TRANSPORT FOR THE NORTH

Internal Audit Progress Report

Audit and Governance Committee meeting of:

1 March 2019

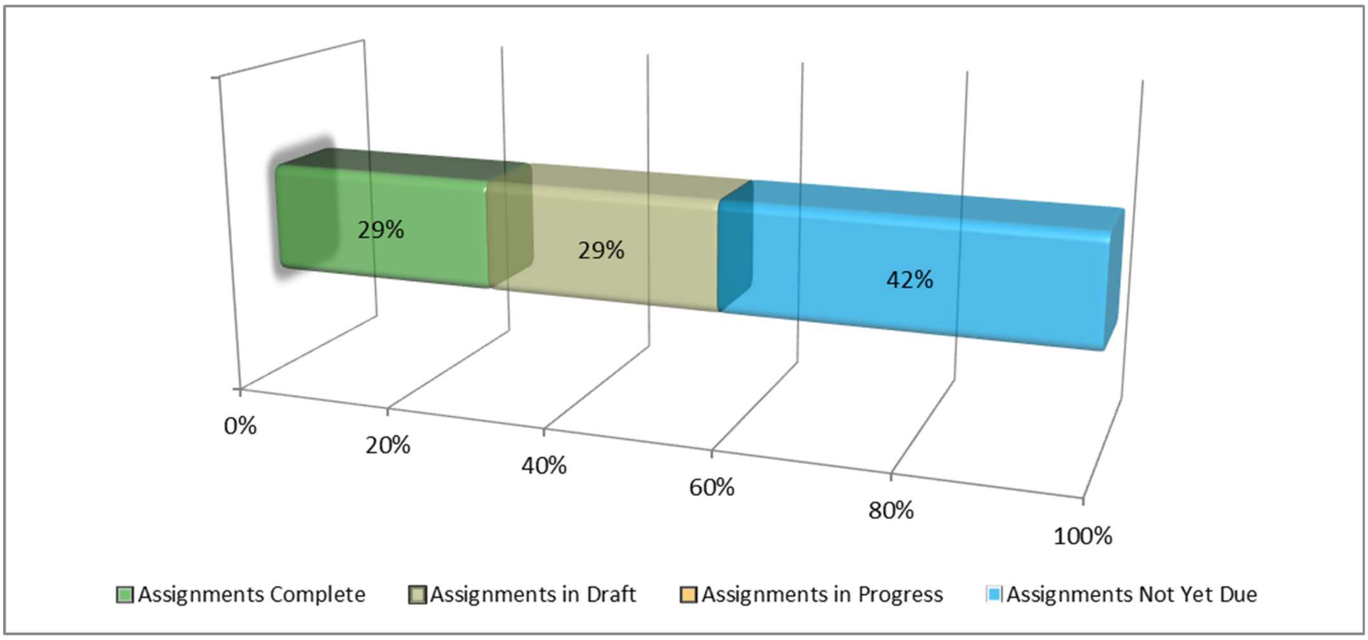
This report is solely for the use of the persons to whom it is addressed.
To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party.

RSM

CONTENTS

1 INTRODUCTION

The internal audit plan for 2018/19 was approved by the Audit and Governance Committee at its meeting on 19 September 2018. This progress report provides an update in relation to the delivery of the plan and summarises our work completed to date.



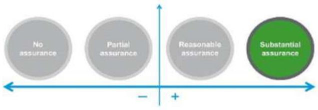
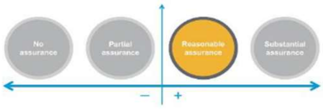
At the time of preparing this Progress report, the following two assignment reports (29% of the total plan) had been issued to management in draft for comment:

- Procurement Framework (3.18/19); and
- IT Audit – Cyber Security Controls (4.18/19).

We have provided a summary of our findings at section 2 below; it should be noted that these may be subject to change following the receipt of management responses to the draft reports.

2 REPORTS CONSIDERED AT THIS AUDIT AND GOVERNANCE COMMITTEE

The table below provides a summary update on progress against the approved Internal Audit Plan and summarises the results of our work completed since the last Audit and Governance Committee, as well as details of work not yet due.

