PART ONE **ITEM 07**

To: **Joint Audit Committee**

Date: **27th July 2017**

By: **Daniel Harris, RSM UK**

Title: **Internal Audit Progress Report**

Purpose of Report/Issue:

To update the Joint Audit Committee of Internal Audit's progress in achieving the 2017/18 Internal Audit Strategy since the last meeting of the Committee.

Recommendation

The Committee is invited to comment on RSM UK's progress to date in achieving the Internal Audit Strategy.

Contact details -

Name: **Lorna Raynes**
Job Title: **Manager, RSM UK**
Email address: **lorna.raynes@rsmuk.com**

OFFICE OF THE POLICE AND CRIME COMMISSIONER FOR SURREY AND SURREY POLICE

Internal Audit Progress Report

Joint Audit Committee presented to:

27 July 2017

RSM

CONTENTS

1 INTRODUCTION

The internal audit plan for 2017/18 was approved by the Joint Audit Committee in March 2017.

Below provides a summary update on progress against that plan and summarises the results of our work to date.

The report also provides an update on the remaining audits from the 2016/17 Internal Audit Plan. The first table in section 2 below confirms that we have finished the 2016/17 Internal Audit Plan and eight final reports have been issued since the previous Joint Audit Committee.

2 REPORTS CONSIDERED AT THIS AUDIT COMMITTEE

This table informs of the audit assignments that have been completed and the impacts of those findings since the last Joint Audit Committee held.

2016/17 INTERNAL AUDIT PLAN

Assignments	Status	Opinion issued	Actions agreed		
			H	M	L
Savings Plan (6.16/17)	FINAL	Partial Assurance	1	2	3
Managing Victims of Crime – Domestic Abuse (9.16/17)	FINAL	Reasonable Assurance	0	4	2
Follow Up of Previous Management Actions (10.16/17)	FINAL	Reasonable Assurance	2	9	0
Strategic Planning And Budgeting (11.16/17)	FINAL	Partial Assurance	1	2	1
Capital Expenditure (12.16/17)	FINAL	Reasonable Assurance	0	0	4
Risk Management (14.16/17)	FINAL	Reasonable Assurance	0	2	0
Preparations for PSN Compliance (15.16/17)	FINAL	Partial Assurance	0	6	0
Vetting (16.16/17)	FINAL	Partial Assurance	0	1	1

2.1 Impact of findings to date

All the reports finalised since the last Audit Committee relate to 2016/17 and therefore are reflected in our annual report which was presented to the March 2017 Joint Audit Committee Meeting.

We have yet to issue any 2017/18 reports.

3 LOOKING AHEAD

Assignment area	Status	Target Audit Committee per the IA Plan 2017/18
Evidential property (management concern)	Undergoing quality review	September 2017
Governance – Code of Ethics (Sector risk)	17 July 2017	September 2017
Tasers (sector risk)	20 July 2017	July 2017
Commissioning - Grants	3 August 2017	December 2017
Collaboration strategy (Joint risk 432)	2 October 2017	December 2017
Financial Controls	30 October 2017	March 2018
Data Protection (Sector risk)	Draft scope issued, dates to be confirmed	March 2018
Estates Strategy and Disposals	Scoping meeting held	December 2017
Proceeds of Crime Act (P+CP and Management concern)	Dates and scope under discussion	December 2017
Business Interests	Dates and scope under discussion	September 2017
Small assets/uniform	Dates and scope under discussion	September 2017
Mandatory Training	Dates and scope under discussion	July 2017
Follow Up	Dates and scope under discussion	September 2017 & March 2018
Procurement	To confirm responsibility for IA[1]	July 2017
Vehicle Maintenance	To confirm responsibility for IA[1]	September 2017
IT reviews (Force risk 458)	To confirm responsibility for IA[1]	March 2018

[1] These audits related to areas which are operated jointly with Sussex Police and therefore we are awaiting confirmation of whether these audits will be led by us or the auditors for Sussex.

4 OTHER MATTERS

4.1 Changes to the 2017/18 audit plan

We have been requested to complete a review of Financial Reporting and Forecasting. We are currently discussing the scope of this potential work with management. In addition the focus of our governance review has been requested by management to be on structures regarding the possible collaboration with Surrey Fire rather than on ethics as originally planned.

4.2 Added value work

Since the last meeting was have issued the following client briefings:

- RSM Emergency Sector Updater – June 2017
- The Apprenticeship Levy
- How vulnerable is your organisation to Cyber attacks?
- Are you vulnerable to email scamming?
- GPDR Readiness

We have appended these to the bottom of this report.

APPENDIX A: 2016/17 INTERNAL AUDIT ASSIGNMENTS COMPLETED TO DATE

Reports previously seen by the Audit Committee and included for information purposes only:

Assignment	Opinion issued	Actions agreed		
		H	M	L
Policies and Procedures (1.16/17)	Reasonable Assurance	1	3	2
Governance (2.16/17)	Substantial Assurance	0	0	4
Crime recording (3.16/17)	Partial Assurance	2	1	1
Complaints (4.16/17)	Substantial Assurance	0	1	0
Cash Handling (5.16/17)	Advisory	0	4	3
Financial Controls (7.16/17)	Reasonable Assurance	0	2	3

FOR FURTHER INFORMATION CONTACT

Name: Daniel Harris, Head of Internal Audit

Email address: Daniel.Harris@rsmuk.com

Telephone number: +44 (0) 7792 948767

Name: Lorna Raynes, Client Manager

Email address: Lorna.Raynes@rsmuk.com

Telephone number: +44 (0)7972 004175

EMERGENCY SERVICES SECTOR UPDATE

June 2017

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

CONTENTS

INTRODUCTION

Welcome to RSM's latest emergency services sector briefing which this quarter focuses specifically around managing risks.

Managing risks effectively has never been more important. The recent ransomware cyber-attack that affected thousands of organisations, including the NHS, demonstrates what can go wrong when appropriate safeguards have not been put in place. Our recent cyber security report explores this in much more detail. With the Policing and Crime Act 2017 now very much in force and increased collaboration on the horizon, it's important that the sector continues to review governance arrangements to manage all risks effectively.

Along with our usual summary of key publications and guidance in this edition we also provide articles on:

- people risk;
- gender pay gap reporting; and
- IR35 – new intermediaries legislation.

Much has been said about the sector already in the build up to the general election in June and many continue to speculate about what may lie ahead. The sector must of course have one eye on the future, but attention must not be taken away from the here and now. Risks must be managed effectively.

We hope you find this update a useful source of insight. If you have any queries, or suggestions for future editions, please contact either myself, or your usual RSM contact and we will be delighted to help.

Daniel Harris
National Head of Emergency Services and Local Government

TECHNICAL UPDATE – FURTHER GUIDANCE AND PUBLICATIONS POLICE AND FIRE

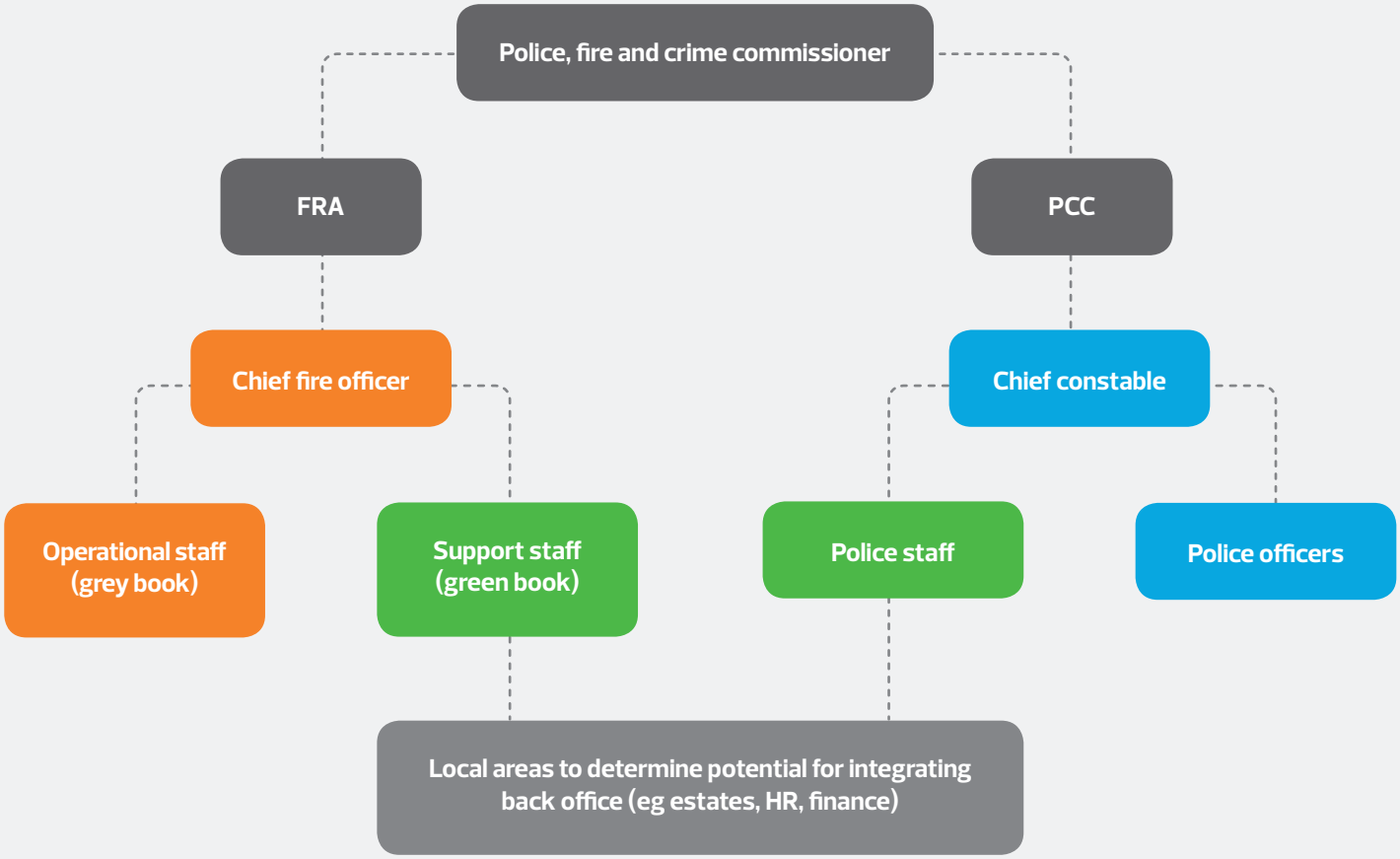
Police and fire business case

With the Policing and Crime Act 2017 now in force, it is pertinent to consider guidance for chief executives of Offices of Police and Crime Commissioners published by the Association of Policing and Crime Chief Executives (APACE) regarding the duty for emergency services to keep opportunities for collaboration 'under review' and where a case is made, for the Police and Crime Commissioner (PCC) to 'take responsibility for the governance of their local fire and rescue service'. The guidance details the processes PCCs are required to follow as a result of the Act, with a particular focus on the 'five case model,' the standard used by HM Treasury for drafting public sector business cases.

