EPSOM AND EWELL BOROUGH COUNCIL

Internal Audit Progress Report

Audit, Crime & Disorder and Scrutiny Committee Meeting

11 April 2017

RSM

CONTENTS

1 INTRODUCTION

The Internal Audit Plan for 2016/17 was approved by the Audit, Crime & Disorder Scrutiny Committee in April 2016.

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

2 FINDINGS CONSIDERED AT THIS AUDIT, CRIME & DISORDER AND SCRUTINY COMMITTEE

This table informs of the audit assignments that have been finalised and the impacts of those findings since our last report to the Audit, Crime & Disorder and Scrutiny Committee.

The Executive Summary and Key Findings of the assignments below are attached to this progress report at Appendix B.

Assignment	Assurance	Management Actions Agreed		
		High	Medium	Low
Barrier Controlled Parking Project – Post Implementation Review (12.16/17)	Advisory – no assurance opinion	-	1	2
PCI Code Of Conduct Compliance (13.16/17)	Partial	2	1	1
Financial Management and Main Accounting (14.16/17)	Reasonable	-	1	1

2.1 Client Briefings

We have issued the following briefing which is appended to the bottom of this report:

- Gender Pay Gap Reporting;

- Apprenticeship Levy;

- How Vulnerable is your Organisation to Cyber Attacks; and

- Are you Vulnerable to Email Scamming.

3 LOOKING AHEAD

Assignment area	Timing per approved IA plan 2016/17	Status
Payroll (11.16/17)	November 2016	Issued in draft 27 January 2017
Allocations, Lettings and Voids (15.16/17)	October 2016	Draft issued 22 March 2017
Commercial Rental Income (16.16/17)	February 2017	Draft issued 27 March 2017
Procurement Of Agency Staff	February 2017	Fieldwork in progress.
Data quality	December 2016	Fieldwork taking place in March 2017
Council Tax (Revenues)	January 2017	Management requested that the audit be rescheduled to April 2017
Benefits	January 2017	Management requested that the audit be rescheduled to May 2017
Implementation of Business Performance Review actions – Homelessness	February 2017	Fieldwork underway
Procurement	March 2017	Fieldwork planned for March 2017
Private Sector Leasing Scheme	March 2017	Deferred to 2017/18

4 OTHER MATTERS

4.1 Changes to the audit plan

Other than some timing changes, there are no changes to the plan proposed at this time.

4.2 Added value work

Our contract risk specialist undertook the review of the Facilities Management contract (1.16/17) which was at the request of management.

APPENDIX A: INTERNAL AUDIT ASSIGNMENTS COMPLETED TO DATE

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

Assignment	Assurance	Management Actions Agreed		
		High	Medium	Low
Facilities Management Contract Review (1.16/17)	Advisory review	Advisory findings only		
Cash Handling (2.16/17)	Reasonable assurance	-	1	2
Data Quality (15/16) (3.16/17)	Reasonable assurance	-	1	2
Housing Rent Accounting and Reconciliation (4.16/17)	Partial assurance	-	3	3
Workforce Planning (5.16/17)	Advisory review	Advisory findings only		
Implementation of Business Performance Review actions – Democratic Services (6.16/17)	Reasonable assurance	-	1	2
Grant audits	Complete – no report required			
Building and Planning Control (7.16/17)	Reasonable	-	1	4
Corporate Governance (8.16/17)	Substantial	-	-	-
Risk Management (9.16/17)	Reasonable	-	1	2
Creditors And Ordering (10.16/17)	Substantial	-	-	1

APPENDIX B: EXECUTIVE SUMMARIES

Assignment: Barrier Controlled Parking Project – Post Implementation Review (12.16/17)	**Opinion:**	**Advisory**

The key findings from this review are as follows:

- The capital spend on the installation of the barrier systems at the four car parks completed, of the six planned, was £119k higher than the budgets agreed in the business cases. The budget was also intended to cover the conversion of the Depot Road and Upper High Street car parks which were delayed pending development decisions and subsequently decided against as they were not expected to achieve savings. There are insufficient records available prior to the handover of the schemes to the Head of Customer Services in April 2015 to allow reasons for the overspend to be identified. Additional work was identified after the handover as required to make the Town Hall and Hope Lodge conversions operational. This added £48k to the cost of these.

