you process the personal data of children, you should pay special attention to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent. This emphasises the requirement to make the guidance as child friendly as possible at onset.

Data Protection Officer A DPO must be appointed

You must ensure that:
The DPO reports to the highest management level of your organisation – ie board level. The DPO operates independently and is not dismissed or penalised for performing their task. Adequate resources are provided to enable DPOs to meet their GDPR obligations.

Due to the obvious importance of this role and its pivotal nature the Authority may wish to consider implementing a deputy DPO role at the same time;

Changes to Data Subject Rights

Complete turnaround of burden of proof, which now moves from the data subject to the processor. Previously it was the case that the subject had to demonstrate legitimate grounds for objection to the data being processed. If questioned the Authority now needs to show legitimate grounds for processing the data.

Right to be forgotten (right to erasure) – as above, the Authority has to prove why it needs to keep the data if a subject requests its removal.

The subject has all of the same rights of access, confidentiality and integrity. Where the Authority needs to perform a task regarding these rights the time within which to respond has been reduced from 40 days to 20 working days.

Processing of data outside of the EU

The following three exceptions are specifically noted within GDPR as not being available for use by public authorities to allow data to be processed outside the EU:

- made with the individual’s informed consent; necessary for the performance of a contract between the individual and the organisation or for
- pre-contractual steps taken at the individual’s request; necessary for the performance of a contract made in the interests of the individual between the
- controller and another person; necessary for important reasons of public interest; necessary for the establishment, exercise or defence of legal claims;

Breach definition and reporting
A breach is more than losing personal data. You now don't have to have lost data for a breach to have occurred. A personal data breach now means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The requirements to notify should be assessed on a case by case basis e.g. loss of customer details where the breach leaves individuals open to identity theft would be reported, whereas loss of a staff telephone list would not normally be reported.

You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. E.g. discrimination, reputational, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly. A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it.

What value can Audit add?

- Ensure that the business is aware that the law is changing to the GDPR and is actively managed with a risk treatment plan;
- Ensure that a project has been established, initiated and resourced appropriately;
- Ensure the organisation is aware of the GDPR operational gaps in their environment and have identified requisite controls;
- Allocate sufficient time and resource in your audit plan to support the project;
- Ensure early engagement with the GDPR project (Q1 2017/18 at the latest);
- Be a 'subject matter expert' - Communicate best practice as identified within more mature GDPR projects within other organisations;
- Provide interim position statements throughout the project lifecycle;

GDPR
EU General Data Protection Regulation

Organised crime procurement

A recent pilot study by the Home Office has identified an increasing threat to public sector procurement activities from organised criminals. The study confirmed suspicions that criminals are targeting local authorities and other public sector bodies. The number and value of contracts involved and a perception that controls are weak may be factors in this.

The pilot study looked at seven areas in England to better understand the nature and scale of the threat. Another aim of the study was to identify a series of simple measures which could be taken to help reduce the risk. The sectors which are considered to be most at risk are waste, taxi / transport services and areas of low value spend. Property maintenance was also identified as being susceptible to fraud.

In 2013, it was estimated that £2.1 billion of fraud was perpetrated against local government of which £876m related to procurement fraud. Procurement is considered to be lucrative and attractive to serious and organised criminals because there are multiple ways to commit fraud. These include, price fixing, bid rigging, double invoicing and so on. Organised criminals may also seek to use businesses providing services to local authorities to launder criminal proceeds. The money gained is used by criminals to help fund other illegal activity including drug dealing and theft.

As well as the obvious risk of financial losses, procurement fraud can result in the provision of sub-standard goods or services, the loss of income to legitimate businesses, reputational damage to the organisation and harm to the public.