Questions for audit committee's consideration:

- What assurance is being obtained on the quality of any business cases developed to ensure they meet the requirement within the 'five case model'?
- Have the financial assumptions been subject to independent scrutiny?
- Is regular and informative progress being received at the right level on the progress made?

GOVERNANCE MODEL



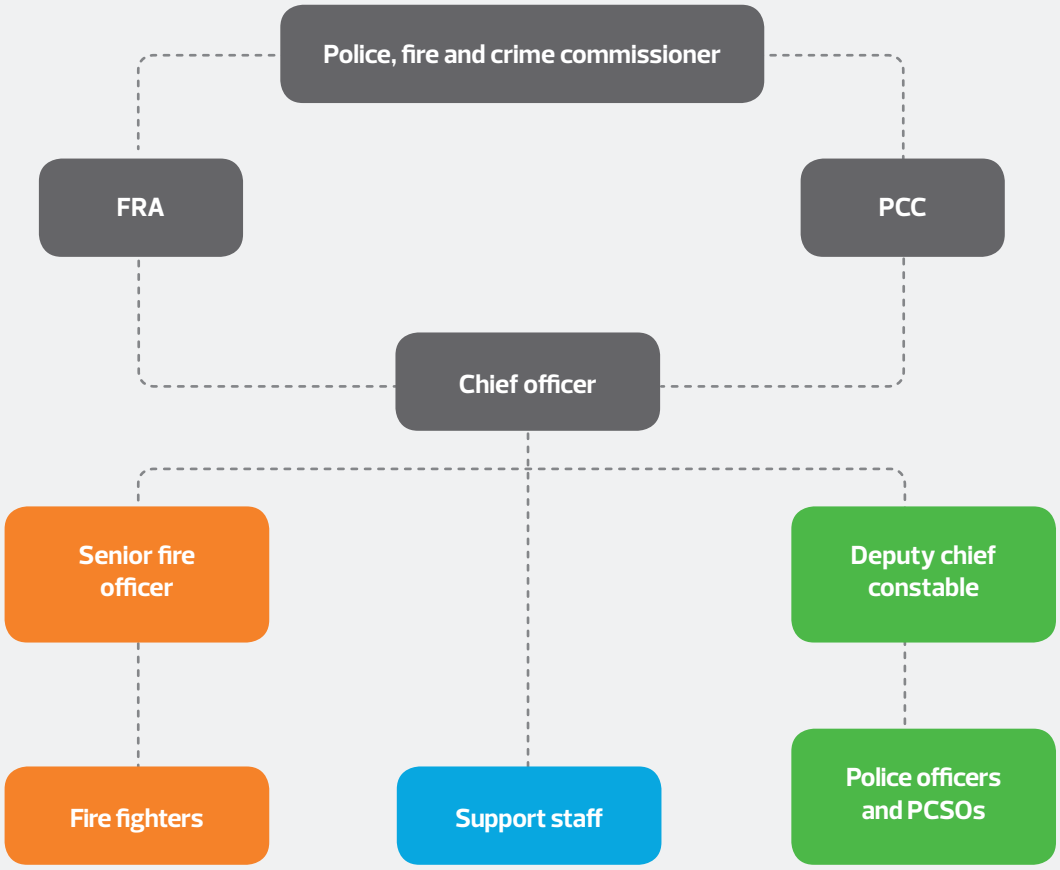
PCC governance of fire and rescue authorities will occur only when a local case is made that is deemed to be:

'in the interests of efficiency, economy and effectiveness, or public safety.'

Various factors that PCCs need to be aware of when looking into taking over governance for a fire and rescue authority (FRA) include:

- the boundaries of the PCCs area and the FRA area they are proposing to take responsibility for must be 'coterminous'. This means that a PCC cannot propose to take responsibility for only one FRA in an area where others are also situated in their police area;
- a PCC responsible for the governance of a FRA would become a 'Police, Fire and Crime Commissioner' (PFCC);
- the PFCC would be required to prepare both a policing and crime plan and a strategic fire and rescue plan but may decide locally whether to combine these plans; and
- the PFCC could decide to run a 'single employer model', whereby one 'chief officer' could be appointed who employs both police and fire personnel.

SINGLE EMPLOYER MODEL



THE CYBER THREAT

Published by the National Cyber Security Centre (NCSC) in collaboration with the National Crime Agency, is the first annual threat assessment of cyber-attacks to the UK, which remarked on the 'significant and growing threat.' Of course this cyber threat posed to individuals, organisations and government has never been more apparent with the recent outbreak of the 'WannaCry' ransomware, which has seen 200,000 victims in over 150 countries affected with many systems still at risk. It is against this backdrop that we have published the results and report of our cyber-crime survey. (https://www.rsmuk.com/ideas-and-insights/tackling-cyber-crime-complacency)

Commenting on the joint annual threat assessment, our Technology Risk Assurance partner, Sheila Pancholi stated

> Today's annual assessment published jointly by the NCA and the NCSC underlines that the risk to business from cybercrime is significant and growing. Within the last year, 65 per cent of large UK firms have detected a cyber security breach or attack and this is likely to be the tip of the iceberg.

The NCSC has also published a report on how the cyber crime online business model actually works; looking in detail at how organised criminal groups (OCGs) exploit low risk low cost criminal activities that are not 'actively prosecuted by the authorities.' The report looks in depth at the various functions of an OCG, from the 'team leader' to the 'data miner', who can extract key data from large bulk intercepts that are growing in prevalence in cyberspace.

If you have any concerns relating to your organisations cyber security please contact a member of our Technology Risk Assurance team. (https://www.rsmuk.com/what-we-offer/by-service/risk-advisory/technology-risk-solutions)

Questions for audit committee's consideration

- How recent is your assurance on cyber threats?
- Are your controls, mitigations and assurance needs kept under constant review as the situations and real life examples of attacks evolve?
- Have you compared the outcome of the threat assessment of cyber-attacks to the UK to your arrangements to identify any vulnerabilities that require action?

Upgrading emergency services communications

The Public Accounts Committee (PAC) is 'greatly concerned' that the introduction of the Emergency Services Network (ESN) has been delayed, but also 'is not likely to be deliverable' within these delayed timescales, and with 'potentially catastrophic' new operational information regarding the use of current system 'Airwave' coming to light.

The hastily published report 'Upgrading emergency communications – recall' which closely follows a report on the ESN by the PAC in January 2017, comes after revelations from Motorola, the owners of Airwave, that extensions to keep the Airwave system running after March 2020 could now not be possible due to upgrade works planned by supplier Vodafone that would make the Airwave system unusable unless additional compatibility work for Airwave is performed. The PAC emphasised the importance of the Home Office engaging with Motorola and Vodafone to find a solution to this impending problem highlighting the huge effects any shutdown of service would have on the emergency services. The Home Office was also criticised for the 'little slippage' (nine months) of the transition period for the ESN to September 2020, and the additional issues this will cause in establishing which regions will require 'dual running' of the ESN and Airwave in the transition period.

In addition the PAC was critical of the Home Office's risk identification and management, stating that the Home Office 'did include a general risk around extending what was ageing equipment but it did not anticipate the specific issue that has occurred,' with the PAC also expressing its surprise that Motorola themselves did not pick up on the issue when conducting due diligence before the companies purchase of Airwave in February 2016.

POLICE

Pre-charge bail

The limiting of pre-charge bail to 28 days has come into force upon the commencement of the Policing and Crime Act 2017 with the Home Secretary, Amber Rudd, calling the limit 'important reforms [which] will mean fewer people are placed on bail and for shorter periods. They will [also] bring about much-needed safeguards – public accountability and independent scrutiny.'

In response the Chair of the Association of Police and Crime Commissioners, Dame Vera Baird QC, stated that whilst welcoming the changes, that 'Police and Crime Commissioners will want to monitor the resource implications of these changes on police forces around the country'. Citing that time should not be wasted seeking extensions in court when operational matters, such as obtaining forensic reports can take months, well beyond this new 28 day pre-charge bail limit.

Custody images

The Home Office has published the report of its review over the use and retention of images of people taken in police custody. The review, brought about by a 2012 high court case regarding the retention of images from unconvicted individuals, sought to advise government ministers on three areas: the current legal and operational framework; the utility and benefits of custody images in 'meeting policing purposes'; and the options for change where this appears necessary in relation to regulation, governance, oversight, policies and guidance.

A major proposal in the report is to allow individuals not convicted of the offence in relation to their custody image to apply to chief officers of the requisite force to have such images deleted. It is reported that despite there being a number of images of the person there are over 19 million images stored on the Police National Database overall.

Use of force

Police forces now have new reporting requirements over their 'use of force' following an announcement by the Home Secretary. The new requirements see forces obligated to record all incidents where force is used, including physical restraint. Police forces are also now required to record the location and outcome of Taser usage, along with the ethnicity and age of those involved, with the first data release due at local level by the summer. The new requirements come as the government confirmed that it plans to introduce 'TASERX2' to all police forces in England and Wales.

More news from Westminster

The Home Affairs Committee has had its first oral evidence session on its inquiry entitled 'policing for the future'. Witnesses including criminology academics and policing experts expressed their views, with one expert calling for better reporting of cybercrime particularly as the sector finds itself in the midst of a 'cybercrime wave'.

Minister of State for Policing and the Fire Service, Brandon Lewis, delivered a speech on police professionalisation, with a focus on the Policing Education Qualifications Framework (PEQF).

Security Minister, Ben Wallace, used a speech at the Home Office's Serious and Organised Crime Conference in Birmingham to highlight the importance of police and local authorities working closer together to tackle serious and organised crime. Mr Wallace called for police and local authorities to share information on known crime groups and identify where attempts are being made to profit from public sector contracts.