Assignments	Status	Opinion issued	Actions agreed		
			L	M	H
Procurement Framework (3.18/19)	Draft	 No assurance Partial assurance Reasonable assurance Substantial assurance – +	3	1	0
IT Audit – Cyber Security Controls (4.18/19)	Draft	 No assurance Partial assurance Reasonable assurance Substantial assurance – +	6	4	0

2.1 Impact of findings to date

As noted at section 1 above, the assignment reports for these two reviews are currently in draft awaiting management responses and therefore the high level findings noted below may be subject to change when the reports are finalised.

Procurement Framework

We confirmed that an appropriately designed framework is in place to ensure the use of quotes and tenders for the procurement of goods and services, recording of contracts and reporting of contract activities. We identified a small number of areas were the control framework could be strengthened, resulting in three 'low' and one 'medium' priority management actions being agreed. The 'medium' priority action related to ensuring that the Supplier Recommendation Report is amended to require staff authorising the procurement of goods and services from a chosen supplier to declare any interests in the supplier.

IT Audit – Cyber Security Controls

We identified that TfN has implemented a number of technical controls in order to secure its network against external attackers. However, some control developments are required to further enhance the cyber security control framework. This resulted in six 'low' and four 'medium' priority management actions being agreed. The 'medium' priority actions related to the following areas:

- TfN does not undertake external penetration testing. In addition, TfN does not have a formal policy over the requirements to undertake vulnerability assessments on a periodic basis.
- TfN allows the use of unencrypted removable media devices on its network.
- All users are currently set up as Local Administrators on their PCs and laptops. There therefore is a risk that users have an inappropriate level of access to privileges on their devices and can install applications or perform actions which create vulnerabilities for the network.

- We noted that six devices were not up to date with the latest security patches. This increases the risk that known network vulnerabilities could be exploited.

3 LOOKING AHEAD

Assignment area	Fieldwork Start Date	Status
Payroll **Assurance**	w/c 11 March 2019	Planning issued
HR Policy Suite **Advisory**	Please see section 4.1 below in relation to proposed change to the approved internal audit plan.	Please see 4.1 below.
Business Planning **Advisory**	RSM specialists would provide advice and support by being a 'critical friend' to the organisation at selected points whilst going through the business planning review cycle.	TfN to confirm best timing.

4 OTHER MATTERS

4.1 Changes to the approved internal audit plan

The approved internal audit plan includes an allocation for an advisory review of TfN's suite of Human Resources policies, to be carried out by our specialist consulting colleagues within RSM HR. We have recently discussed this piece of work with the Finance Director and suggest that this is deferred to a later year, with the approval of the Audit and Governance Committee.

There have been no other changes to the approved plan for 2018/19 to date.

4.2 On-going liaison

There has been ongoing liaison with management during our last on-site visit and in the finalisation of our audit assignments, as well as planning of forthcoming audits. We have also discussed the indicative internal audit plan for 2019/20, which is included on the agenda as a separate item for this meeting.

4.2 Information and Briefings

We have appended to this Progress Report the following briefings:

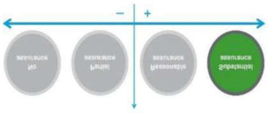
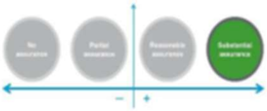
- Brexit: Determining Your Direction – Are you Ready?
- Cyber Security – Staff at Work, at Home and on the Move

In addition, management have been invited to participate in our Not for Profit – Key Performance Metrics research and feedback exercise. This thought leadership thematic review will include data collated from clients, and compares national trends to consider how organisations can maximise their performance through improving employee behaviours and engagement. Data will be collated on a number of key metrics, including the following areas:

- Workforce composition
- Recruitment & retention
- Sickness & absence
- Employee relations
- Skills & competencies
- Performance management
- Employee engagement & voice
- Pay & reward

APPENDIX A: INTERNAL AUDIT ASSIGNMENTS COMPLETED TO DATE

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

Assignment	Opinion issued	Actions agreed		
		L	M	H
Risk Management Framework (1.18/19)	 – + No assurance Partial assurance Reasonable assurance Substantial assurance	4	1	0
Payment Authorisation Processes, Expenses and Use of Procurement Cards (2.18/19)	 No assurance Partial assurance Reasonable assurance Substantial assurance – +	2	0	0

FOR FURTHER INFORMATION CONTACT

Lisa Randall, Head of Internal Audit

lisa.randall@rsmuk.com

07730 300 309

Sarah Massel, Manager

sarah.massel@rsmuk.com

07484 040 612

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of Transport for the North, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.

