

# An Internal Audit View

## Welcome to the fifth 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.

We welcome two new audit partnerships to Audit Together — the South West London Audit Partnership which covers the 5 boroughs of Richmond, Wandsworth, Sutton, Merton and Kingston and which also provides audit services to Achieving for Children (AfC), a community interest company wholly owned by Richmond and Kingston — and Central Midlands Audit which has the following 6 partners (all from within Derbyshire and Nottinghamshire):

- Derby City Council (partnership Host)
- South Derbyshire District Council
- Ashfield District Council
- Amber Valley Borough Council
- Derbyshire Fire & Rescue Service
- Derby Homes.

Contents: **High Impact Risks** 2    **Public and Private Sectors** 3    **Partnership Working** 4    **Cyber fraud** 5

## IR35 Legislation Change

### What is IR35?

IR35 (sometimes referred to as the Intermediaries Legislation) has been in place since 2000. This legislation aims to ensure that individuals who work through their own company, pay employment taxes in a similar way to employees, where they would be employed were it not for the intermediary that they work through.



### What's Changing?

From 6th April 2017, the responsibility for deciding whether the legislation applies, has shifted from the worker to the Public Sector Body (including schools), agency or third-party that is paying them. From this date, Public Sector Bodies (PSB's) are required to identify workers provided through intermediaries and assess whether the workers are in-scope of IR35. PSB's will be required to deduct PAYE and NI from payments for workers assessed as being in-scope, and remit them to HMRC as part of the normal payroll processes.



### What happens if we don't get this right?

PSB's that do not deduct and pay over PAYE and NI for affected workers will be liable themselves for the deductions that they should have made. HMRC also has powers to charge interest and levy a penalty where it considers that an employer has not acted with due care. A failure to put appropriate processes in place could result in the PSB facing a significant bill.

### What can we do?

PSB's will have hopefully already taken action to ensure that they are complying with the change in legislation. However, a checklist has been included below to assist with implementing the recent changes:

- ✓ PSB's should start by identifying a long-list of suppliers that are potentially in scope

- ✓ PSB's should review the ownership and employment status tests in order to identify what information will be required to assess IR35 suppliers
- ✓ PSB's should ensure that all service suppliers are contacted to advise them of the change in legislation, and what the PSB's approach to assessment will be
- ✓ PSB's should consider how each type of supplier might best be paid, and document this decision
- ✓ PSB's should consider whether or not to allow an appeals process, for contractors affected by the legislation change, and how any such process would operate
- ✓ PSB's should consider including an indemnity in relevant contracts to protect the PSB in the event of a successful challenge to a good-faith decision on IR35 status
- ✓ PSB's should ensure that pro-forma tenders and contracts for services are updated to include information about the application of IR35. Pro-forma tenders should also contain a section requesting the information required for the IR35 assessment to be carried out

Whilst the above checklist is not a definitive list of every action that the PSB will need to take, it hopefully provides a useful reference point for those organisations who are just starting to consider the implications of the new legislation. Further guidance in relation to the changes has been made available, and we have highlighted some key links below.

#### **Background to the new policy**

<https://www.gov.uk/government/publications/off-payroll-working-in-the-public-sector-reform-of-the-intermediaries-legislation/off-payroll-working-in-the-public-sector-reform-of-the-intermediaries-legislation>

#### **Overview of the changes**

<https://www.gov.uk/guidance/off-payroll-working-in-the-public-sector-reform-of-intermediaries-legislation>

#### **Tool to assist Public Sector Bodies with the assessment process**

<https://www.gov.uk/guidance/check-employment-status-for-tax>

## High Impact Risks - Are we learning the lessons?

The recent tragic events resulting from the Grenfell fire have saddened us all.

We know that such events do not occur that often, but when they do the impact on individuals, communities and organisations can be, and is, profound.

We also know that neither individuals or organisations are perfect; mistakes will be made and there is the awful inevitability that, occasionally, these kind of events can occur.

So, how can we learn from what has occurred at Grenfell and use this learning for future good? We are sure that every organisation started a review of their own buildings as soon as practically possible after Grenfell, and the results of this work will result in practical changes for the good.