FIRE

An inclusive service

The Local Government Association (LGA), a representative of all fire and rescue authorities in England and Wales, has launched a new report outlining a major drive to change the public perceptions of firefighters, including potential new recruits, with the LGA stating that many 'are deterred by outdated perceptions of the job'. The document has three principle objectives:

- to provide an opportunity for representatives of female, ethnic minority and the lesbian, gay, bisexual and transgender (LGBT) community, firefighters to set out their problems that fire and rescue services needs to address;
- to suggest some of the practical steps that can and are being taken to improve diversity; and
- to pose questions that fire and rescue authority members may ask of themselves and the wider service.

The report details a recruitment survey that features some revealing statistics, such as: around a third of firefighters are expected to retire in the next five years; and 48 per cent of respondents stated they had processes in place to monitor the application progress and thus the dropout rates of females, black and ethnic minority groups and of LGBT candidates.

Questions for audit committee's consideration

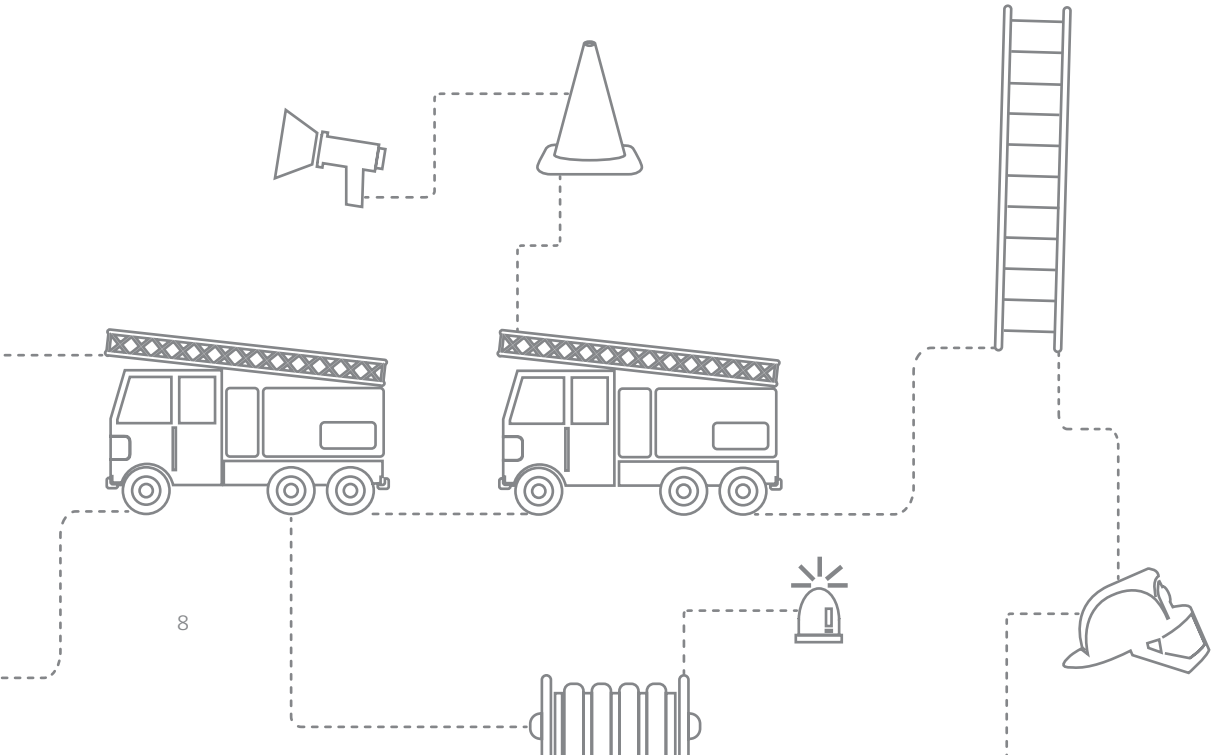
- Have you reviewed the LGA report to identify what further actions can be taken?
- What are you doing locally to make your fire service more inclusive and are you getting assurance on its success?

Updated framework

The Home Office has published the third edition of the national coordination and advisory framework (NCAF) for the fire service in England. Developed jointly between the Home Office and the National Fire Chiefs Council, the framework aims to provide the advice and guidance needed to support fire and rescue services in times of major emergencies or incidents. The revised NCAF has come about due to organisational changes and lessons learned from emergencies.

Questions for audit committee's consideration

- Are all relevant officers in your organisation aware of the updated framework and adjusting working practices if required?



SOURCES OF FURTHER INFORMATION

'Guidance for OPCC Chief Executives' – Association of Policing and Crime Chief Executives http://apace.org.uk/documents/APACE_Police_Fire_Business_Case_Guidance.pdf

'The cyber threat to UK business' – National Cyber Security Centre & National Crime Agency http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file

'The Icarus effect: tackling cybercrime complacency' – RSM UK https://www.rsmuk.com/ideas-and-insights/tackling-cyber-crime-complacency

'Weekly threat report 24th October 2016' – National Cyber Security Centre https://www.ncsc.gov.uk/report/weekly-threat-report-24-october-2016

'Cyber threat facing business is 'significant and growing'' – Sheila Pancholi, RSM http://www.rsmuk.com/news/cyber-threat-facing-business-is-significant-and-growing

'Cyber crime: understanding the online business model' – National Cyber Security Centre https://www.ncsc.gov.uk/file/2390/download?token=kZc2hbea

'28 day pre-charge bail limit comes into force' – Home Office https://www.gov.uk/government/news/28-day-pre-charge-bail-limit-comes-into-force

'28-day pre-charge bail limit comes into force' – Comment by APCC Chair Dame Vera Baird QC http://www.apccs.police.uk/press_release/28-day-pre-charge-bail-limit-comes-force/

'Review of the Use and Retention of Custody Images' – Home Office https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf

'New transparency measures for Taser use announced by Home Secretary' – Home Office https://www.gov.uk/government/news/new-transparency-measures-for-taser-use-announced-by-home-secretary

'Oral evidence: Policing for the Future: Changing Demands and New Challenges' – Home Affairs Committee http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/policing-for-the-future-changing-demands-and-new-challenges/oral/49475.pdf

'Speech to the Police Education Qualification Framework conference' – Brandon Lewis MP https://www.gov.uk/government/speeches/speech-to-the-police-education-qualification-framework-conference

'Closer partnerships needed to fight serious and organised crime' – Ben Wallace MP https://www.gov.uk/government/news/closer-partnerships-needed-to-fight-serious-and-organised-crime

'An inclusive service, The twenty-first century fire and rescue service' – Local Government Association http://www.local.gov.uk/inclusive-service-twenty-first-century-fire-and-rescue-service

'The National Coordination and Advisory Framework (NCAF) England' – Home Office and National Fire Chiefs Council https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/604453/2017_03_23_NCAF.pdf

HOW SAFE ARE YOUR PEOPLE?

Senior management and audit committees are fully aware of risk management and the need to put assurance measures in place. But how often do you think people risks are included within risk management?

When we visit emergency services organisations we often hear:

- we are a people business;
- our people are our greatest asset; or
- we are customer focused.

Or their organisational objectives relate to:

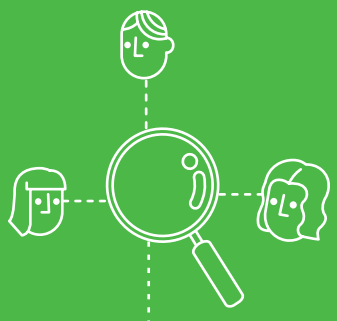
- developing people;
- ensuring service quality;
- building workforce capability; or
- creating a fit for future culture.

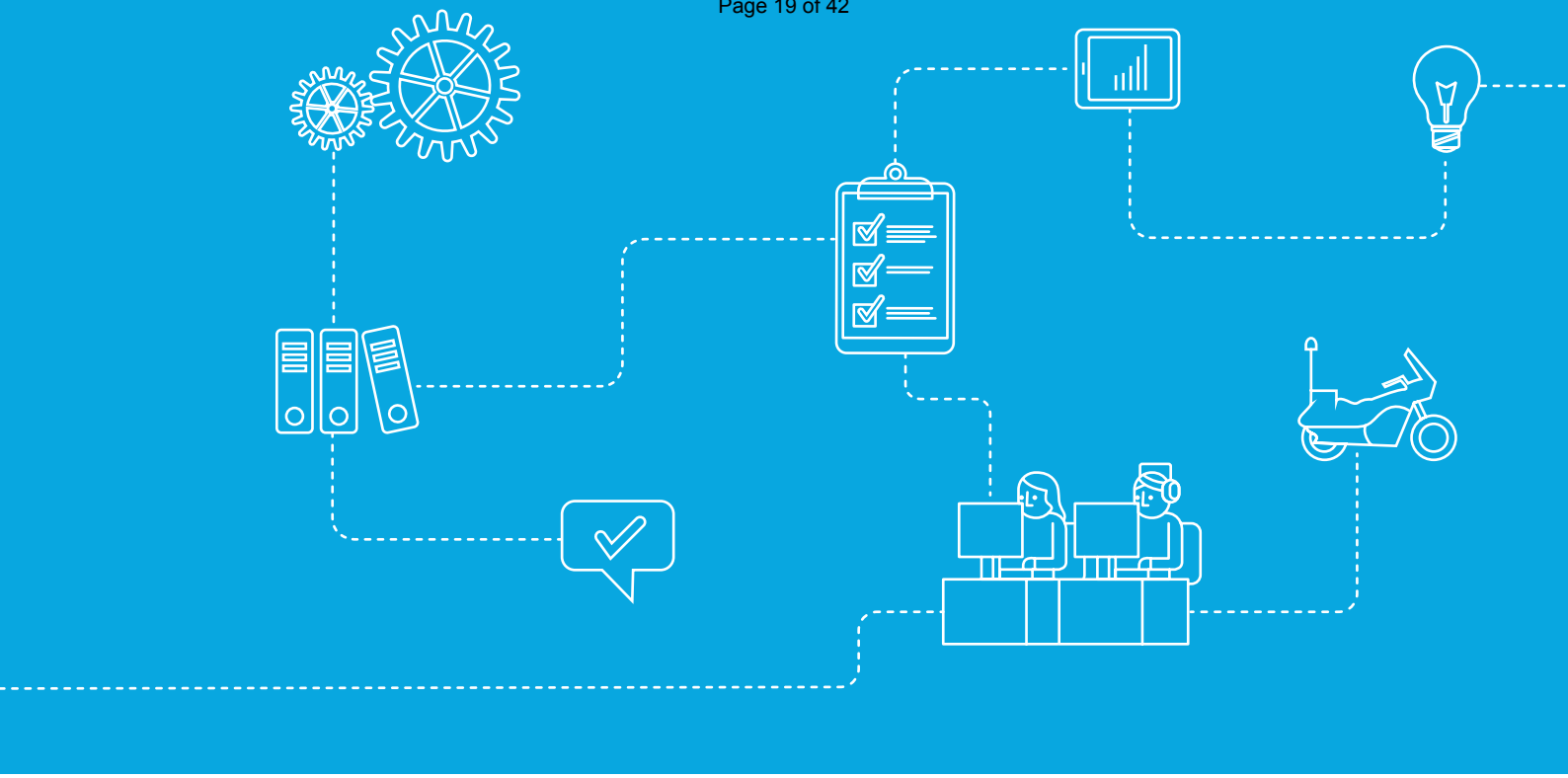
These statements demonstrate the importance of 'our people' and how the right people will represent your organisation to drive growth and development. Unfortunately many recent high profile cases have highlighted where the people have got it wrong. The damage in some cases is irrecoverable to the organisation but in all instances organisations incur unexpected rectification, fines and reputation damage at a personal and entity level.