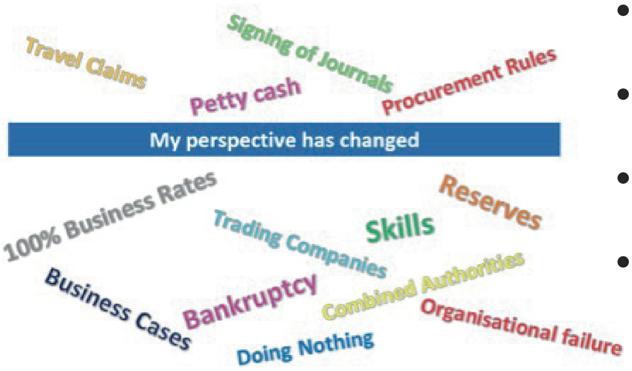
Local authority taxi contracts were identified as being at particular risk. The main focus of these contracts is to provide transport for some of the most vulnerable members of society. Recent events in Rotherham and Oxford have demonstrated the importance of having robust safeguards in place to help protect children and vulnerable adults from predatory groups who use taxis to perpetrate their crimes.

Fraud involving waste can take various forms. Organised criminals can undercut legitimate operators by ignoring environmental standards, avoiding tax completely or by mixing high-risk waste (which attracts higher rates of tax) with low-risk waste. Land can also be used illegally for dumping or storing waste. Organised crime groups involved with illegally transporting waste abroad can also be involved in other serious crimes such as people smuggling and drugs trafficking.

For many of the local authorities who participated, one of the key benefits of the pilot study was that it helped raise awareness of the risks from organised criminals. It also showed how important it is to work collaboratively with other authorities and agencies, including the police.

Local authorities and other public sector bodies are encouraged to establish and maintain systems to help reduce the likelihood of procurement related crime. Specific measures include:

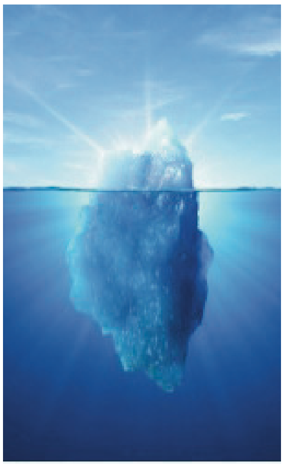
- Raising awareness of the risks of organised crime throughout the organisation, particularly with those services considered to be most at risk
- Carrying out a serious and organised crime audit with managers in key departments to help identify areas of vulnerability
- Reviewing procurement, contract management and due diligence procedures to ensure they are robust, fully implemented, scrutinised and are able to detect fraud and prevent companies with links to organised crime groups successfully securing contracts.
- Increasing scrutiny of the declarations of interest and the gifts and hospitality registers, and cross referencing the details to suppliers / Companies House information.
- Checking potential contracts over a certain value with the police and/or internal fraud team before they are finalised
- Carrying out enhanced checks on suppliers – cross checking against other local authority datasets held such as business rates, planning notices etc
- Carrying out a series of fraud themed audits where a specific service area or process is reviewed from the perspective of preventing and detecting fraud and corruption.
- Encouraging closer working relationships internally between procurement and fraud teams
- Developing multi-agency partnerships and data sharing arrangements.



Risk – What’s Your Focus?

Risk Management has been the talk for a number of years and most organisations will have a process for capturing and reporting on risk. But how much value is the process adding and how is it helping to inform the business? Is it something that is periodically reported or is it embedded within your organisation to inform key decision making?

All too often we find that risks are poorly defined and captured as reverse objectives or controls. This can lessen the seriousness of the risk when considering the true impact of a course of action. For example ‘Safeguarding Children’.



What does that mean as a risk? What is it we are trying to mitigate against? Is it not the injury in one form or another to a child? If the risk is not well defined, then the controls to mitigate will not be clearly understood.

What are your key risks?
What lies beneath?
It is often the risks that we have not foreseen, or not articulated well, that have the biggest organisational impact.

Jason Vaughan, Strategic Director & S151 Officer at Dorset Council’s Partnership, has articulated how his view of risk has changed, as he faces increasing financial challenges.

The diagram below shows how this has changed; he now has to focus on things that may well not have been imaginable a few years ago – for example, will his organisation face bankruptcy?

How can Internal Audit Help? Internal Audit can provide you independent expertise in risk management. This can include:-

- Assurance that your Risk Management process is capturing the real risks
- Training for key staff and members – getting ownership and understanding of risk
- Provide meaningful risk comparisons with like organisations
- Consultancy/Advice for new and emerging risks – how can you mitigate your risks?