BREXIT: DETERMINING YOUR DIRECTION – ARE YOU READY?

With Brexit dominating the news, there is no doubt that it will have a far-reaching impact on many organisations and so with Brexit uncertainty levels running high, RSM has summarised five key areas that organisations should be reviewing.

1. Regulation

- How will you keep up-to-date and maintain compliance with the changing regulatory frameworks?
- Will you still be able to trade easily and efficiently with other countries/suppliers through your existing legal structures?

2. Finance and supply chain

- In what ways will decisions and uncertainties impact your cash-flow and access to finance?
- What is the impact of Brexit on your supply chain?
- Have you considered current commitments / guarantees – the security of income?

3. People

- How will you continue to recruit and retain the right people?
- Have you assessed the right-to-work status of your workforce?
- Do you know of any possible risks to key members of the workforce?
- How will you ensure the right-to-work status as part of the recruitment process?

4. Business Management

- What tools will you put in place to avoid any disruption to core operations whilst maintaining business continuity?

5. Trade/Contracts

- Have you reviewed your existing supplier contracts and do any of them need updating or amending?
- Will you be able to enforce existing contracts and how might existing contracts be interpreted?
- How big is your exposure to contract risk and do you know which contracts to focus on to assess your exposure?
- Will Brexit impact your ability to meet the requirements of existing contracts?

Did you know?

The UK Government website holds a comprehensive library of published papers, consultations and technical notices, dating from July 2016, covering all aspects of the Brexit process. Latterly this has focused on a no deal Brexit. The full library can be accessed here: Read More

The technical notices published since August 2018 provide both business and citizens with guidance on Brexit, focusing on a ‘no deal’ Brexit.

Taking into consideration the continuing challenges as possible opportunities, around preparing for Brexit, the uncertainty of the unknown impacts and consequences of a no deal Brexit, and continuing to meet the pressures of day to day operations; as a minimum management should be considering:

- Is there a team in the organisation responsible for reviewing the technical notices issued by the Government, and considering whether or not they are, or may be, applicable to the organisation? How they may impact and what needs to be done to prepare in the short, medium and longer term as a result?
- Has the responsibility for Brexit been assigned to a lead point or contact through the existing management and governance structures of the organisation?
- Is there any formal reporting on progress to date on Brexit preparations?
- Has the organisation considered and assessed the key risks in relation to Brexit; including the potential impact and contingency planning?

- Has the organisation engaged with suppliers to understand their Brexit plans and contingencies, and whether plans need to be made to align with contractors / suppliers / stakeholders?

How can we help?

RSM is working directly with other organisations, supporting their Brexit planning. We offer assessments and support from high end strategic planning through to detailed financial modelling scenario mapping, business structure reviews, goods and duty impact reviews.