People risks relate not only to your employees but to the actions those people take and the decisions they make once recruited.

With the potential implications for your organisation, your staff and service users being significant, could your organisation confidently answer the questions below?

- How do you ensure your staff and contractors continue to perform to the required levels?
- How do you ensure that the public remain satisfied?
- Is your reputation in tact?
- How do you keep your employees safe?





How to avoid your greatest assets becoming your greatest liability

Based on our experiences, we have identified the following key elements that help achieve 'safe people' and how to mitigate the risks associated.

- **A robust recruitment process** thorough vetting and checks on applicant references, experiences, qualifications, health and background.
- **On boarding and induction procedures** ensure new starters have a strong understanding and fit with your organisation and provide regular feedback as they learn their job.
- **Personal objectives and appraisal** establishing clear expectations for employee performance and enabling everyone to know when individuals and the organisation is succeeding.
- **Policy and procedures** ensure they're up to-date, communicated and understood across all levels. This enables your people to understand what is expected of them, to know their operating boundaries and what is acceptable and what is not.
- **Training and development** ongoing, mandatory training, throughout the year, for your people to maintain and build the skills and knowledge required to perform their role to the best of their abilities.
- **Equipment and tools** whether it's IT equipment, vehicles or high vis jackets. Ensure they are fit for purpose to enable your people to fulfil their roles safely.
- **Creation of the right culture** continuously communicates your organisation's vision, mission and core values. After all you want your staff to behave correctly and act accordingly for the organisation and its service users.
- **Monitoring, reporting, review and rectification** management and governance mechanisms must provide assurance that the arrangements in place keep your people, and you, as the employer, safe. The procedures should be regularly reviewed to ensure they're effective and if not, how to correct them.

To avoid your organisation becoming one of those that are not considered a 'safe pair of hands' we recommend you seek assurance that your people are safe by:

- an assessment, by HR specialists, of the arrangements in your organisation that keep your people safe;
- a review of your policy and procedures to ensure that they are relevant and reliable; and
- the deployment of a policy management and learning system to assist in the communication and understanding of policy and procedures by your people.

So, just how safe are your people?

For further information please contact our risk and governance team (details on back page) and visit **www.insight4GRC.com** – RSM's Governance, Risk and Compliance suite.

GENDER PAY GAP REPORTING

The essentials of gender pay gap reporting

New legislation on gender pay gap reporting came into force on 31 March for the public sector. The overall aim is to address the imbalance in pay between men and women in the workplace.

The legislation requires organisations with 250 or more employees to publish online any gender pay or bonus gaps for men and women, the proportion of men and women who receive bonuses and quartile statistics for all employees in the organisation.

Employers need to publish their gender pay gap results within one year of their snapshot date (31 March for the public sector). Failure to do so will be unlawful so employers need to take steps now in order to become compliant.

The regulations are fairly complex, more so if your organisation is part of a group of companies/bodies/authorities or co-joined organisational groups: has a number of different types of workers (employees, casual workers, contractors) and/or has a complex payroll with numerous pay elements.

Once employers have decided on the number of reports they need to run they must ensure they include all the right people within them. This is not as straight forward as it sounds as the regulations ask employers to use the Equality Act's extended definition of an employee. There is also specific guidance on how to treat part time workers, partners and overseas workers.

RSM is already working with a number of clients who require additional support in order to comply with the new legislation and in particular the two areas discussed above. If you are unsure about anything, we recommend you seek specialist advice in these areas before you pull together your figures.

Finally, employers will need to make sure they treat all the pay elements correctly. Some pay items are classified as 'ordinary pay' for the purposes of the regulations and others are not. For example, basic pay and allowances are classified as ordinary pay but overtime and redundancy payments are not. There are also some complex rules surrounding the treatment of salary sacrifice.

GENDER PAY GAP REPORTING NARRATIVE

The figures that are required to be published online simply provide a snapshot. This will keep you compliant. However, in our opinion, figures will be best supported by a narrative.

The narrative is voluntary but employers should consider what their figures might say about them without organisational or sector context. A well-researched, analysed and scripted narrative will help employers successfully position their own organisation's figures. It is for this reason RSM are seeing quite a few employers not only ask for help running their calculations, but also in drafting a narrative based on a deeper analysis into their figures and the sector they work within. If a gap is particularly high, a narrative can help to explain the reasons for this. If the figure is favourable, you may want to share the initiatives that have led to you achieving this.

If you are concerned about what a deeper analysis and narrative might uncover, you may decide it prudent to engage legal advice before you carry out this piece of work to ensure the findings are covered under legal privilege.

ADDITIONAL REPORTING REQUIREMENTS FOR THE PUBLIC SECTOR

In addition to the reporting requirements applying to private and voluntary sectors, public sector employers are required to provide additional reporting.

The regulations state that:

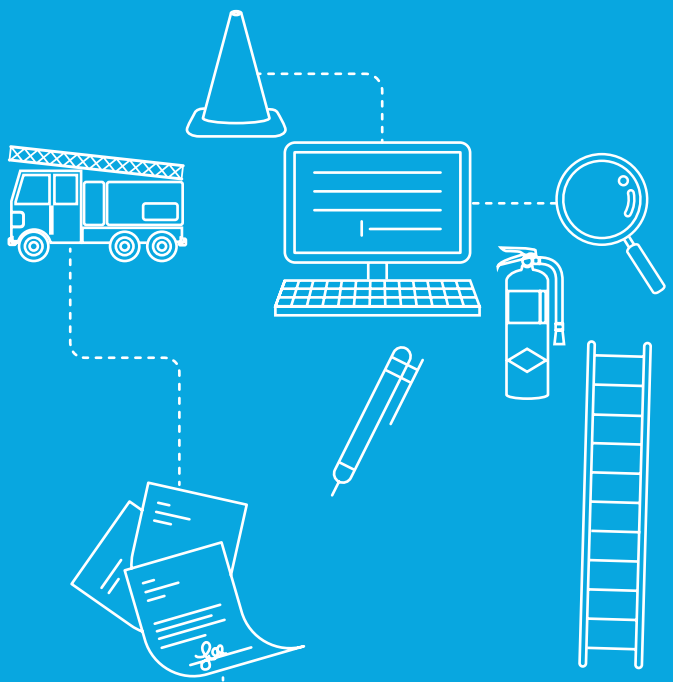
> The information a public authority publishes in compliance with paragraph (1) [of the regulations] must include, in particular, information relating to persons who share a relevant protected characteristic who are— (a) its employees; (b) other persons affected by its policies and practices.

This is in line with the requirements which already exist under the Public Sector Equality Duty (PSED), the deadline for reporting has simply been amended to be aligned with the Gender Pay Gap reporting timetable.

The Gender Pay Gap reporting requirements will now be incorporated into the reporting requirements of the PSED.

PSED aims to:

- eliminate unlawful discrimination, harassment, victimisation and any other conduct prohibited by the Equality Act 2010;
- advance equality of opportunity between people who share a protected characteristic and people who do not share it; and
- foster good relations between people who share a protected characteristic and those who do not.



HOW CAN YOUR ORGANISATION CLOSE ITS GENDER PAY GAP?

1) HR Strategy
If you haven't already placed the gender pay gap on your HR strategy for 2017/18 now would be the time to do so. Some larger organisations may already have Diversity and Inclusion Managers in place and have been reporting for some time. However, for many organisations this will be a new regulatory requirement to tackle.

The requirement is annual so it should be a permanent fixture in your HR strategy, not just a one off exercise.

2) Attracting and recruiting women
Some organisations will already be acutely aware of the difficulties their industry, sector or occupation has in attracting women into certain roles. But with the new reporting requirements perhaps now is the time to focus on how you can address those issues.

A lot of work takes place in schools to encourage girls into science, technology, engineering and mathematics (STEM) industries. Could you look to deliver something similar to attract more females into your sector and organisation?

3) Anonymous recruitment
There has been much written in the last few years about how unconscious bias could be contributing to some recruiters discriminating unfairly. Some employers have taken the step to carry out anonymous recruitment in order to remove that from the equation and that's something you could consider introducing.

4) Mentoring
Gender specific mentoring programmes for committed employees that show real potential is a great way to help individuals progress their careers and push themselves up into more senior positions.

5) Senior management development programmes specifically aimed at women
Many employers will already be committed to training and development programmes for all their staff in order to foster and develop talent. With the advent of this piece of legislation now is the time to review the courses you run and assess whether they are attracting and supporting women into those higher level programmes successfully enough.

6) 'Returnships'
Some employers are already offering 'returnships' to previously dedicated employed females who once held positions of responsibility, often having studied and worked really hard for their positions, but who exchanged roles in the corporate world for full time motherhood and a long career break.

Some investment banks and professional services companies have embarked on 'returnships' with much success; harnessing female talent back into their workforces. Gender diversity in senior roles depends on these sorts of programmes and it is definitely something worth considering.

7) Increased flexibility, working remotely, family friendly initiatives and enhanced maternity packages
Women can benefit greatly from the current technology that allows them a flexibility that never existed 10-15 years ago. Supporting remote and flexible working may help you to retain more female employees who may have to leave otherwise.

Offering an enhanced maternity pay policy is another good way to attract and retain more female employees within your organisation.