Cyber Risk

While rapid technological developments have provided new opportunity and efficiencies for organisations, they have also brought unprecedented threats. Cyber security is a critical issue for all organisations and will become more important with the increased drive toward the ‘digital agenda’ Cyber crime is a global phenomenon which affects everyone, from individuals and employees to small and large organisations.

There are two key exploits to a cyber attack:

- Technical exploit – attack on the vulnerability in technology; and
- Human exploit – utilising human nature in order to gain access

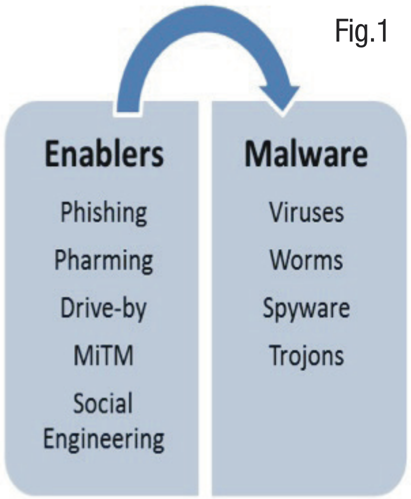
Although local government has not been a target for large-scale cyber-attacks so far, the risks are growing as more data is shared between councils and the ‘Internet of Things’, in which everyday objects have internet connectivity, becomes a reality.

The threat to local government became reality in the recent high profile attack on Lincolnshire County Council in which computer systems had to be closed for four days after being hit by computer malware demanding a £1m ransom.

Local government must play an active role in tackling the cyber security challenge and in developing effective Cyber Security Strategies.

Cyber criminals operate remotely, using numerous means of attack which broadly fall under the umbrella term of malware, these forms of attack are perpetrated through numerous enablers (fig.1)

Fig.1



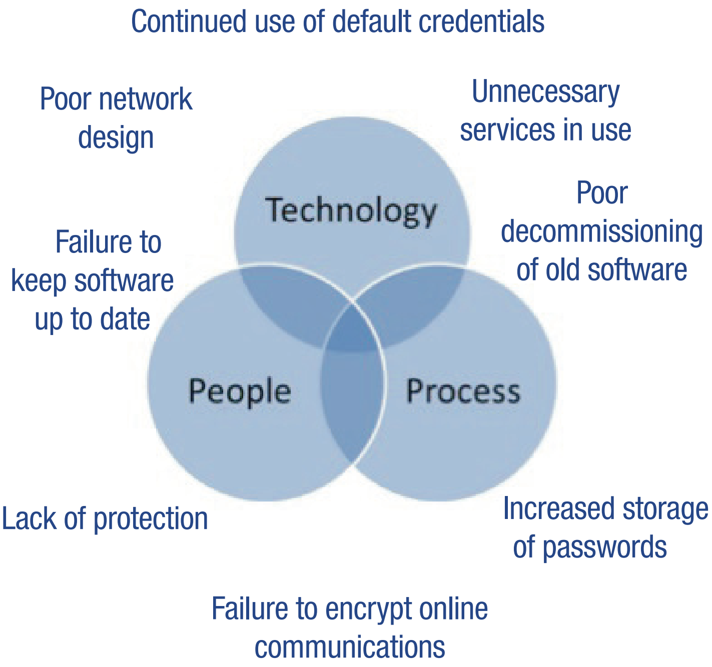
The most targeted information is commercial, including intellectual property, customer lists and related information, business and commercial strategy and financially sensitive information. Data assets such as banking information, payment card details, PII (personally identifiable information) and contact details are also on the top of cyber criminal’s agenda.

Cyber criminals are indiscriminate. Where there is a weakness, they will try to exploit it. Therefore, all organisations need to understand the cyber threats they face, and safeguard against them. No single standalone solution is sufficient to combat cyber crime.

An effective cyber security posture should be proportional to the risks faced by each organisation, and should be based on the results of a risk assessment.

Expensive software alone is not enough to protect organisations from cyber threats. Cyber security technology is only effective where processes are in place to keep it that way. Processes on the other side are dependent upon the skills of the people who implement them and the awareness of those who need to adhere to them.