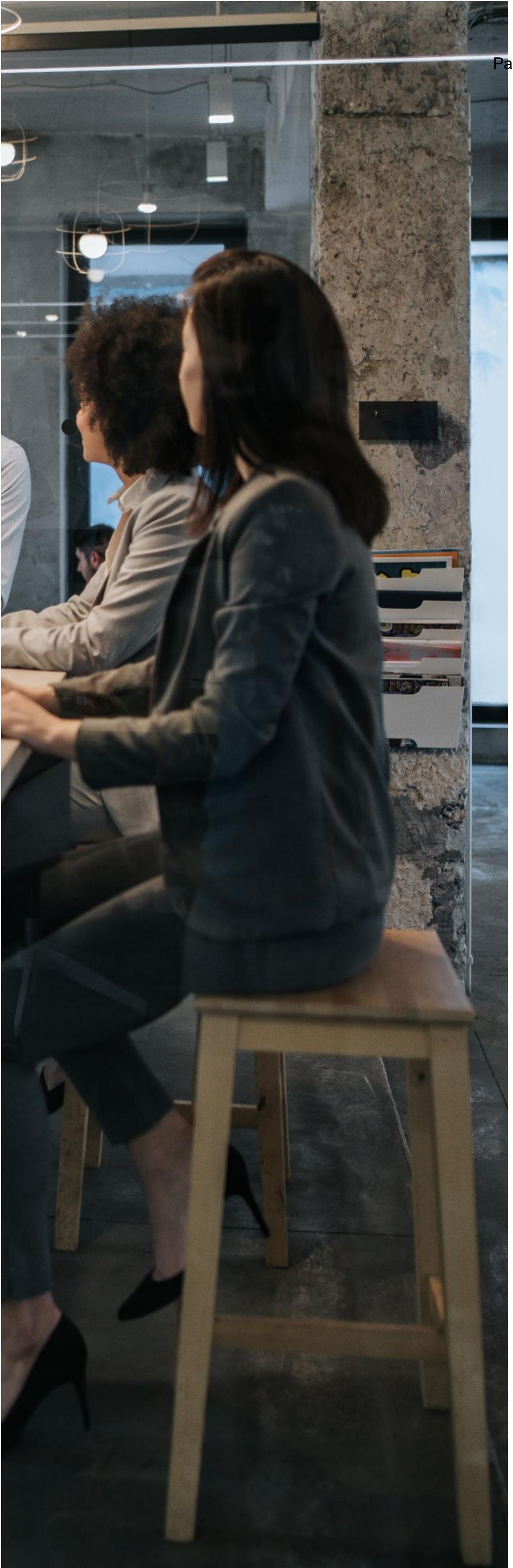
We have supported clients in implementation and action mapping organisational readiness from both March 2019 and beyond. All delivered by subject matter specialists relevant to your specific needs.

www.rsmuk.com/brexit

DO YOUR STAFF KNOW ENOUGH TO PROTECT YOUR ORGANISATION?

Why cyber security is crucial for staff at work, at home and on the move

RSM



Human error is a major factor in data breaches. From misaddressed emails to lost devices, mistakes can be common and can be costly. Consequently, education and awareness of staff at all levels is paramount.

Staff are the first and last line of defence against cyber criminals. Staff who are up-to-date on current risks and have been provided with clear instructions on what to do to prevent them are a great company asset. As such, it is very important to get the basics right.

This flyer presents a no-nonsense, practical guide to good cyber practices that can be used by staff to check their behaviours both at work and at home. It incorporates our practical experience gained from working across multiple clients in many different business sectors.

To help you make practical use of this guide, we have formatted it so your staff can use it as a practical checklist, ticking off those elements that they already comply with and helping you to highlight those aspects where work may be required to strengthen controls and awareness.

HOW TO PROTECT YOUR DATA

The use of mobile and portable devices in the workplace has exploded and will continue to increase. Whilst this brings advantages in terms of new working practices and productivity, practical measures need to be taken to ensure that you are not exposed to unnecessary risk.

Physical security when off-site

❑ Don’t leave laptops, phones or tablets in plain view - put them in the boot or take them with you.

❑ Don’t leave electronic equipment in the car overnight.

❑ Don’t keep company information on personal laptops or storage devices.

❑ Make sure storage devices with company information have password or PIN protection and appropriate encryption.

❑ Where possible, enable 2 factor authentication for your personal devices and accounts.

□ Watch out for distraction thefts of phones and tablets.

□ Be careful when using laptops etc in places such as trains – shoulder surfing is very common and is a frequent cause of data loss.

□ Ensure that your mobile devices - be they company owned or private – can be tracked, logged or wiped in the event of theft or loss.

Physical security in the office

□ Do not let people tailgate into your office – ensure staff challenge them and ask their business.

□ Clear desks at the end of the day and lock all drawers and cabinets.

□ Lock offices when leaving them.

□ The last person to leave the office should put the alarm on.

□ Report any lost key cards, passes or other access equipment immediately.