Our specialist HR team are working with many of our clients to help them meet their gender pay gap reporting requirements. Please contact a member of our team (details on the back page) if you would like to discuss how we can help you too.

WILL PUBLIC BODIES BE READY FOR THE NEW INTERMEDIARIES LEGISLATION?

The intermediaries legislation (known as IR35) has been in existence for many years and is well known by those affected by it. It ensures that individuals who work through their own personal service companies (PSC) pay employment taxes in a similar way to employees, where they would be employed were it not for the PSC or other intermediary that they work through.

However, due to concerns that IR35 is open to abuse and has not been effective in collecting all taxes due from such arrangements, the government has decided to adopt more stringent off-payroll workers rules for individuals working for public sector organisations through PSCs or their intermediary agents.

For all direct engagements between public sector organisations and PSCs, if the engagement falls within the intermediaries legislation conditions, income tax and NICs will need to be withheld by the public sector body at source through PAYE, and the relevant payment made to HMRC through RTI. In addition, the public body will also need to account for employer's NICs and any apprenticeship levy costs arising. If the engagement falls outside the intermediaries legislation conditions, the public body may pay the PSC or intermediary gross.

Where a public body engages a PSC worker through an intermediary agency, the public body will need to consider the intermediaries legislation and notify the agency whether income tax and NICs should be withheld from payments to the PSC at source.

What do public bodies need to consider?

- The new rules affect all payments to a PSC (whether direct or through an intermediary agent) made on or after 6 April 2017, even if the services were provided prior to this.
- The 5 per cent allowance available to PSCs engaged by other (non-public sector) organisations is not available as a deduction for the public body (or the PSC).
- VAT will remain payable to the PSC if the PSC is VAT registered.
- HMRC has set up an employment status intermediaries team that will monitor compliance of the new rules.
- The release of HMRC's online check employment status for tax digital tool should be used by public bodies and intermediary agencies that intend to rely on it to support their decision making in relation to ongoing engagements.

What should public bodies do to get ready for the changes?

- ensure that the consequential expected increase in costs for temporary workers is reflected in budgets for 2017/18;
- review and consider the impact on existing contractors whose services are likely to continue after April 2017;
- ensure they have a robust policy and process for engaging and paying the PSC/intermediary agency;
- ensure there are good communication channels with PSCs and agencies so that they can communicate the outcome of employment status reviews under the intermediaries legislation to them efficiently and effectively;
- review all existing contracts for services with PSCs and intermediary agencies; and
- consider the potential impact of the loss of key talent.

What should intermediary agencies be doing in relation to public body engagements?

- communicate details of the impact to existing workers;
- consider whether to increase agency rates to reflect a fall in the net take home pay by the worker and the increased employment costs (due to employer's NICs and apprenticeship levy contributions) of the agency;
- review all contractual relationships for temporary workers provided to public bodies; and
- consider the impact of some workers choosing to no longer work for public sector organisations.

Wider effects

The new off-payroll rules have wide reaching ramifications, both in relation to increased costs within the public sector as well as significant additional administration to ensure robust compliance by affected parties. This will put added pressure to frontline public services, which could lead to many workers terminating contracts with public sector bodies and thereby creating a major skill shortage in critical areas.

Moreover, increased scrutiny by HMRC and cases in which insufficient action is taken by public bodies to comply with the new rules will lead to additional tax settlements, interest and penalties, which could affect the budgets available to public sector organisations in the near future.

FOR FURTHER INFORMATION PLEASE CONTACT

Daniel Harris
National Head of Emergency Services and Local Government
M +44 (0)7792 948 767
daniel.harris@rsmuk.com

Matt Humphrey
Partner, Governance and Risk
T +44 (0)116 282 0550
matthew.humphrey@rsmuk.com

Caroline Rai
Partner, Tax and VAT
T +44 (0)20 3201 8162
caroline.rai@rsmuk.com

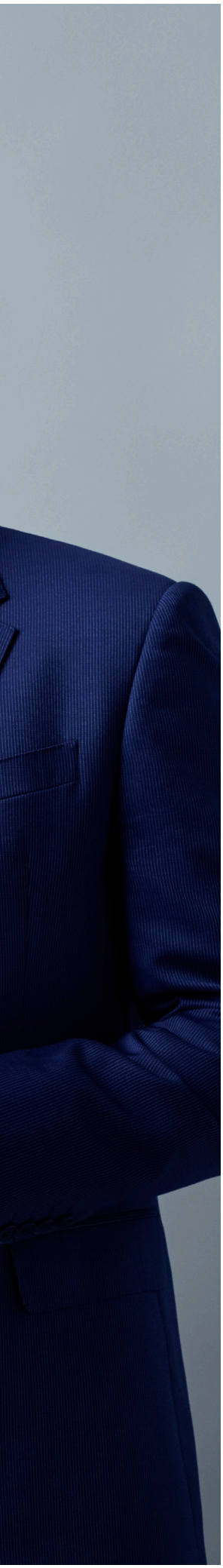
Kerri Constable
HR consultancy – Head of Centre of Excellence
M +44 (0)7823 531055
kerri.constable@rsmuk.com

Emma Griffiths
Managing Consultant, Technical Risk Advisory
M +44 (0)7528 970 287
emma.griffiths@rsmuk.com

rsmuk.com

THE APPRENTICESHIP LEVY

In 2015 the government introduced its plans to expand the National Apprenticeship Service through the introduction of the apprenticeship levy (levy). Although we expect the system will continue to evolve after its introduction in April 2017, the government has released further detail as to how it will work.



Basis of payment

The levy is to apply to employers in all sectors across the UK, with the amount payable being 0.5 per cent of their total pay bill, less an allowance. Pay bill, for purposes of the levy, is defined as the total amount of earnings payable by the employer subject to employer's class 1 National Insurance Contributions (NIC), including those earnings falling below the secondary NIC threshold. The allowance available to each stand-alone employer to set against the levy is an amount of up to £15,000 per annum. This means that only employers with a total annual pay bill in excess of £3m will ultimately bear a cost. Connected companies, however, will only have one allowance available to the group and they must decide how this is to be allocated.

Based upon earnings attracting employer's class 1 NIC, the levy will be applied to salary, commission, bonuses, employee pension contributions and non-tax advantaged share awards, but will not apply to earnings of international assignees where they stay within the social security system of their home country. Also, benefits that have traditionally been reported on forms P11D or in a Pay As You Earn (PAYE) settlement agreement will not be considered in the calculation as they attract NIC under Class 1A or Class 1B.

The levy will be collected by HMRC through the PAYE process and will be calculated on a monthly cumulative basis. Even after a deduction for corporation tax, this levy will be seen by many employers as an extra tax.

The government has recently confirmed that only employers with a wage bill of £3m will have to register for the levy. It had previously intimated that those with a wage bill of £2.8m would be required to register in case they exceeded the £3m threshold.

Planning for the levy

In preparation, employers need to make an early assessment of all earnings attracting an employer class 1 NIC liability, whilst planning for any anticipated growth before April, to know how the new levy will affect their business.

Companies may wish to give renewed consideration to their reward strategy in light of this new charge, for example, by considering:

- the timing of bonuses in the lead up to April 2017, which may mean they do not attract this additional 0.5 per cent payroll charge;
- providing equity rewards through tax advantaged share schemes, such as the Enterprise Management Incentive (EMI) scheme and Share Incentive Plan (SIP), which do not attract income tax and NIC;
- using benefits in kind that attract NIC charges under Class 1A or Class 1B and which currently do not attract employee NIC;
- where possible, choosing a means of remunerating business performance such as through dividends to shareholders of owner managed businesses, rather than paying directors' bonuses; and
- using salary sacrifice arrangements, where appropriate, to structure remuneration packages in a more tax and/or NIC efficient way. For example, salary sacrifice in favour of employer pension contributions brings savings in Class 1 NIC liabilities to both employees and employer.

In considering these options, it should be noted that arrangements put in place with the main purpose, or one of the main purposes, of obtaining an advantage in relation to the levy will be caught under anti-avoidance rules. Employers must also remain mindful of the government's recent decision to restrict the use of salary sacrifice arrangements. However, it has pledged not to challenge such arrangements in relation to employer supported child care, pensions and cycle to work schemes, so these options remain available as a means of providing tax efficient remuneration.

Using the levy as an opportunity

In England levy funds will be held in a apprenticeship service (AS) account which will be linked to their PAYE scheme. From 13 February 2017, the government has invited employers to register to create their individual AS account. Employers can utilise the funds held in these accounts to pay for apprenticeship training from approved training providers. All employers will receive a 10 per cent top up from the government to their AS account, so that an employer can recover more from the scheme than the payments they make through the levy.

A key issue for most employers is understanding how they can access what they pay in relation to the apprenticeship levy. Levy funds can only be used towards the cost of apprenticeship training with an approved training provider for new and existing staff. It cannot be used towards any unapproved training, or to fund the apprentice's salaries. The employer will negotiate the price for training with the provider. Each apprenticeship standard or framework will be placed into one of 15 bands, ranging from £1,500 to £27,000. These bands will determine the maximum amount that can be spent from the AS account on each apprenticeship. If the employer has agreed an amount higher than the cap they will need to pay any amount over the cap in full. The Department of Education has recently published the bands and these can be found at **https://www.gov.uk/government/publications/apprenticeship-levy-how-it-will-work**

Employers will access the levy funds in different ways depending on whether they are located in Scotland, Wales and Northern Ireland. Employers should review the devolved country's' education board's website for more details as these vary from country to country.

How long will employers have to spend their levy?

The government was originally intending to give employers 18 months to spend the levy; however this was increased and now levy funds will expire 24 months after they first enter the AS account unless spent on approved apprenticeship training. The account will work on a first-in, first-out basis. The AS account will be set up so that funds that enter the account at the earliest date will automatically be used first.

The levy will start to be collected based on April 2017 payroll and will be available for spend incurred from May.