Top eight computer vulnerabilities


Continued use of default credentials
Poor network design
Unnecessary services in use
Technology
Poor decommissioning of old software
Failure to keep software up to date
People
Process
Lack of protection
Increased storage of passwords
Failure to encrypt online communications

The Cyber Essentials scheme has been developed by the UK Government to help organisations deal with the business-critical issue of cyber security and cyber resilience. The scheme provides a set of controls that organisations can implement to achieve a basic level of cyber security. https://www.itgovernance.co.uk/cyber-essentials-scheme

Auditor – Trusted Advisor

To what extent is your organisation making the most effective use of internal audit and the knowledge, skills and experience that this service has to offer? For those who are, internal audit is delivering far more than traditional compliance and risk based audits, with auditors working closely with management to provide proactive advice, support and challenge over both existing activities and new developments.

For this to be truly effective though, there needs to be trust, both in terms of the individual auditor concerned and the quality and nature of the advice provided. So, how is this achieved and what are the attributes you should expect from this 'trusted advisor'?

Well, for a start, the modern auditor will be receptive and open minded in their approach, especially in times where there are huge pressures on our organisations to make savings, often through modernisation and innovation, which may ultimately lead to some reduction in control. Clearly, as well as producing financial savings, these initiatives are also likely to result in a greater risk exposure for the business. This is where the modern, truly effective auditor comes to the fore, by supporting innovation and (perhaps rather scarily for some!) even encouraging properly informed and considered risk taking.

Whilst risk taking is not necessarily an attribute you would expect from an auditor, we, as a profession, recognise that there are times when this is absolutely the right thing to do, providing the implications are properly understood and there is the right level of reward relative to the risk.

Rather than act as a barrier to these initiatives, your auditor will utilise their professional expertise and understanding of the business, and its drivers, to help management ensure risk implications are clearly identified, evaluated and, on the occasions where it is necessary to do so, effectively mitigated.

Clearly, there may be times where the advice from the auditor does not necessarily align with the original views of management. This is fine. What is important, is that your auditor appreciates all perspectives, has a clear rationale for their opinions, which are founded on an evidence based, objective judgement, and this is all communicated in a clear and constructive manner. A trusting relationship between management and the internal auditor, will enable all opinions to be expressed and considered, leading to far better business decisions.

Finally, it is also important to recognise that, due to the nature and scope of their work, your auditors will have an extensive knowledge of your entire organisation and its activities, supplemented by information and intelligence about other organisations available through strong professional networks, regionally and nationally. This is therefore a valuable resource which is openly available and which management should be seeking to exploit at every opportunity. Are you?

Contact details

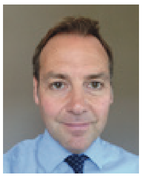
Gerry Cox

Chief Executive,
South West Audit Partnership
01935 385906
gerry.cox@southwestaudit.co.uk

Neil Pitman

Head of Partnership,
Southern Audit Partnership

01962 845139
neil.pitman@hants.gov.uk



Russell Banks

Chief Internal Auditor,
Orbis,
01273 481447
russell.banks@eastsussex.gov.uk

Robert Hutchins

Head of Partnership,
Devon Audit Partnership
01392 383000
robert.hutchins@devonaudit.gov.uk

Max Thomas

Director and Head of
Internal
Audit, Veritau
01904 552940
max.thomas@veritau.co.uk

Jean Gleave

Head of Internal Audit,
Salford and Warrington
shared service
01925 442354
jgleave2@warrington.gov.uk

Terry Barnett

Head of Assurance,
Hertfordshire Shared Internal Audit
Service 01438 845508
terry.barnett@hertfordshire.gov.uk

Alix Wilson

Head of the South West London Audit
Partnership
020 8891 7291
alix.wilson@richmond.gov.uk

Richard Boneham

Head of Audit Partnership,
Central Midlands Audit Partnership
01332 643280
richard.boneham@
centralmidlandsaudit.co.uk

The group meets quarterly and we circulate periodic bulletins to our Partner organisations with the aim of sharing information and best practice.

We hope that you find the bulletins useful. If you have any comments or feedback on this bulletin or have suggestions for future articles then please contact one of the individuals above.