But we wonder if organisations can use the learning from key events (such as this) to help them envisage where a significant issue could arise, and how they can be better prepared to deal with it?

Risk Management arrangements generally provide a matrix scoring approach to determine probability and

impact. As we work with decreasing resources it may be that with “highly probable” risks receive more attention and are addressed more quickly than “high impact, but low probability” risks. Is there a concern that some low probability, but high impact risks are put on the back burner – after all they are unlikely to occur?

The Risk Management process can often not predict the cause of a risk, but it can help predict the risk itself. In the case of Grenfell, the risk would have been along the lines of “Fire, or other significant event threatening the life and property of residents in a high rise building”. The enquiry will reveal the actual causes in this case, but the risk itself will not be changed. Having a good understanding of the risk does help organisations consider their mitigating actions, and how effective these can be.

There will be lots of lessons from Grenfell that will help ensure there is no repeat. But there is a need to ensure your risk management arrangements help, as best they can, in identifying those high impact, but low probability risks, that can have catastrophic results.

If you want further advice or assistance on capturing your risks, please contact your internal audit team.

# When the Public and Private Sectors Meet

With local authorities facing significant funding challenges over the next four years and beyond, additional budget requirements will need to be funded through a combination of efficiency savings and income generation.

It is against this backdrop that many local authorities are giving consideration to how they can maximise revenue generation, encourage innovation, improve commercial acumen and become more enterprising. As a result of this, some traditionally cautious approaches to risk, and potentially risk appetites as a whole, may need to be revisited and adjusted.

**“...maximise revenue generation, encourage innovation, improve commercial acumen and become more enterprising.”**

Schemes that are being considered by some authorities range from those activities that would be seen to be more aligned with local authorities e.g. Recruitment Services and Property Development Companies; to those that are taking councils into uncharted areas such as local taxi services based around the ‘Uber’ model.

The modern day Internal Auditor works with the business to establish proportionate levels of control delivered in a pragmatic way and it is important that they respond to the challenges that clients are facing with an equally flexible and open minded approach to providing assurance.

**“The modern day Internal Auditor works with the business to establish proportionate levels of control delivered in a pragmatic way...”**

Two factors that may initially cause public sector auditors concern are: the speed of decision making; and the need to take advantage of opportunities that may not be able to be realised if a highly bureaucratic process is required. Here it

is important to go back to first principles i.e. how material is the area of activity being considered? What is the likelihood of associated risk coming to fruition? Importantly, they need to constantly ask themselves how much does a too stringent approach to control impact on the overall successful completion of the task, project etc.

Many outputs based contracts provide for a particular level of flexibility around decision making; this can include operating without the need for every part of a process to be documented in triplicate and authorised by multiple parties. Whilst the use of public funds means that there must be an agreed minimum which Internal and External Auditors are comfortable with, consideration must also be given to the potential loss of value that may occur if a local authority enters into a venture which requires a pace of activity that it cannot match.

**“...operating without the need for every part of a process to be documented in triplicate and authorised by multiple parties.”**

Partnerships with private sector providers of internal audit services is one way for their public sector equivalents to gain an insight into how the correct approach to internal control can be maintained in this brave new world. Such arrangements can also include specific training in how to approach what the traditional public sector auditor would consider the ‘grey’ areas as well as audit staff from both sectors working in tandem on a project.

Doubtless, in time, the question of whether public money has been spent correctly will be judged on the final outcome of a project or the financial return realised by an initiative rather than whether the risks that form part of the journey to get there have been fully mitigated. As uncomfortable as that may sound, acceptance of this, even in part, may be the only way for the profession to be able to prove its continued relevance and provide value to its stakeholders.

**“...what the traditional public sector auditor would consider the ‘grey’ areas.”**

# The Benefits of Partnership Working

Pressures on public sector budgets means that organisations are required to maintain services whilst absorbing inflationary increases and in reality are often struggling to do more with less!

Internal Audit teams are no exception and, as the risk environment changes and becomes increasingly more complex, raising the quality and expertise of small in-house teams can create a real challenge.