Example

	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV
Levy allowance								
In month	£1,250	£1,250	£1,250	£1,250	£1,250	£1,250	£1,250	£1,250
Cumulative	£1,250	£2,500	£3,750	£5,000	£6,250	£7,500	£8,750	£10,000
Pay Bill	£320,000	£400,000	£370,000	£500,000	£420,000	£450,000	£480,000	£450,000
Cumulative	£320,000	£720,000	£1,090,000	£1,590,000	£2,010,000	£2,460,000	£2,940,000	£3,390,000
Levy @ 0.5%	£1,600	£2,000	£1,850	£2,500	£2,100	£2,250	£2,400	£2,250
Levy allowance	£1,250	£1,250	£1,250	£1,250	£1,250	£1,250	£1,250	£1,250
Levy payable	**£350**	**£750**	**£600**	**£1,250**	**£850**	**£1,000**	**£1,150**	**£1,000**
Cumulative	**£350**	**£1,100**	**£1,700**	**£2,950**	**£3,800**	**£4,800**	**£5,950**	**£6,950**

Many companies have a grow their own philosophy and recognise the benefits of training staff on the job, using external courses to fill the gap in technical skills whilst learning to apply these skills within the ethos of that company. The levy used in this way is even easier to stomach when considered in conjunction with the exemption from employer's NIC introduced in April 2016 for apprentices up to the age of 25.

DEC	JAN	FEB	MAR
£1,250	£1,250	£1,250	£1,250
£11,250	£12,500	£13,750	£15,000
£500,000	£460,000	£500,000	£480,000
£3,890,000	£4,350,000	£4,850,000	£5,330,000
£2,500	£2,300	£2,500	£2,400
£1,250	£1,250	£1,250	£1,250
£1,250	**£1,050**	**£1,250**	**£1,150**
£8,200	**£9,250**	**£10,500**	**£11,650**

Those employers willing to embrace the new levy would be well placed to start planning the process now to ensure maximum use. They may need to rethink their current recruitment and training policies offered to trainees. Where they do not fall within the government's requirement of a qualifying apprentice working towards an approved apprenticeship standard or within an approved apprenticeship framework, they should think about what changes can be made to their training programme to maximise use of funds in the AS account.

The term apprenticeship is legally protected and can only be used to describe a statutory apprenticeship as set out in the Enterprise Act 2016. Apprenticeship in this context means the training and (where applicable) end point assessment for an employee as part of a job with an accompanying skills development programme.

There are rules governing what an apprenticeship is, the main ones being:

- the apprentice must be employed in a real job whether existing or new;
- there should also still be a job at the end of the apprenticeship;
- the apprentice must work towards achieving an approved apprenticeship standard or framework;
- the cost of the apprentice's wages must be met by the employer;
- the job role must provide the opportunity to gain the knowledge, skills and behaviours needed to achieve the apprenticeship;
- the apprenticeship training (not just the employment period) must last at least 12 months;
- the apprentice must spend at least 20 per cent of their time on off-the-job training; and
- the individual must be eligible under the funding rules.

The National Apprenticeship Service provides more detail on how to employ an apprentice at **https://www.gov.uk/take-on-an-apprentice**.

Grouped companies should consider in advance where they will best utilise their levy funds and can register their different PAYE schemes to pool the levy into a single AS account to maximise opportunities for use.

Training providers are generally staying well-tuned to the new apprenticeship levy and listening to the needs of employers to develop training programmes that fit the needs of the job and fall within the scheme parameters.

HOW CAN EMPLOYERS SPEND THE LEVY

Apprenticeship service accounts

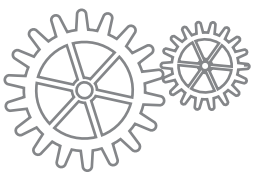
Can the levy be used for pre-May 2017 registrants?
The government has recently stated that any apprentices who started their apprenticeship pre-May 2017 will be funded for the full duration of their apprenticeship under the terms that were in place at the commencement of the apprenticeship. Therefore employers will not be able to utilise funds in their AS account funds to cover these apprentices.

For post May 2017 starters, if an employer pays the levy but AS account funds do not cover the full cost of the apprenticeship training, additional government support will be provided to help the employer meet the additional costs, up to the maximum amount of funding available for that apprenticeship. Employers will also be expected to make additional contributions for the extra amount they wish to spend. The contribution by the government will be 90 per cent and employers will contribute an extra 10 per cent.

Employers will also be given a £1,000 incentive for employing a 16-18 year old apprentice, which also applies to 19-24 year old care givers or young adults with additional learning needs. The £1,000 will be paid in two instalments in months three and 12 of the apprenticeship.

How will payments be made to the training provider?
When an employer agrees to buy apprenticeship training from a provider, monthly payments will be automatically taken from the AS account and sent to the provider. This spreads the cost over the lifetime of the apprenticeship. Employers will not need to have sufficient funds in the AS account to cover the entire cost of the training at the start. As payments are taken from the AS account monthly, employers will need to have sufficient funds in the account to cover the monthly cost of each apprenticeship chosen. The Department for Education will make sure the payments reach the provider.

Employers should note that not all AS account funds will be taken out on a monthly basis; 20 per cent of the cost of the apprenticeship will be retained and taken from the AS account at the end of the apprenticeship. The government believes that employers will increasingly move to training apprentices to approved apprenticeship standards, where there is an end point assessment. The price negotiated with the training provider at the beginning of the apprenticeship should include payment for the end point assessment.



Employer responsibilities
The employer will need to have an employer agreement with the Secretary of State for Education acting through the Skills Funding Agency. This will bind the employer into the funding rules. The employer will also need to have an apprenticeship agreement with the apprentice at the start of and throughout their apprenticeship.

The employer, provider and apprentice all need to sign a commitment statement setting out how they will support the successful achievement of the apprenticeship. There will also be a written agreement with the main provider.

There are certain evidence requirements with which the employer will need to comply.

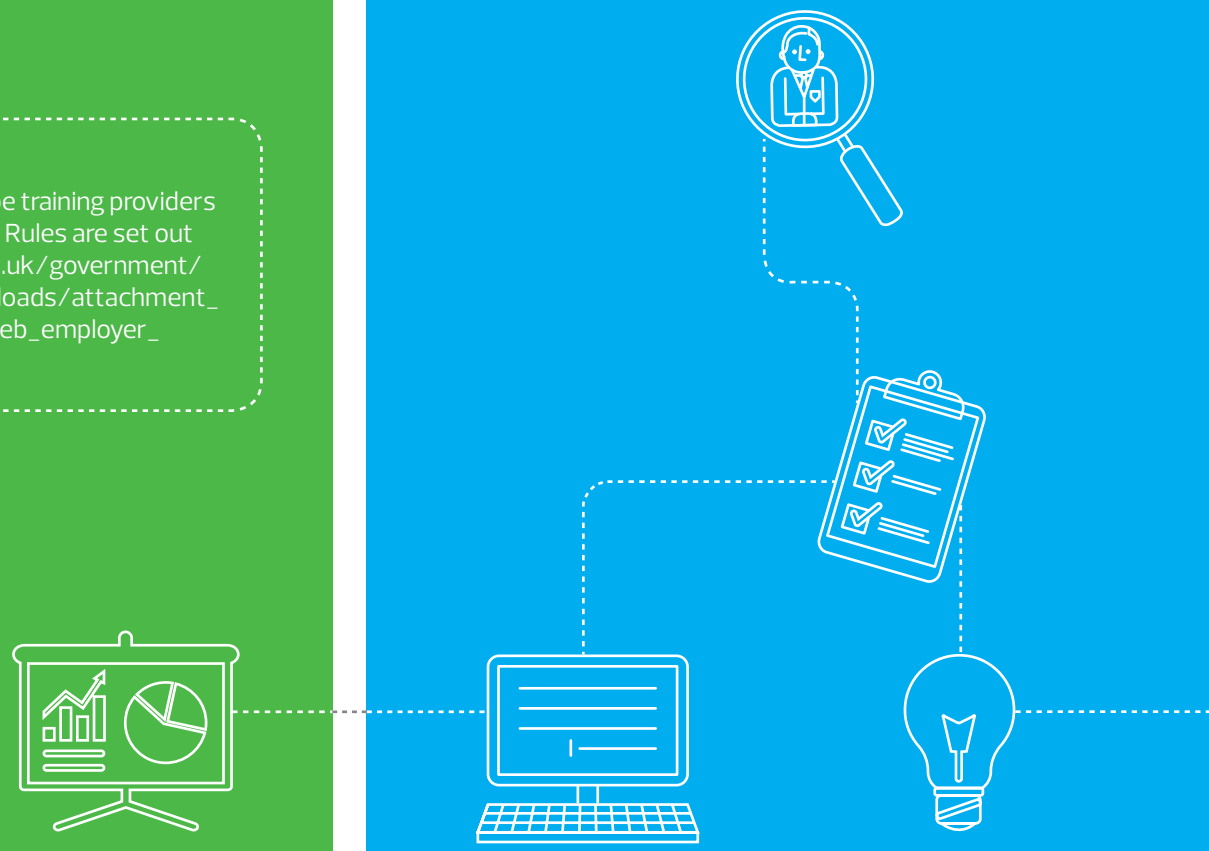
In some cases the apprentice will be required to undertake further maths and English training. This is funded separately (not from the levy funds) and the employer must allow time for study.

Employer providers
Employers can also be training providers for their apprentices. Rules are set out at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/590269/Feb_employer_provider_guide.pdf

Non-levy paying employers
The new funding system will be implemented on 1st May 2017. Once this comes into effect, the proposal is that employers will pay 10 per cent of the cost of the apprenticeship and the government will pay 90 per cent. The maximum cost will depend upon which one of the 15 bands the apprenticeship falls into. Employers in these circumstances will also be able to negotiate the price of the apprenticeship with the training provider.

Where employers have fewer than 50 members of staff and also employ 16–18 year old apprentices, the employer contribution will be waived so the cost of training such young persons will be free.

Employers that do not pay the levy will be able to look for training options and search for a provider using the tools on the apprenticeship service. However, such employers will not need to use the apprenticeship service to pay for apprenticeship training and assessment until at least 2018. Prior to this they will be required to pay their provider on agreed payment terms.