- The papers presented to the Environment Committee setting out the business cases for the barrier system installations had not been reviewed and approved by the Chief Finance Officer or the Monitoring Officer. They were not therefore independently reviewed to ensure they were based on sound financial evidence and there were no legal issues.

- The business cases lacked detail on the work and equipment required and how these were costed. No Project Implementation Document has been identified. This would have defined the project in terms of its elements and stages and allowed clear comparison between what was planned and what was delivered. The project management templates developed in 2016 provide templates for business cases and project initiation documents which require clearer detail of what is to be delivered and the budget for it.

- The savings proposed in the business case for the Ashley Centre and Hook Road car parks were not achieved. In terms of the items where savings were identified in the business case, Ashley Road achieved a saving of £33k in the first year as opposed to £125k expected savings. Hook Road did not achieve any savings in the first year. The business case proposed £18k savings.

- The business case for the conversion of the Town Hall and Hope Lodge car parks stated that there was less scope for savings from these car parks. It projected savings of £8k. As a full financial year of actual figures are not yet available for these conversions in December 2015, a comparison with the budgets for 2016/17 indicates the saving is expected to be £9.5k in the first full year.

- Parking fee income has increased over the last six years at all four of the car parks where the new barrier equipment was installed. There is no clear trend of increase following conversion. The non-financial benefits of barrier system inherent in this approach were achieved: newer machines can give change, smarter permit cards are in use, the system prevents cars entering a full car park. There has been no survey of user experience to establish if users prefer the system.

- The business case for the conversion of the Town Hall and Hope Lodge car parks included a reduction of one Civil Enforcement Officer. This was the expected reduction in enforcement time from no longer needing to check pay and display tickets. However some parking enforcement is still required at barrier system car parks to ensure parking bays and disabled bays are used correctly.

- The number of Civil Enforcement Officers has fallen since 2014/15 but only half a Full Time Equivalent is regarded by management as due to the reduced workload of the barrier system car parks. There were long delays in the delivery of the conversions compared to the original target date. The first car parks became operational six and 10 months after the target date, in April 2012 and August 2012. The second phase became operational 20 months later than planned, in December 2015. The records before the handover of the projects were insufficient to allow identification of reasons for these delays.

- Additional installations were identified as required in the course of the projects, both by the former Director of Operations and by the Head of Customer Services. The lack of detail in the business cases and the lack of project documentation mean it is not possible to compare what was originally planned to what was subsequently required.

- Handover of the project by the former Director of Operations was by a verbal talk through on his last day of service. This did not allow any further questions to be asked. There was little documentation to be taken over and so no structured project records. Knowledge of the project was held by one officer making the Council vulnerable to the loss of this officer.

- Although the Council has not formally considered and recorded the lessons from this project, the new project management templates developed in 2016 address the project management failures identified above. They provide for Project Initiation Documents, structured milestones, project oversight, shared knowledge of the project and a Post Implementation Review. Importantly there is now greater visibility of all projects in operation through a central record of projects as well as consideration of their progress by the Strategic Leadership Team. In addition the equipment and infrastructure needs of installing a barrier system have been captured in a draft Post Implementation Review which management has agreed to formalise.

	Agreed Management Action	Implementation Date	Manager Responsible
1	The Head of Governance will ensure that committee processes ensure committee papers that have not been reviewed by the Chief Finance Officer and the Monitoring Officer will be identified and no decision based on them acted on until these reviews have taken place.	30 September 2017	Gillian McTaggart
2	The Post Implementation Review of the Town Hall and Hope Lodge Car Parks will be finalised, reported and made part of the formal documentation of car parking arrangements.	30 September 2017	Joy Stevens
3	Project management templates will be revised to include: identification of opportunities as well as risks.	30 September 2017	Gillian McTaggart

Assignment: PCI Compliance (13.16/17)	Opinion:	Partial

The Council has provided five ways that members of the public can use debit/credit cards to make payments for services:

- By using an automated telephone system;
- Via the Council website;
- Via a car parking payment point;
- By direct contact with a member of staff authorised to use a chip and pin machine; and
- By direct contact with any member of staff who is authorised to take card payments via the telephone.