Audit Together is a collaboration of Audit Partnerships from across the UK. Between us we now cover 11 County, 11 Unitary, 5 London Borough, 31 District/Borough Councils – 7 Police and 4 Fire Authorities - there are also a range of educational establishments, including Academies and other public-sector bodies such as Town Councils.

As standalone partnerships each recognise the following benefits:

- Sharing of ideas and best practice
- Access to specialist skills and knowledge
- Benchmarking and comparative data
- Challenge and a different perspective
- Efficiencies in time and effort
- No need to reinvent the wheel
- Affordability of resources



Through Audit Together these benefits are enhanced even further. We can help to support your Internal Audit Team in any of the following areas:

- Support the plans of other teams or provide specialist auditors as required
- Provide consultancy and advice
- Conduct Quality Assurance Reviews to assess compliance with the Standards
- Deliver Fraud Awareness Training

or you may wish to consider joining a Partnership in your region to enjoy the full benefits of working together. Please don't hesitate to contact us if you wish to explore any of these options further.

# Avoid being a victim of cyber fraud

## Phishing Attacks

Phishing involves the fraudster sending fake emails, social media messages or text messages to large numbers of unsuspecting potential victims. The emails or messages are designed to entice the recipient to hand over personal information, make a payment or download malware. In some cases the fraudster will also create a fake website to re-direct people to. Often these phishing emails 'spoof' the sender's address so they appear to originate from a legitimate organisation with a well-known and trustworthy brand (such as hmrc.gov.uk). Other variations also exist – fraudsters who call pretending to be from a bank or government agency and ask for personal information or text messages that encourage the recipient to call a fake premium rate number.

**“In some cases the fraudster will also create a fake website to re-direct people to.”**

These types of attack are well known but they often appear convincing so it is perhaps not surprising that people can still fall victim to them.

## Whaling

Another but more sophisticated variation is 'whaling'. This involves the fraudster sending a personalised email to a member of staff (usually in a senior position) that appears to have originated from a 'trusted' source for example the chief executive or director of finance. The e-mail will appear to be genuine but is designed to trick the recipient into disclosing information or initiating a payment. Sometimes the recipient will be directed to a bogus website specifically created for the purpose or the email will be followed up with a phone call. The email will often include the target's name, job title or other relevant information to make it appear more authentic. They will also usually convey a sense of urgency. Due to their focused nature, whaling emails are usually more difficult to detect than standard phishing attacks.

Whaling does not require the fraudster to have any detailed technical knowledge but the possible returns mean they are increasing in number.

The following actions can help reduce the threat of phishing and whaling attacks:

- Alert all staff to these types of fraud and remind them to be vigilant.
- Review the adequacy of defences (including sending internally generated 'spoof' emails to test behaviours) and follow up with training and guidance
- Instruct staff to treat unusual requests for payments extremely cautiously. Always try to speak to the person face to face or by phone, rather than relying on email or text message.
- If someone calls, hang up and call back using established contact details.
- Look closely at email addresses. Right click on the address and select Outlook Properties. If an email address has been spoofed then the actual email address will appear.

Remember that some attacks will be too well crafted and no amount of user awareness and training can guarantee their detection. Agree reporting mechanisms so that if you do fall victim you can act quickly. In some recent cases organisations have been able to recover funds through prompt action.

The National Cyber Security Centre is also promoting the use of domain protocols to help reduce the risk of spam emails and phishing attacks. The guidance is intended for IT managers and systems administrators and is available from the NCSC website – [www.ncsc.gov.uk](http://www.ncsc.gov.uk)

Other sources of advice include:

Action Fraud – [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

CIPFA Counter Fraud Centre - [www.cipfa.org/services/counter-fraud-centre](http://www.cipfa.org/services/counter-fraud-centre)

Cyber Aware – [www.cyberaware.gov.uk](http://www.cyberaware.gov.uk)

Cifas – [www.cifas.org.uk](http://www.cifas.org.uk)

**“Due to their focused nature, whaling emails are usually more difficult to detect than standard phishing attacks.”**

## 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.