If you would like more information on the apprenticeship levy then please contact your usual RSM advisor or:

Graham Farquhar
Partner, Employment Tax
T +44(0)118 953 0417
graham.farquhar@rsmuk.com

Jackie Hall
Partner, Tax
T +44(0)1482 607200
jackie.hall@rsmuk.com

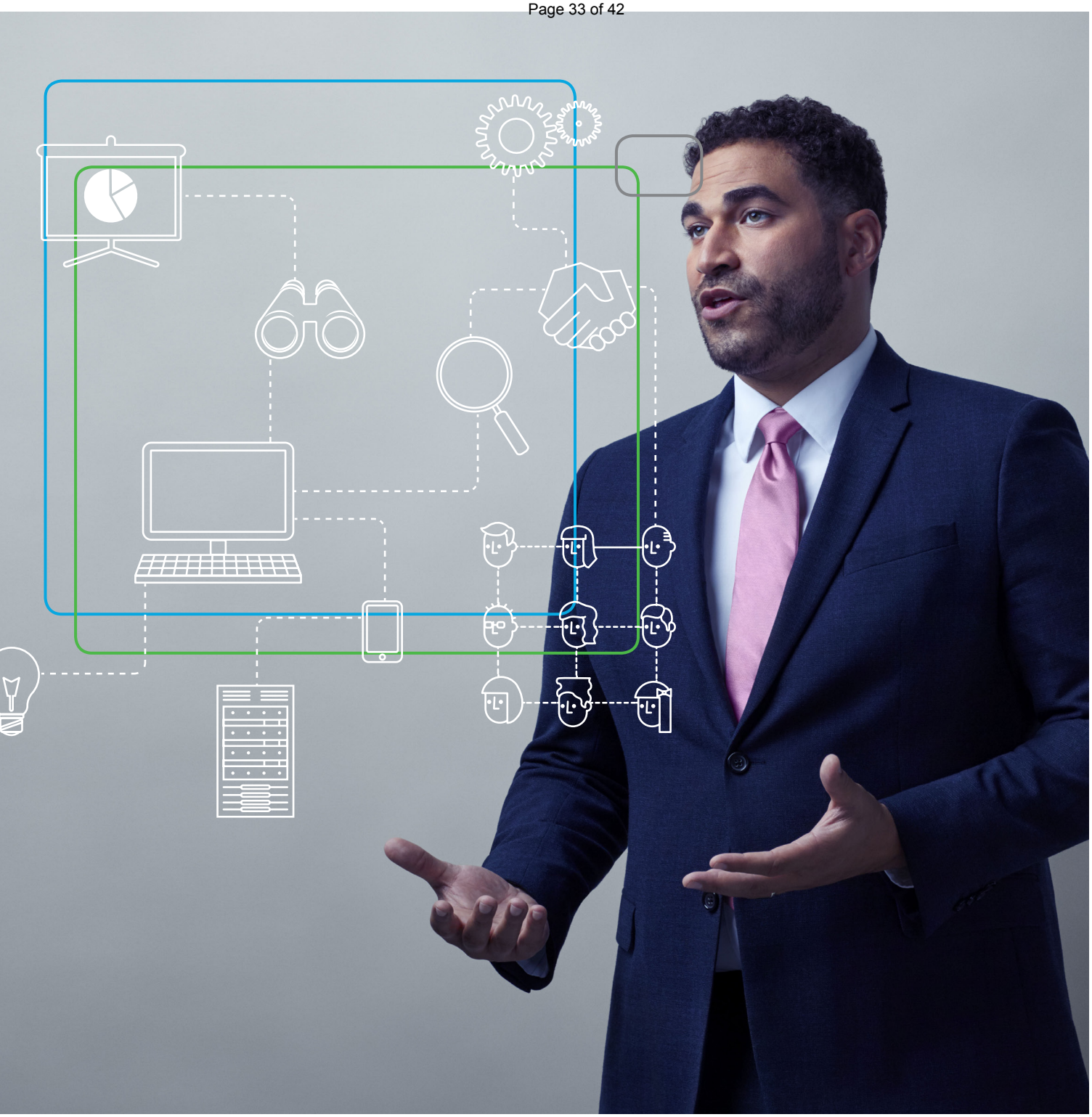
Lee Knight
Associate Director
T +44(0)20 3201 8508
lee.knight@rsmuk.com

Bill Longe
Partner, Head of Employer Solutions
T +44(0)121 214 3100
bill.longe@rsmuk.com

Stephanie Mason
Head of Further Education and Skills
T +44(0)121 214 3263
stephanie.mason@rsmuk.com

David Williams-Richardson
Partner, Tax
T +44(0)845 057 0700
david.williams-richardson@rsmuk.com

rsmuk.com

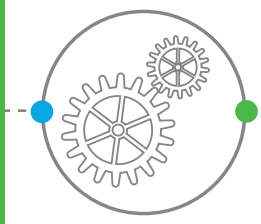


HOW VULNERABLE IS YOUR ORGANISATION TO CYBER ATTACKS?

Confidence through our cyber assurance services

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

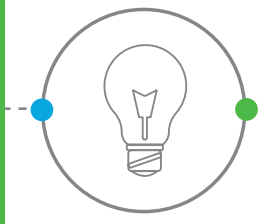


We have benefited from the use of ethical phishing in that we were given insight into the behaviours of individuals within our organisation and have been able to use this to educate our staff further in the identification and management of suspicious e-mails. We will be repeating this exercise now periodically in order to give us assurance that staff are listening to the advice and behaviours have changed.

Deputy Chief Information Officer, large health trust

Having read numerous news articles recently about the increasing number of cyber-attacks on organisations similar to ours, we discussed with RSM about delivering a cyber-security audit that they were already undertaking for our organisation. From scope, planning, execution and reporting, RSM's approach was straightforward yet comprehensive. The results from the exercise clearly proved that we needed to do more – further, they pointed us in the right direction in order to address the issues. Cyber-security needn't be complex, especially when you've got RSM providing you with expert assurance.

Head of ICT, large housing group



RSM demonstrated the necessary cyber security expertise and professional maturity to simulate a phishing attack on our Group as part of a wider cyber security review. The exercise enabled a full independent assessment to be performed of the quality of both our IT security control and procedures to prevent such an attack, and the responsiveness of management in reacting to such an incident.

Group Head of Audit, private company

HAVE YOU CONSIDERED THE IMPACT THAT A CYBER ATTACK COULD HAVE ON YOUR ORGANISATION?

Malicious hacking, identity theft and high profile cyber disruption have become common occurrences in today's business environment. The impact of attacks can vary in severity but most common is a disruption to every day operations and reputational damage that is very difficult to recover and rebuild.

Despite a better awareness of the risks, many firms not only have inadequate defences but also are yet to assess how such an attack would impact their operations.

Weaknesses of any degree across your infrastructure, suppliers and third party providers can expose the whole business. It is critical that you take steps before those vulnerabilities are exploited.

Technology related risks are rarely isolated to one area. As such, our approach to tackling risk is to assess the exposure across your whole organisation.

Internal vulnerability testing

This explores the integrity of your server environment and is often performed in advance of planned external reviews. We check the security of your environment and compare it to accepted good practice.

External penetration testing

Can hackers access your system? What can they do once they're in your system? Our external testing process emulates the hacking process by using commercial and public domain tools to identify network vulnerabilities so you can take steps to correct them.

Ethical Phishing

We can test your training effectiveness by simulating a phishing or whaling campaign. This illustrates an organisation's vulnerability to such attack and provides structured, on the spot user awareness training.

Cyber Assessments

We will perform a formal cyber security risk assessment and gap analysis across your organisation. This requires the completion of a detailed set of questions that map where your strengths and weaknesses currently lie. We will compare your scores against the UK government's 10 Steps to Cyber Security model which was developed by the CESG and business groups.

Training Services

We can deliver specific training course designed to inform both IT and non-IT staff of current cyber security risks and the good practice needed to address them.

For further information contact

Steve Snaith
Partner

T +44 (0)79 6603 9009
steven.snaith@rsmuk.com

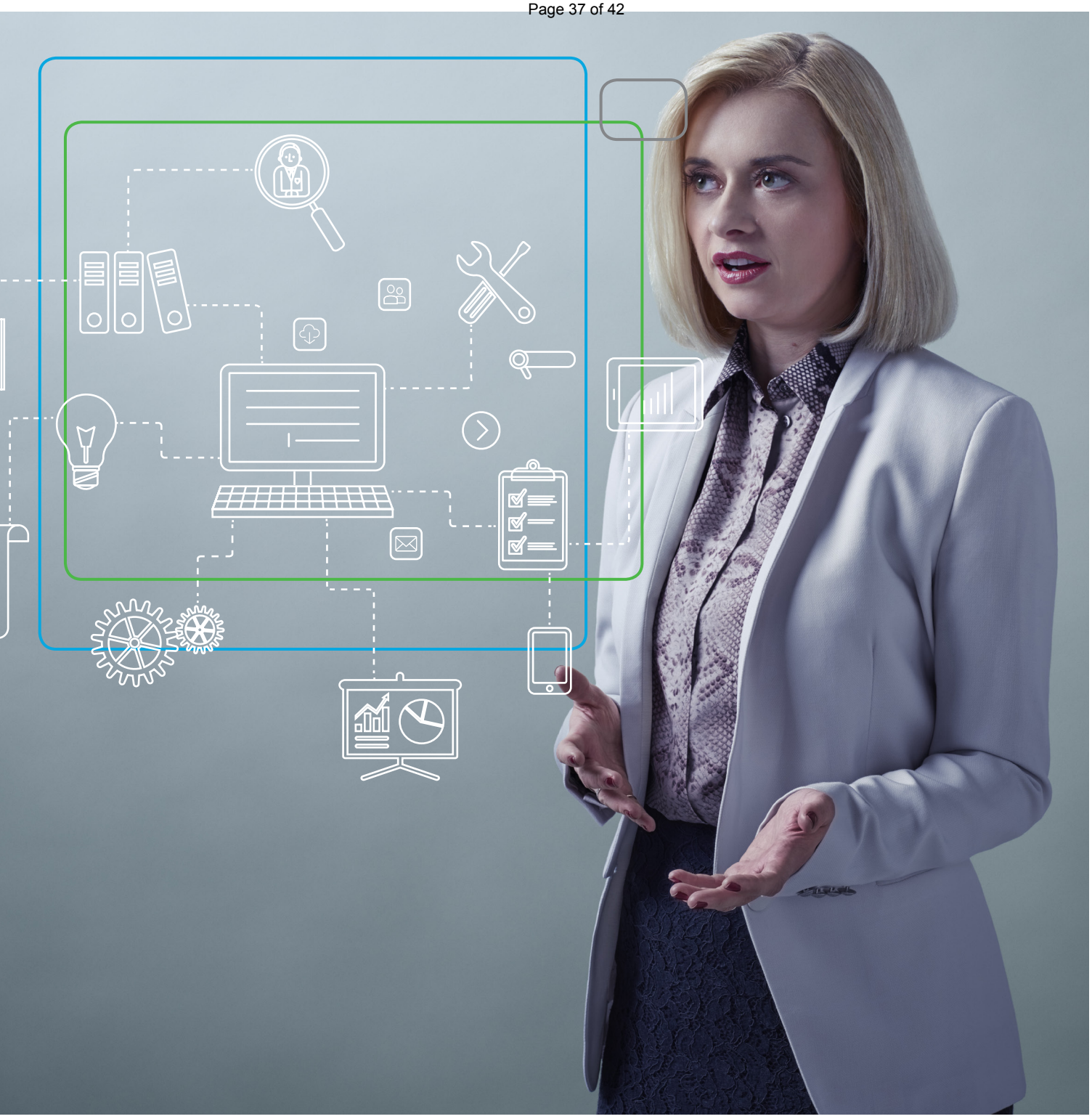
Sheila Pancholi
Partner

T +44 (0)78 1136 1638
sheila.pancholi@rsmuk.com

David Morris
Director

T +44 (0)78 00617128
david.morris@rsmuk.com

rsmuk.com



ARE YOU VULNERABLE TO EMAIL SCAMMING?