□ Lock your desktop PC when away from it by pressing Windows Key + L.

Using free wi-fi

□ Be very cautious about using free wi-fi in places like coffee shops or pubs – these networks are rarely secure and other people could see the systems activity.

□ If you need to gain access to the internet, use your mobile phone as a hotspot and take advantage of the secure telecommunications network.

Passwords

Whilst they are not ideal, passwords provide the best basic defence against hackers - they need to be managed appropriately.

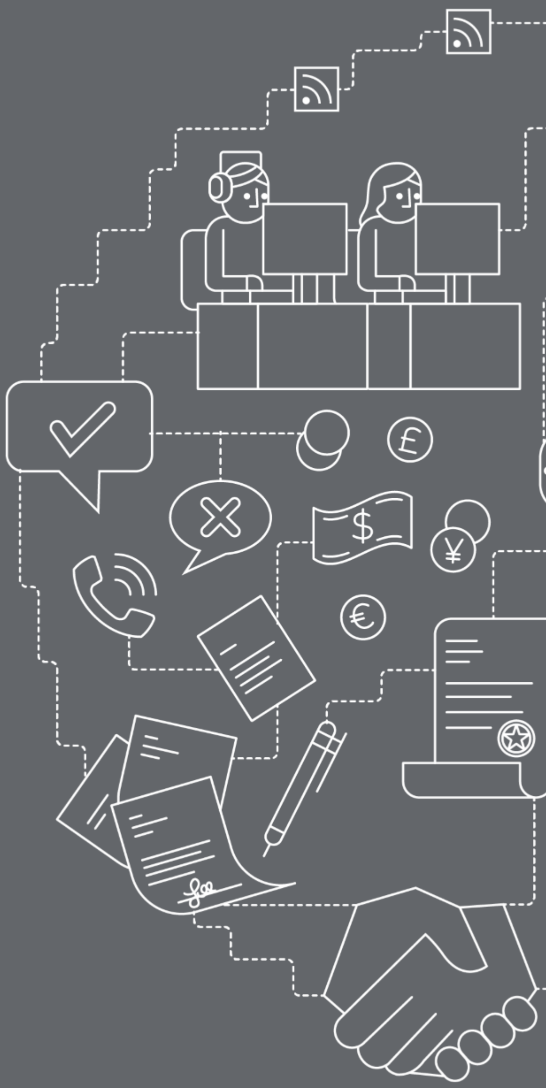
□ Use password protection on all devices – tablet, laptop, mobile phone and wearables.

□ Try to use non-predictable passwords such as phrases or random sets of letters and numbers.

□ Change passwords regularly – every 60 days is sufficient.

□ Make sure passwords are sufficiently complex and are not obvious (birthdays, QWERTY etc).

□ Make sure passwords contain a mix of alpha numeric and special characters.



- ❑ Use different passwords on different accounts and devices – that way, when one is compromised, you still have some protection over the others.
- ❑ Do not tell anyone your passwords whoever asks.
- ❑ Do not write down passwords anywhere.
- ❑ The same advice applies to PIN numbers for bank cards and devices

Phishing attacks

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies or individuals to induce your staff to reveal information such as passwords and account numbers that can then be used for fraud.

- ❑ Do not offer personal information in response to emails – never give out your password or company bank details.
- ❑ Always verify the sender of an email before clicking on any links or downloading any attachments. For example, would an Apple employee really send you an e-mail from a Gmail account?
- ❑ Consider the content of the email ie whether there are spelling mistakes, is the language too colloquial? Are pictures fuzzy and pixelated?
- ❑ Does it relate to something that shouldn't impact you eg it's from Apple when the company doesn't use Apple products.
- ❑ Is there missing data that you would expect to see?
- ❑ Does it contain veiled threats to the on-going activities of the business?
- ❑ Hover over links before clicking on them - see if the information that appears in the pop-up boxes matches the supposed sender.
- ❑ Report any suspicious emails or activity to management immediately.
- ❑ Instead of clicking on links, go to the appropriate website and find the destination for the link that way.
- ❑ Never provide sensitive business data to unfamiliar individuals outside the company.
- ❑ Do not link your work email to any email subscription lists. These lists pose an intrinsic threat as far as phishing emails are concerned. In a corporate network, limiting such vulnerabilities is a priority.