Also able to take card payments for seats is the Council's Playhouse theatre.

The Council is required to comply with the PCI DSS in order to permit it to take payments by card. The PCI DSS is a proprietary information security standard for organisations that use credit cards from the major card schemes (Visa, Mastercard, American Express, Discover and JCB).

The standard was created to increase controls around cardholder data to reduce credit card fraud. The standard is mandated by the major card brands and administered by the Payment Card Industry Security Standards Council.

The Council has to complete a Self-Assessment Questionnaire (SAQ) annually in order to substantiate its compliance with PCI DSS. The most recent version of the PCI standard (version 3.1) came into effect on 1 July 2015.

The Council has negotiated contracts with third parties for card handling services; Adelante provide card payment software and World Pay provides Acquiring services.

The key findings from this review are as follows:

a) Although the Council has not achieved PCI compliance, the network scans run by Worldpay have confirmed that the network configuration does not present any vulnerabilities, having been passed as compliant for the year to April 23 2017.

b) A PowerPoint presentation has been produced covering the correct handling of card payments and the use of chip and pin machines across the Council landscape.

c) A PCI policy has been documented by the Council. The policy identifies roles and responsibilities of Council officers and staff for PCI compliance. The policy provides hyperlinks to the PCI training material. This reduces the risk of staff breaching PCI as a result of not knowing their responsibilities

d) The PCI policy document at Appendix A contains details of the scope of PCI within the Council. It also identifies that the Council completes PCI compliance self-assessment questionnaire D (SAQD). This reduces the risk of PCI breach due to areas being missed during annual reviews.

e) A PCI data flow diagram has been documented by the Council. It is dated 15/08/2016 and identifies the flows across the network of PCI data for the various payment methods. This reduces the risk of a lack of oversight of the PCI environment and increases security awareness of PCI.

f) An Excel spreadsheet has been designed to enable the PCI status of third parties to be recorded and tracked. The spreadsheet also identifies the process followed to process the card payment at each processing location.

g) Overall responsibility for PCI compliance is with The Director of Finance and Resources. This is delegated to two Heads of Service within this directorate – Head of Financial Services and Head of ICT. Staff within these two divisions carry out reviews of processes and training according to the policy. The Head of ICT and Head of Financial Services co-ordinate compliance and any significant changes with the support of other Head of Service. The PCI policy document is dated October 2016. This reduces the risk that staff are not aware what needs to be done to achieve and maintain PCI compliance.

We identified the following areas for improvement which management have agreed actions to address:

h) The Council has not completed the self-assessment questionnaire D for achieving PCI DSS compliance. This increases the risk of breach and possibility of the Council being charged non-compliance fees by the Bank.

i) The voice recording system used by the Council to record incoming calls to Customer Services has been upgraded to comply with PCI requirements. It must automatically stop recording when payment card details are being provided by a customer. However the system is not working when coupled to CRM, increasing the risk that customer payment card details could be retained on Council systems, resulting in breach of PCI regulations.

j) The Council is failing to ensure that the third party organisations that it deals with to facilitate card payments are themselves PCI compliant. This increases the risk of the Council failing to comply with PCI requirements.

	Agreed Management Action	Implementation Date	Manager Responsible
1	The Council is not PCI compliant as it has not yet completed the self-assessment questionnaire. We were informed that it has completed approximately 50% of the questions. There is a risk that it could be charged non-compliance fees by the Bank until it is compliant. The Council will ensure that the questionnaire is completed as soon as possible. (High)	31 March 2017	Paul Wilcox, Business Systems Application Manager
2	The Council is not able to demonstrate that all appropriate staff have received training as it does not maintain a record of the people attending the training. An attendance record of staff receiving the PCI training will be retained. (Low)	1 March 2017	Paul Wilcox, Business Systems Application Manager and Chris Morgan, Senior Accountant
3	To comply with PCI requirements the Council has to ensure that its third party providers are PCI compliant, however the Council has failed to ensure this by holding copies of their current certificates. The Council will ensure that it confirms the PCI status of all third party organisations used by the Council to facilitate card transactions. (Medium)	June 2017	Chris Morgan, Senior Accountant

4	Although the Council's call recording system has been upgraded and is PCI compliant it fails to be compliant when connected to the CRM system, risking the Council holding customer credit card details in breach of PCI requirements. The Council will until the voice recording system can be fully PCI compliant halt the recording of calls via CRM. (High)	31 March 2017	Joy Stevens, Customer Services Manager

Assignment: Financial Management and Main Accounting (14.16/17)	**Opinion:**	**Reasonable**

Savings plans were identified as part of the budget setting process. Service Heads at the Council are responsible for devising savings plans. Savings plans are incorporated into service level budgets and monitored by Service Heads themselves as well as an appointed Senior Accountant on a quarterly basis.

With a number of external cost pressures including reductions in support from the Government as well as increased expenditure in relation to dealing with homelessness in the Borough, achievement of savings plans is of key importance to the Council. As part the Council's Medium Term Financial Strategy a target reduction of £3.1 million in net expenditure is planned to be achieved by 31 March 2020.

The key findings from this review are as follows:

Well-Designed Controls Being Applied Effectively:

a) Manual journals are completed in an electronic form. These are printed and signed by the completing officer and reviewed and signed. Narrative and audit trail of input and authorisation are maintained within the system. We found that for a sample 10 manual journals authorised that segregation of duty was in place and supporting narrative was evidenced.

b) On an individual leaving the organisation as part of the 'leavers' process' their access to IT systems at the Council are removed. We were provided with a current list of Civica users and found that all were current employees at the Council. In addition we found their access rights were appropriate for their role.

c) Bank Reconciliations are undertaken on a daily basis by the Exchequer Services Team Leader, reviewed weekly by the Senior Accountant and monthly by the Head of Financial Services. We found that for a sample of 15 bank reconciliations that all had been subject to daily review by the Exchequer Services Team Leader and where appropriate the Senior Accountant and Head of Financial Services.

d) There are two active suspense codes payroll and the GL interface. The Finance team are provided with a daily notification of all items that have been posted to the suspense account. These will be cleared by the Finance Officer and signed off by the Senior Accountant. We found that both suspense accounts were subject to monthly review by the Senior Accountant. Where balances existed at month end explanations were sought and provided.

e) The Finance Team electronically reconcile the cash receipting system within the General Ledger to Council Tax and NNDR on a weekly basis. Finance maintains a spreadsheet that highlights General Ledger balances to date as well as those of NNDR and Council Tax. Variances between the two systems were explained with the majority of differences put down to timing differences.

f) Payroll to General Ledger reconciliations were satisfactorily reviewed as part of the payroll 2016/17 audit. Creditor to general ledger reconciliations were reviewed as part of our Accounts Payable 2016/17 audit.

g) The Council has a Financial Plan 2016-2020 which outlines the Medium Term Financial Strategy (MTFS). The plan outlines the current economic environment as well as the Council's target of reducing net expenditure by £3.1 m by March 2020. We found that the MTFSprovided a sufficient framework for guiding the Council's saving plans over the medium term.

h) Savings plans are incorporated into annual budgets and subsequently the Council's overall budget which is preliminarily reviewed by the Financial Planning Policy Group, then subsequently finally approved by the Council in February of each year. We found that the annual budget for this year had been approved by the Council on 11th February 2016. We found that approved savings plans were complete with a robust set of financial analysis to support the plan.

Areas where control design and application may be improved:

i) There is no corporate guidance in place to assist staff in drafting savings plans. Service savings plans therefore differ in the level of detail provided. Going forward there is scope for more consistent breadth of narrative and context particularly with regards to impact assessments being carried out and the risks associated with implementing the savings plans proposed. Officers have agreed an action going forward to address these issues.

j) Savings plans are incorporated into each service areas individual budget. Budget holders meet with a Senior Accountant on a quarterly basis to monitor their financial performance against the budgeted savings plans. We were provided with evidence that Q1 budget monitoring took place as per the control. Variances were investigated as well any spend anomalies. In addition monthly budget reports were sent to Management. However over the course of a few months four staff members left the Finance Team . As a result staff resources within the department have been stretched and formal evidence of Q2 and Q3 monitoring was limited. There is a risk that if formal consistent monitoring of budgets is not taking place the Council are not tracking the achievement of saving plans effectively.

	Agreed Management Action	Implementation Date	Manager Responsible
1	Over the course of a few months four staff members left the Finance team at the Council. As a result resources within the department have been stretched and formal evidence of Q2 and Q3 monitoring was limited. There is a risk that if formal consistent monitoring of budgets is not taking place the Council are not tracking the achievement of saving plans effectively. Once a full a complement of staff are back in place within the Finance Team the Council will re-establish consistent quarterly budget holder meetings with budget holders.	Q2 2017/18	Head of Finance
2	There is currently no corporate guidance in place for staff to assist in drafting savings plans. As confirmed by our findings there is an inconsistent approach by Service Heads to creating savings plans. We observed there was a varying level of detail in each plan with key areas such as quality impact assessments not being carried out and the risks associated with implementing the savings plan not being mapped. Basic guidance will be issued to Service Managers on what should be included within savings plans in order to provide a more consistent and comprehensive approach. Corporate guidance will cover key areas such as; i) An analysis of how services will be impacted by the proposed savings plan ii) An analysis of how stakeholders will be impacted by the proposed savings plan and the risks associated with this iii) Potential risks that could impact on the implementation will be identified and risk mitigating strategies will be put in place.	Q2 2017/18	Head of Finance

FOR FURTHER INFORMATION CONTACT

Karen Williams

karen.williams@rsmuk.com

Tel: 07818 002463

GENDER PAY GAP REPORTING

New regulations planned to be effective by 6 April 2017 will require employers with 250 or more relevant employees in an individual entity on a snapshot date each year to publish within 12 months details of their employees' gender pay and bonus differentials.

The Equality Act 2010 (Gender Pay Gap Information) Regulations 2017 will apply to private and voluntary sector organisations. The Equality Act (Specific Duties and Public Authorities) Regulations 2017 are planned to be effective from 31 March 2017 and will apply to English public authority employers. The public sector reporting model is very similar to the private sector one.

What is the gender pay gap in the UK workforce?

Men's average pay is greater than that for women. The Office for National Statistics says that over the last 20 years the median gender pay gap has narrowed from 27.5 per cent to 9.4 per cent for full-time employees.

What are employers affected required to do?

To publish annually for employees in scope a report on:

- overall gender pay gap figures calculated using both the mean and median average hourly pay between genders;
- the numbers of male and female employees in each of four pay bands (quartiles), based on the employer's overall pay range; and
- for a 12 month period, both the difference between male and female's mean and median bonus pay and the proportion of relevant male and female employees who received a bonus.

An explanatory narrative, although not required, is strongly encouraged as is a statement of the actions planned to narrow the gaps.

The annual cycle of gender pay gap reporting

What are the timescales?

A snapshot of employees' pay for private and voluntary sector organisations must be taken on 5 April 2017 and on 5 April in each subsequent year and for public sector bodies on 31 March 2017 and on 31 March in each following year.

The first gender pay private and voluntary sector reports must be published both on the employer's own website and uploaded to a government website no later than 4 April 2018, to include hourly pay rates at 5 April 2017 and bonus payments between 6 April 2016 and 5 April 2017. The data must remain on the employer's website for three years.

Dry runs of data should be prepared now to ensure that any gaps are identified prior to the snapshot date/reporting period closing.

How can RSM help?

RSM has experts in payroll, HR consultancy and legal employment advice to support you in meeting both the requirements and the business opportunities of gender pay gap reporting.

Our services include:

We can analyse your data to determine relevance and to identify and assist in resolving any areas of uncertainty. This can include:

- status and relevance of employees including those working overseas;
- consideration of whether and what data is readily available; and
- analysis of the reportable elements of remuneration packages.

Calculations and narrative

RSM will work with you to collate your data on the required snapshot date to:

- prepare and process all reportable calculations;
- provide the calculations to you in a template statement which can be approved and published;
- guide on the voluntary narrative to support your results and to demonstrate accuracy of data; and
- make initial recommendations on publication dates and ensure that you receive an annual reminder.

Consultancy

RSM can review and analyse your results to create supporting action plans which may include:

- a review of current pay practices and audit of bonus schemes across your organisation;
- identification of skills shortages – recruitment process review;
- facilitation of analysis discussion identifying areas of risk and exposure; and
- formulation of communications plan and benchmarking data (industry/geographic/function) to provide context.

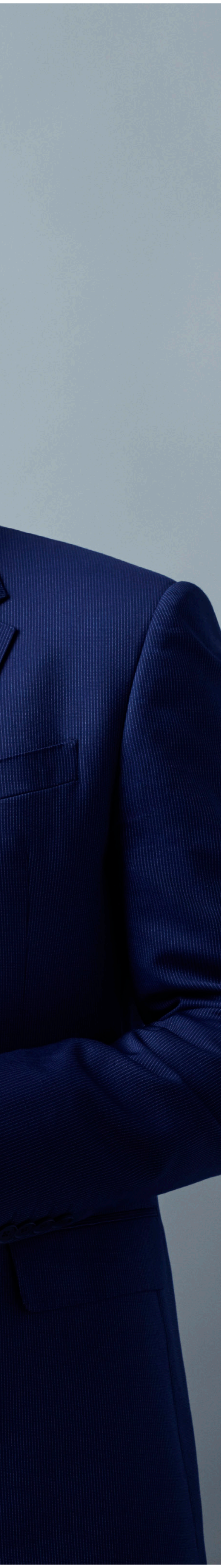
rsmuk.com

THE APPRENTICESHIP LEVY

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

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.

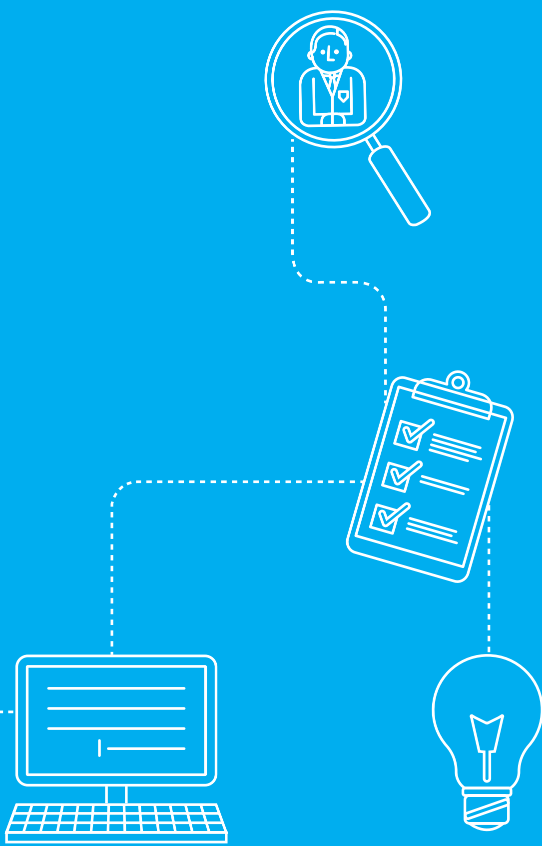
In some cases the apprentice will be required to undertake further maths and English training. This is funded separately (not from the levy funds) and the employer must allow time for study.

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

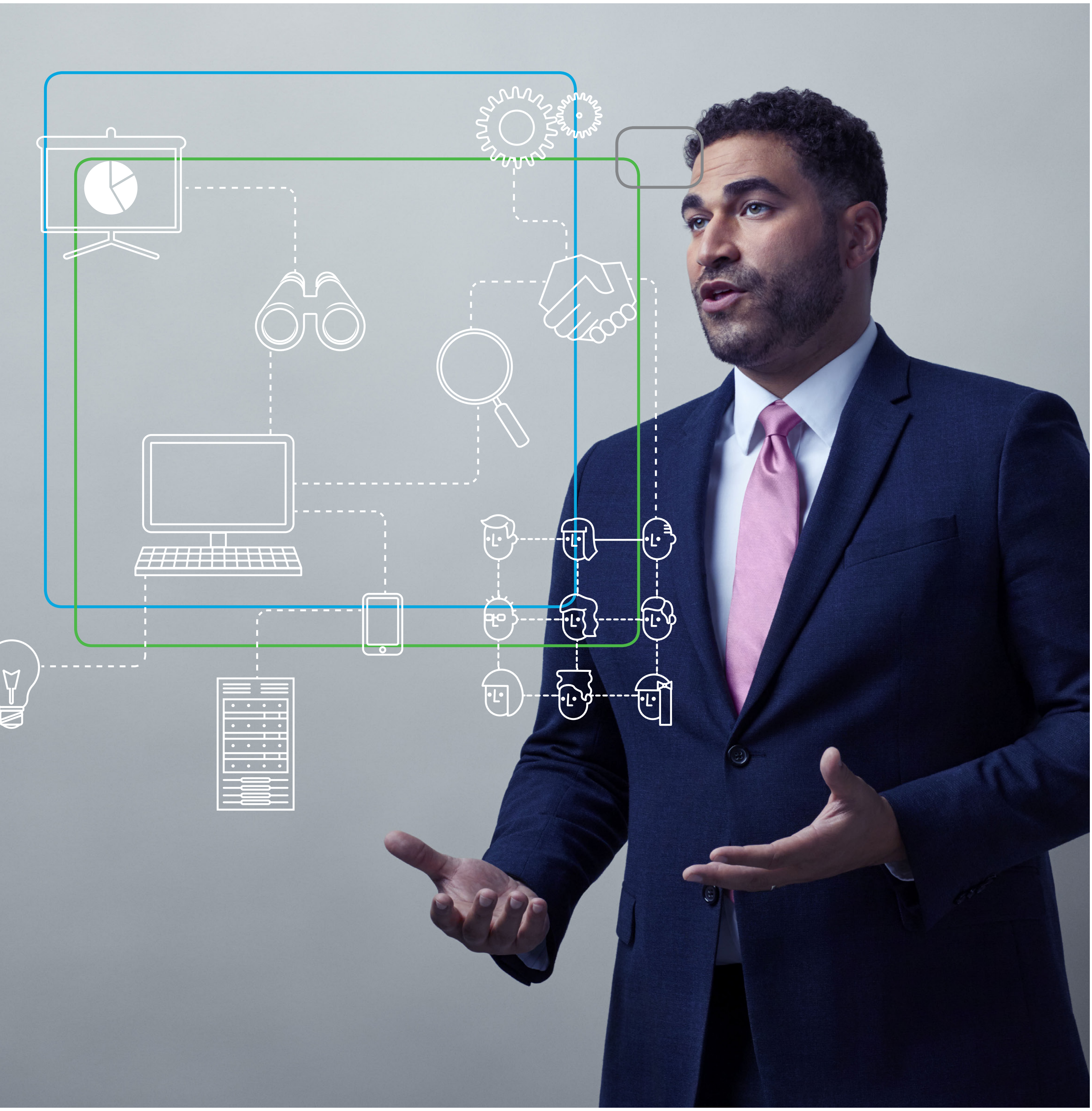
Lee Knight
Associate Director
T +44(0)20 3201 8508
lee.knight@rsmuk.com

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

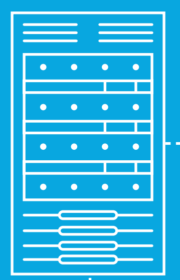
Can hackers access your system? What can they do once they're in your system? Our external testing process emulates the hacking process by using commercial and public domain tools to identify network vulnerabilities so you can take steps to correct them.

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

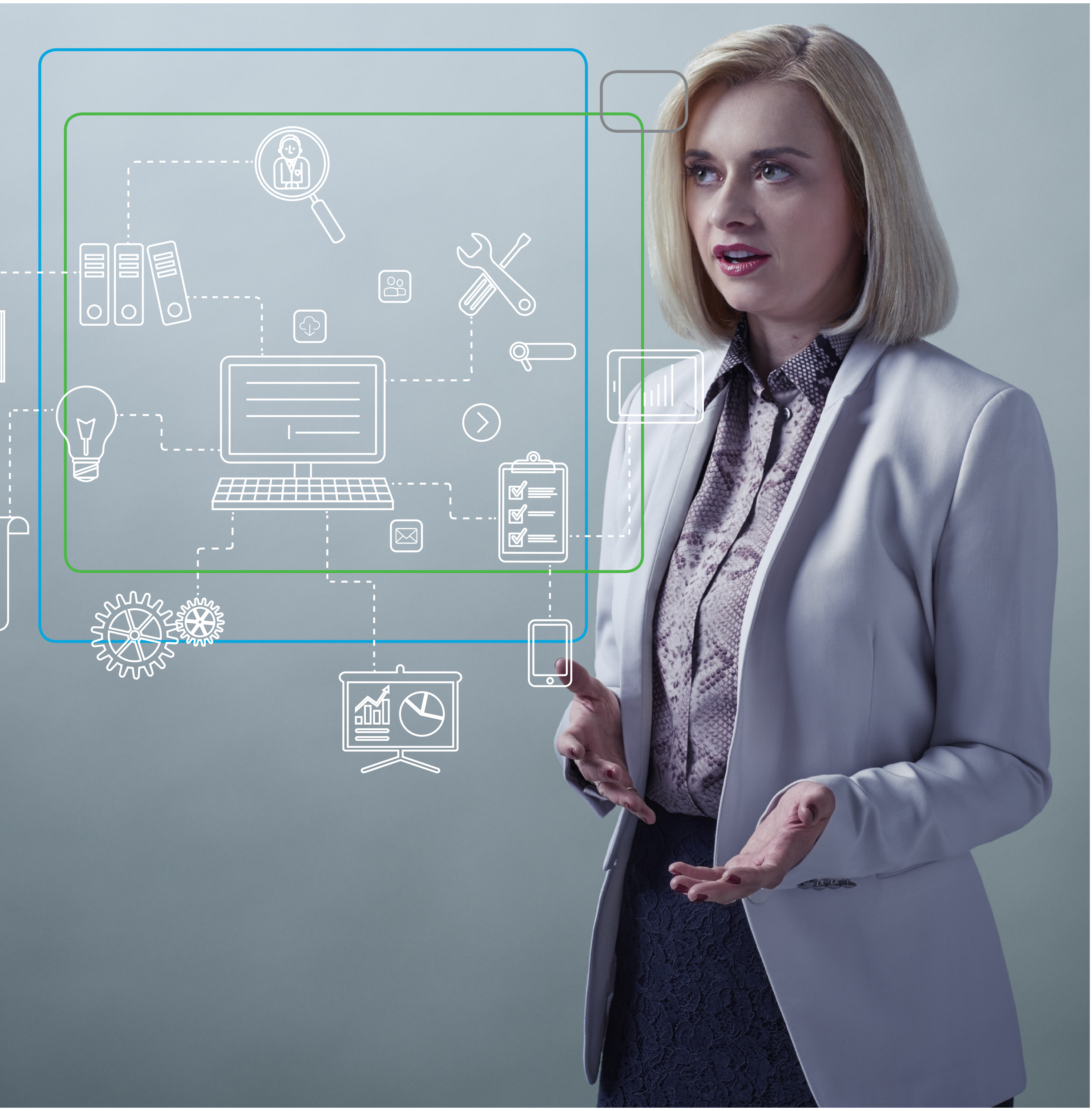
Sheila Pancholi
Partner

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

David Morris
Director

T +44 (0)78 0061 7128
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.

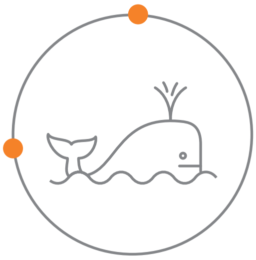
HOW DO CYBERCRIMINALS ATTACK?

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.



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.

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.

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?

STEP 1

Use provided mail extension (also sourced online)

STEP 2

Agree format and content of covert email

STEP 3

Send and track emails

STEP 4

With help from clients, monitor number of help desk queries

STEP 5

Benchmark results against database

- whether the email gets through the firewall and spam filters
- how many people recieve the email
- how many people open it
- how many people forward it on
- how many people click on the link within the email

STEP 6

Formal report and analysis of results

- 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 0061 7128
david.morris@rsmuk.com

rsmuk.com