The growing threat of phishing and whaling
2017

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

HOW VULNERABLE ARE YOU?

Across all sectors we can see security breaches and data loss destroying reputations and causing tangible loss of profit and turnover. We are seeing new threats continue to target organisations at their most vulnerable – their staff and third parties.

The practice of phishing and whaling is no different and means sending emails claiming to be from reputable organisations to encourage individuals and companies to reveal valuable personal or corporate information.

HOW DO CYBERCRIMINALS ATTACK?

Insider attacks

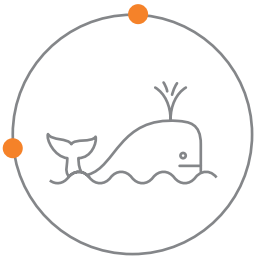
Employees download sensitive or confidential data and sell it on.

Phishing activity

Multiple individuals are targeted by a single scam. Typically, a blanket email is sent in the hope that some will reply with sensitive information, transfer funds or open rogue links or attachments.

Ransomware attacks

A hacker gains access to a system and takes it over. It holds the organisation to ransom by blocking system access until a substantial payment is made.



Whaling attacks

A small group of individuals with significant data access are targeted. Typically, a hacker poses as a senior official and requests personal information, bank detail changes or a large funds transfer.

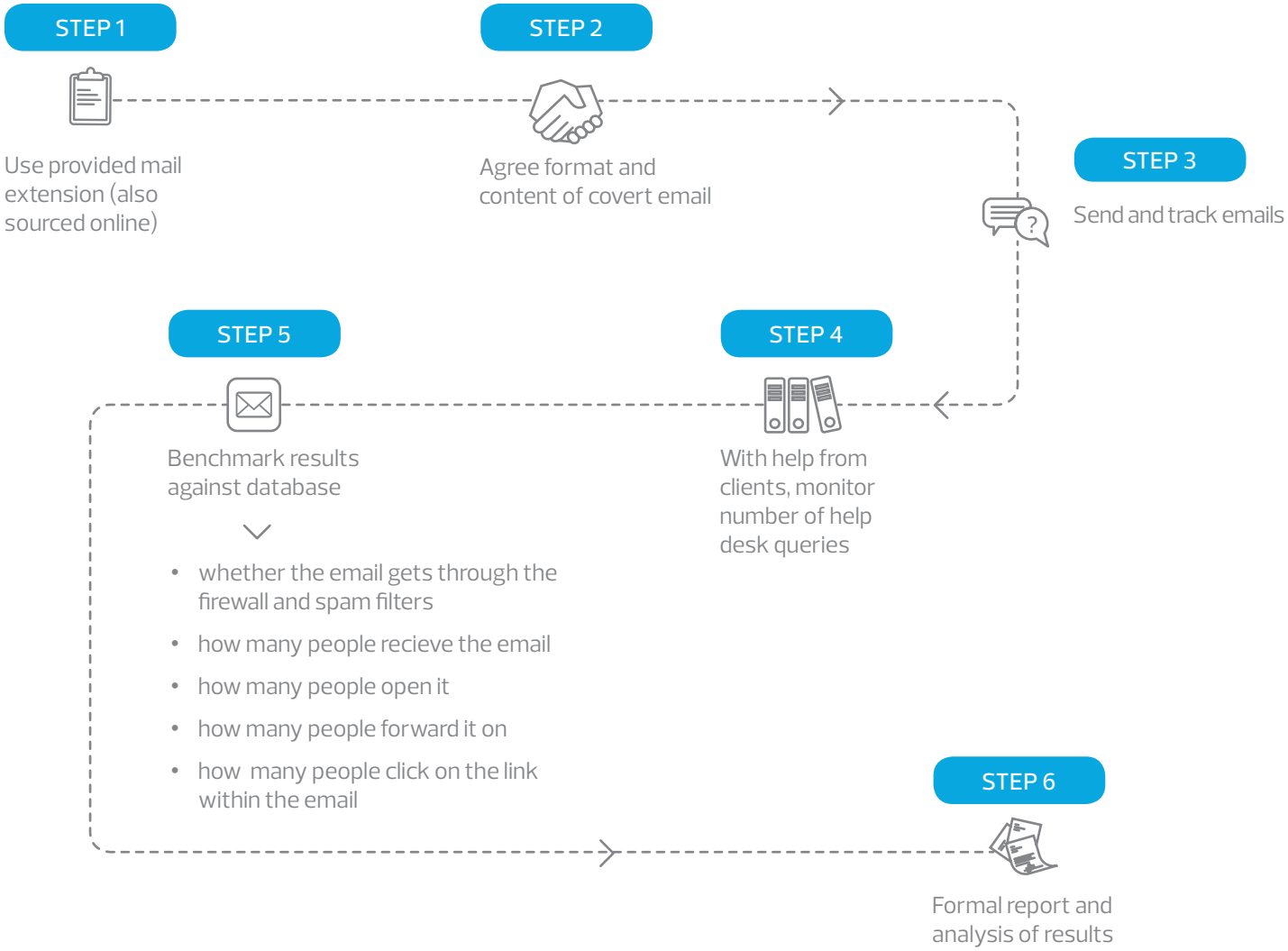
What can you do to address this threat?

Typically, a company will implement technical controls that use firewalls and gateways to identify and filter out spoof, spam and infected emails. However, these will not catch every threat and some emails do make it through. Consequently focus should shift from technical controls, to training and education. It is critical they be trained on their responsibility for keeping information and data secure and how to respond.

What risk factors should concern you?

- recent frauds or losses through cybercrime;
- a history of issues with viruses and malware;
- a large non-technical workforce;
- reliance upon remote working practices;
- reliance upon on-line business activities; and
- limited training on the topic.

How would we help through simulated phishing?



- Illustrates an organisation's vulnerability to such an attack, showing what percentage of their employee base is likely to fall victim;
- Provides structured, on the spot user awareness training where employees learn the importance of keeping the organisation safe and secure in future; and
- Provides an agreed base-line that future training can be measured against.

For further information contact:

Steve Snaith
Partner

T +44 (0)79 6603 9009
steven.snaith@rsmuk.com

Sheila Pancholi
Partner

T +44 (0)78 1136 1638
sheila.pancholi@rsmuk.com

David Morris
Director

T +44 (0)78 00617128
david.morris@rsmuk.com

rsmuk.com

IS YOUR BUSINESS GDPR READY?

The General Data Protection Regulation (GDPR) will come into force in the UK on 25 May 2018 after four years of negotiations and unprecedented levels of lobbying by businesses.

These new rules will cause significant disruption to how organisations store, manage and process personal data, with significant penalties for those who don't comply.

This will impact all businesses but especially those in the consumer sector where data has become such a large part of customer loyalty, marketing and delivery.

What is the GDPR?

The new legal framework is the biggest change to data privacy legislation in over 20 years. Digital advancements over this time have meant that consumer data is created, collected and stored within seconds. It is more important now, than ever, to have clear laws and safeguards in place given the growing digital economy and associated cyber security risk.

Does Brexit impact GDPR?

The GDPR aims to protect EU citizens' personal data, regardless of borders or where the data is processed. The new rules are much broader than the 1995 Data Protection Act with a more expansive definition of personal identifiers, such as an IP address, which is now classified as personal data. Businesses based outside the EU will still need to be compliant if they have EU customers. As such the UK's decision to leave the EU will not affect the need to comply with GDPR.

What are the penalties?

The penalties are significant, fines for non-compliance of up to €20m or 4 per cent of annual global turnover could be imposed.

How does this affect my business?

Any company who processes consumers' personal data will need to comply with the new obligations. That means firstly understanding the changes to the existing processes under the new rules:

Consent – do you have explicit consent from individuals for the data you hold about them?

Under the new rules the requirements have been tightened significantly. Requesting consent from a consumer to process their personal data must be 'unambiguous'.

New responsibilities – are you a data processor or data controller responsible for processing personal data?

Under the GDPR, data processors will have greater legal liability and are required to maintain records of personal data and processing activities. There are also further obligations on controllers to ensure that any third-party contractors also comply with the GDPR eg cloud hosting or outsourcing.

Accountability – do you have a data protection programme and are you able to provide evidence of how you will comply with the requirements of the GDPR?

Organisational and technical measures to protect personal data are now the responsibility of the data controller and data processor – data protection and privacy requirements should be built into the development of your business processes and systems.

Mandatory breach notification – would you be able to notify a data protection supervisory authority of a data breach within 72 hours?

You will need internal processes that allow you to report and manage communications with affected consumers quickly and accurately.

New rights – do you know how you will comply with the new rights; the 'right to be forgotten', the 'right to data portability', and the 'right to object to data profiling'?

You will need processes in place to comply and reassure that these rights have been adhered to (including notifying third-parties).

Data protection officers – do you conduct large scale systematic monitoring (including employee data) or process large amounts of sensitive personal data?

Where 'large scale' processing of data is evident a dedicated Data Protection Officer needs to be appointed.

How we can help

Our specialists can help you to ensure compliance in the first instance, and provide the evidence to prove it in the second. Through robust analysis we will identify any risks and implement processes and systems to ensure compliance:

- GDPR gap analysis
- Privacy Impact Assessment
- GDPR awareness sessions
- Breach management processes
- Security monitoring and reporting

Please contact one of the team below for further information:

Sheila Pancholi
Partner
sheila.pancholi@rsmuk.com

Steve Snaith
Partner
steve.snaith@rsmuk.com

David Morris
Director
david.morris@rsmuk.com

rsmuk.com