MALWARE AND RANSOMWARE

Malware is software which is specifically designed to gain unauthorised access to a computer system or otherwise damage it. Ransomware is a very specific sub-set that denies companies access to their own systems. Companies should take the following precautions to protect themselves.

On company devices

- □ Do not allow staff to download any software onto work devices.
- □ Transferring data with USB flash drives should be avoided where possible – they are the easiest way to infect a computer with a virus because it is very difficult to stop a malicious program on a device physically connected to the computer.
- □ Keep security and operating systems updated – don't refuse patches and security up-dates.
- □ Do not encourage staff to save work on local devices if you can help it. Back it up onto the work servers at every opportunity.
- □ Protect against ransomware by taking regular back-ups which are stored in the cloud or elsewhere.

On the web

- □ Surfing the Internet on suspicious websites should be avoided – some websites are developed with the sole purpose of spreading malware. Look for the symbol that denotes that a website is secure – this is a small padlock symbol in the address bar (or elsewhere in your browser window) and a web address beginning with https:// where the 's' stands for 'secure').
- □ If a website's security certification is expired, do not go on it – it may be an administration error but there may be a reason why it appears.
- □ Install and maintain up-to-date firewalls and anti-virus software.
- □ If a website is blocked by the firewall or antivirus, do not attempt to go around it – it's been blocked for a reason.

Using free software and Apps

- □ Beta or Open Source software should not be installed on company computers / laptops / mobile devices. This is because it is often targeted by hackers who put malware or viruses in the code.
- □ Staff should only be permitted to download free Apps from a manufacturer approved store eg Google Play.

At home

- □ Employees should install anti-virus software on their private devices and enable its automatic updating.
- □ Home computers should be password protected.

SOCIAL MEDIA

There are certain risks associated with social media that must be realised and addressed.

- Delete social media accounts pertaining to the company that are no longer in use
- Change your passwords regularly
- Be careful what staff post on social media – it could be of use to those who want to pretend to be you
- Check privacy settings regularly, particularly after any software upgrade as they can sometimes revert to factory settings

ATMs

- □ Don’t use ATMs that looked damaged or tampered with.
- □ Use your hand to cover the number keys as you type in your PIN code, try to remember the pattern of keys so you don’t have to see them when typing.
- □ Beware distraction thefts ie one person taps you on the shoulder and another takes your money when you look round.

AWARENESS

A well-trained and knowledgeable workforce is potentially the greatest asset. It is imperative that staff are trained on the importance of cyber security.

- □ Staff should be required to read and understand company IT policies and guidelines, and that they follow procedures in relation to cyber risk.
- □ Regular and informative cyber security training should be provided to all staff. Keeping security awareness high is a key defence against cyber risk.
- □ The single most important thing an employee can do is immediately report a data breach. Regardless of the cause, employees must know that it is their duty to report a breach to the appropriate individuals.
- □ Management should ensure that they are up-to-date on current threats. For example, the Action Fraud website provides regular up-dates on known scams and can be configured to send regular updates.
- □ Tone at the top is key – staff will not implement good practice if management and owners do not.
- □ Management should review working practices on a regular basis to ensure that they protect against current threats. For example, a current risk is the receipt of emails and invoices from people masquerading as a supplier. They will ask for bank account changes which should not be approved without due process.
- □ Management need to establish a security culture where it is OK to question suspicious activities and where staff will not be criticised for trying to do the right thing.

For further information please contact

Sheila Pancholi
Partner
T +44 (0)7811 361638
sheila.pancholi@rsmuk.com

Steve Snaith
Partner
T +44 (0)7966 039009
steven.snaith@rsmuk.com

David Morris
Director
T +44 (0)7800 617128
david.morris@rsmuk.com

Jan Hameed
Director
T +44 (0)7900 051599
jan.hameed@rsmuk.com

RSM

25 Farringdon Street
London
EC4A 4AB
T +44 (0)20 3201 8000
F +44 (0)20 3201 8001
www.rsmuk.com

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM