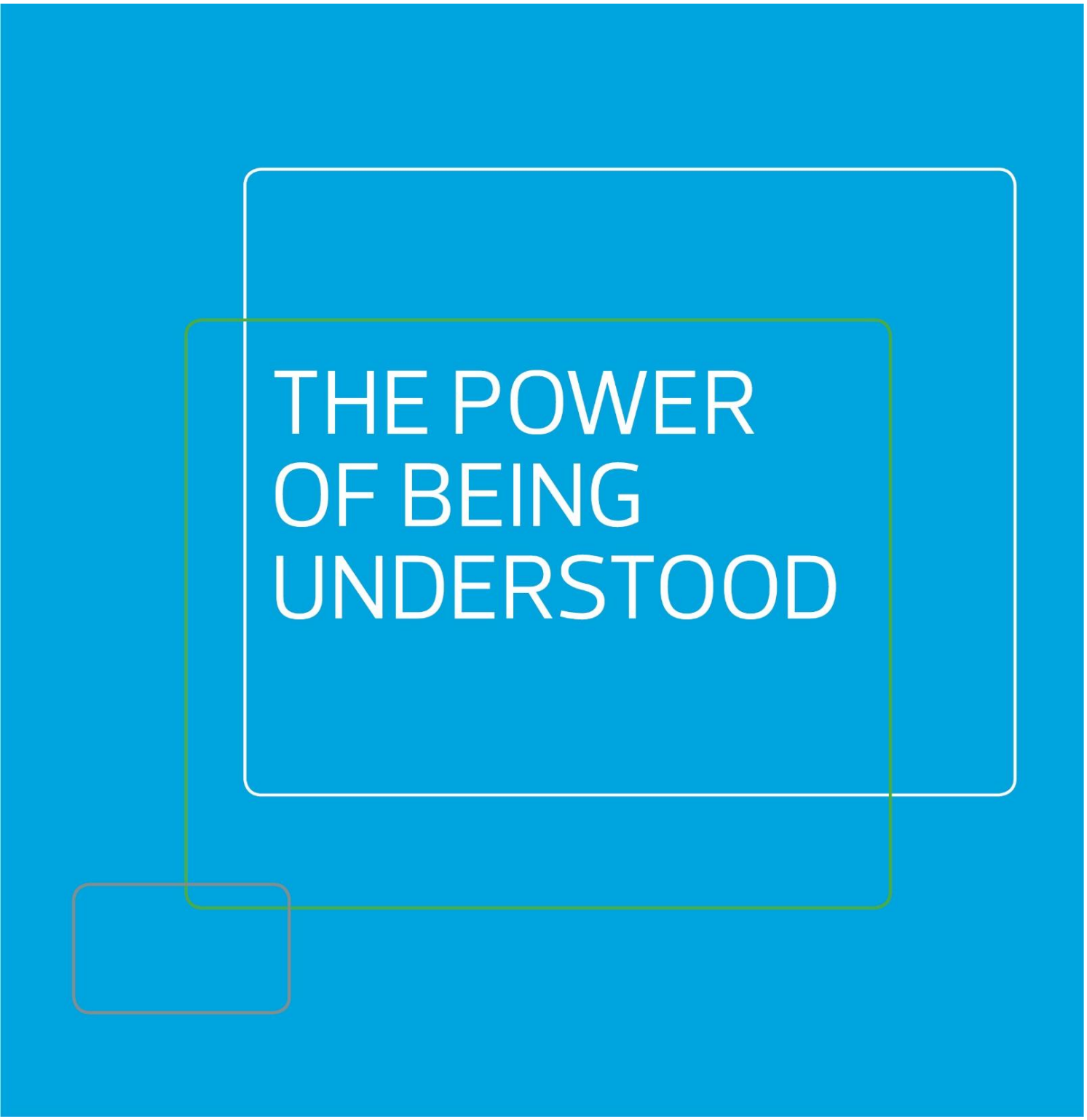


ESSEX FIRE AUTHORITY

IT General Controls Healthcheck

FINAL

Internal Audit Report: 1.15/16

3 November 2015

RSM

CONTENTS

Debrief held	17 September 2015	**Internal Audit team**	Daniel Harris, Partner Suzanne Lane, Client Manager David Morris. Technology Risk Assurance (TRA) Director Joe Webb, Consultant TRA
Draft report issued	8 October 2015		
Responses received	3 November 2015		
Final report issued	3 November 2015	**Client sponsor**	Glen McGuinness, Deputy Director of Finance Jan Swanwick, Head of ICT
		Distribution	Glen McGuinness, Deputy Director of Finance Jan Swanwick, Head of ICT

As a practising member firm of the Institute of Chartered Accountants in England and Wales (ICAEW), we are subject to its ethical and other professional requirements which are detailed at http://www.icaew.com/en/members/regulations-standards-and-guidance.

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. Recommendations for improvements should be assessed by you for their full impact before they are implemented. 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. Therefore, the most that the internal audit service can provide is reasonable assurance that there are no major weaknesses in the risk management, governance and control processes reviewed within this assignment. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

This report is supplied on the understanding that it is solely for the use of the persons to whom it is addressed and for the purposes set out herein. Our work has been undertaken solely to prepare this report and state those matters that we have agreed to state to them. 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 party other than the Board which obtains access to this report or a copy and chooses to rely on this report (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 our Client 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.

1 EXECUTIVE SUMMARY

1.1 Background

An IT Healthcheck was carried out as part of the 2015/16 internal audit plan. The objective of our review was to assess the risks, processes and controls commonly associated with the IT control framework, to consider the adequacy of internal controls, processes and procedures governing the IT control framework and operating environment and to identify areas of immediate risk to Essex Fire and Rescue Service ("the Service") where improvements would benefit the control framework.

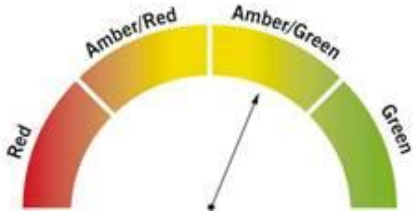
The IT Healthcheck can also be used to identify areas that would benefit from specialist IT audit review and therefore inclusion in the Internal Audit Strategy in future periods. However, it is necessary for management to consider the results and make their own judgement on the risks affecting the Service and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised.

1.2 Conclusion

Our review did not highlight any matters that present significant IT risk to the Service. Three medium priority management actions have been agreed with the service.

Internal Audit Opinion:

Taking account of the issues identified, the Board can take reasonable assurance that the controls in place to manage this risk are suitably designed and consistently applied. However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified risk.



1.3 Key findings

The key findings from this review are as follows:

We have identified the following well designed controls:

- Environmental monitoring is in place within all server rooms. Going forward, Solarwinds is being used to monitor and alert on environmental factors (e.g server room temperatures, UPS state, humidity).
- The server rooms all have Uninterruptable Power Supplies (UPS) in place to provide power until the generator is powered up. Note: during the review the Service had genuine power issues: the controls in place were able to protect the server rooms during this power shortage.
- Each server room has redundant air conditioning to cool the room.
- The main server room has a system in place that prevents fires from being ignited within the confines of the server room.
- The Service utilise Sophos antivirus to protect the network and computer devices from malicious code. The antivirus is updated throughout the day automatically on both servers and computers.
- The Service has a firewall in place within the server rooms which has failover capabilities. Only a limited number of staff have access to the firewall in order make changes, which are recorded and reviewed as required.

- The Service has a replication process in place that copies data and stores the data at their disaster recovery server room which is offsite. Backup is a separate activity in addition to replication; the content is stored externally (stored at the Supplier's two UK based locations).
- Backup success is monitored regularly by the IT department. In addition, the Service is supported by a third party named Backup Technology. They also review backup failures and perform remedial action to correct any issues.
- Internet and email filtering is in place to reduce the risk of inappropriate content and malicious code from effecting the computer network.
- The Service has a documented Data Protection Act policy to provide staff guidance, and the Service is registered with the Information Commissioners Office (ICO) in order to process personal data.
- We selected a sample of 20 devices that included servers, desktops, laptops and virtual desktops and confirmed that Sophos antivirus was installed and up to date. This reduces the risk of malicious code affecting the IT infrastructure.

We have identified two medium and three low priority recommendations in relation to the design of controls. Below is a summary of these findings:

- Leaver accounts are disabled when the IT department are informed by HR. Daily reports should be received to identify all staff leavers. However this process would not identify agency staff and there is not currently a process in place to capture these leavers. We selected a sample of 20 staff leavers and confirmed that in 2 cases, the accounts had not been disabled. This was due to the IT department not being provided with the leaver reports. Unless both agency and staff accounts are disabled in a timely manner, there is an increased risk of unauthorised access to the network.
- The information security policy does not include all of the information that should be within such a policy; for example, physical security arrangements, logical security, data backup processes, asset management and security incident reporting. Unless a documented policy is in place, there is an increased risk that there is inadequate guidance for staff. If the policy is documented in line with the ISO standard as planned, this would demonstrate the well-designed controls in place regarding information security.
- Backup restore testing is not performed as part of a defined testing schedule. We confirmed that no restore testing schedule is in place at the Service. The IT team confirmed that ad-hoc file restores are performed to restore files and emails when the need arises. However, there are no scheduled restore tests in place for restoring servers in a disaster recovery environment. Oracle restore testing has been performed - this highlighted that the restore process was not simple to carry out. There is a risk that the Service is not able to restore data and servers should a major incident occur. Restoring files from back-ups does not replicate the scenario of a major incident requiring backup restoration across a number of servers.
- Processes are in place to update the virtual desktop image and servers on a monthly basis. Desktops and laptops are set to automatically update, however a small minority of legacy devices are not monitored to identify devices that are not updating. Unless all devices are monitored to ensure that they are installed with the latest updates, there is an increased risk that some devices may be vulnerable to current security weaknesses.
- The Service has third parties that it shares information with on a regular basis. We were informed by the ICT Security Officer that information sharing agreements are documented. However there is not an information sharing register which identifies all of the sharing arrangements in place. This would reduce the risk that information is being transferred insecurely, both now and in the future.

In general we identified that recurring controls were being complied with. However, we have identified one medium and one low priority recommendation in relation to the application of controls. Below is a summary of these findings:

- From review of the server room access reports we identified staff that would not have a business requirement or the expertise required to work within the room. This increases the risk that inappropriate access is gained and potentially activity is performed within the room, which could impact on IT server availability.

- We selected a sample of 20 new starters to confirm if the new user form was received to confirm that a new account was required and the account access requirements are identified. For our sample of 20 new user accounts, 3 forms could not be located. Note: we identified the original request for two of these, without the form. This increases the risk that accounts are not created in accordance with procedure and staff may therefore not have the appropriate access.

.

1.4 Additional information to support our conclusion

Risk	Control design*	Compliance with controls*	Agreed actions		
			Low	Medium	High
Control weaknesses exist that result in a loss to systems integrity, confidentiality and availability.	5 (17)	2 (17)	4	3	0
Total			**4**	**3**	**0**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

2 ACTION PLAN

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may, with a high degree of certainty, lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The table below sets out the actions agreed by management to address the findings:

Ref	Findings summary	Priority	Management action	Implementation date	Owner responsible
Risk: Control weaknesses exist that result in a loss to systems integrity, confidentiality and availability.					
1.1	From review of the access reports we identified staff that would not have an obvious business requirement or expertise required to work within the server room.	Medium	We will review the access levels to the server rooms and will consider removing access to staff that do not have the required expertise and the business requirement.	31/12/2015	IT to review access and Property Services to update / maintain Control.
1.2	3 new starter forms from a sample of 20 could not be located as part of the new user account process.	Low	We will ensure that prior to account creation, a form is received and uploaded onto the service desk.	31/10/2015	Service Desk Manager

Ref	Findings summary	Priority	Management action	Implementation date	Owner responsible
1.3	In 2 out of the sample of 20, the staff leaver accounts had not been disabled. There is no process in place to identify agency staff leavers.	Medium	We will communicate with the HR department the importance of receiving regular leaver updates. For agency staff, we will introduce an expiry date onto all such accounts. If a leaving date is not known in the first instance we will use an appropriate time period of 1-3 months.	30/11/2015	Service Desk Manager
1.4	The information security policy does not include all of the information that should be within such a policy.	Low	The Service will be documenting a full information security policy and this will be completed using ISO 27001 guidance.	31/12/2016	ICT Security Officer
1.5	Backup restore testing is not performed as part of a defined schedule.	Low	The Service will implement a defined schedule to confirm that servers and data can be restored in a continuity event.	30/06/2016	Service Delivery Manager
1.6	Small subset of legacy laptops and desktops are not proactively monitored to identify devices that are not up to date with the latest security patches.	Low	We will continue to monitor the updates for our desktops and laptops to ensure that all devices remain up to date with the latest security updates. Any devices that do not comply, we will investigate and ensure that device is appropriately managed.	Implemented	Service Delivery Manager

Ref	Findings summary	Priority	Management action	Implementation date	Owner responsible
1.7	Information sharing agreements are in place with third parties, however there is not an information sharing register which identifies all of the sharing arrangements in place.	Low	We will complete a register to identify the information that we transfer that will include the transfer methods and the information types. This will ensure that all data is transferred securely.	31/12/2016	Senior Information Risk Owner

3 DETAILED FINDINGS

This report has been prepared by exception. Therefore, we have included in this section, only those risks of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Management action
Risk: Control weaknesses exist that result in a loss to systems integrity, confidentiality and availability.						
1.1	Physical security to server rooms is provided using dongle access which is managed by the Property Services department.	Yes	No	From review of the access reports we identified staff that would not have a business requirement or the expertise required to work within the room. This increases the risk that inappropriate activity is performed within the room.	Medium	We will review the access levels to the server rooms and will consider removing access to staff that do not have the required expertise and the business requirement. Control is managed by Property Services.
1.2	In order to obtain a user account, new user forms are signed and then sent to the Service desk system for action, unless a form is provided the account should not be created.	Yes	No	We selected a sample of 20 new starters to confirm if the new user form was received to confirm that a new account was required and the account access requirements are identified. For our sample of 20 new user accounts, 3 forms could not be located. Note: we identified the original request for two of these, without the form. This increases the risk that accounts are not created in accordance with procedure and may not have the required access.	Low	We will ensure that prior to account creation, a form is received and uploaded onto the service desk.
1.3	Leaver accounts are disabled when the IT department are informed by HR. Daily reports should be received to identify all staff leavers. However this process would not	No	NA	We selected a sample of 20 staff leavers and confirmed that in 2 of the 20 sample, the accounts had not been disabled. This was due to the IT department not being provided with the leaver reports. Unless both agency and staff accounts are disabled in a timely manner, there is an	Medium	We will communicate with the HR department the importance of receiving regular leaver updates. For agency staff, we will introduce an expiry date onto all such accounts and inform the hiring manager. If a leaving date is not known in the first instance we will use an appropriate time period of 1-3 months.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Management action
	identify agency staff and there is not currently a process in place to capture these leavers.			increased risk of unauthorised access to the network.		
1.4	The information security policy does not include all of the information that should be within such a policy. An updated draft policy is under progress and is being written in line with the ISO 27001 Information security management standard.	No	NA	Unless a documented policy is in place, there is an increased risk that there is not documented guidance for staff. If the policy is documented in line with the ISO standard as planned, this would demonstrate the good controls in place regarding information security.	Low	The Service will be documenting a full information security policy and this will be completed using ISO 27001 guidance.
1.5	Backup restore testing is not performed as part of a defined schedule.	No	NA	We confirmed that no restore testing schedule is in place at the Service. The IT team confirmed that ad-hoc file restores are performed to restore files and emails when the need arises. However, there are no scheduled restore tests in place for restoring servers in a disaster recovery environment. Oracle restore testing has been performed, this highlighted that the restore process was not a simple process. There is a risk that the Service is not able to restore data and servers should a major incident occur. Restoring files from back-ups does not replicate the scenario of a major incident requiring backup restoration across a number of servers.	Low	The Service will implement a defined schedule to confirm that servers and data can be restored in a continuity event.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Management action
1.6	Patch management to ensure that computer devices remain up to date with security hot fixes is performed using Windows Server Update Service (WSUS). Processes are in place to update the virtual desktop image on a monthly basis, and the servers are updated. Desktops and laptops are set to automatically update, however they are not monitored to identify devices that are not updating.	No	NA	Unless all devices are monitored to ensure that they are installed with the latest updates, there is an increased risk that some devices may be vulnerable to current security weaknesses. Comment: The approach here is around management, as not all devices can be patched/updated.	Low	We will continue to monitor the updates for our desktops and laptops to ensure that all devices remain up to date with the latest security updates. Any devices that do not comply, we will investigate and ensure that device is appropriately managed.
1.7	The Service has third parties that it shares information with on a regular basis. We were informed by the ICT Security Officer that information sharing agreements are in place, however there is not an information sharing register which identifies all of the sharing arrangements in place.	No	NA	An information register would enable the Service to identify all of the information that may be sent out to third parties, it would also document the controls used when transferring the data and would therefore reduce the risk that information is being sent insecurely.	Low	We will complete a register to identify the information that we transfer that will include the transfer methods and the information types. This will ensure that all data is transferred securely.

APPENDIX A: SCOPE

Scope of the review

To evaluate the adequacy of risk management and control within the system and the extent to which controls have been applied, with a view to providing an opinion. The scope was planned to provide assurance on the controls and mitigations in place relating to the following Risks:

Objective of the area under review	Risks relevant to the scope of the review	Risk Source
A system has been designed to ensure that computer, network resources and data are adequately protected from operational risk and security threats	Control weaknesses exist that result in a loss to systems integrity, confidentiality and availability.	Internal Audit

When planning the audit, the following areas for consideration and limitations were agreed:

Areas for consideration:

- Best practice standards compliance;
- IT infrastructure planning;
- End user governance and policy framework;
- Change and release management;
- Roles and responsibilities;
- Security control environment;
- Resilience control environment; and
- Configuration control.

Limitations to the scope of the audit assignment:

- The IT General Controls is a high level review covering some areas of risk within the IT control framework, its purpose to identify areas of immediate significant risk that in our opinion would benefit from specialist Technology Services (TS) review.
- The information provided in the final report should not be considered to detail all errors or risks that may currently or in the future exist within the IT environment, and it will be necessary for management to consider the results and make their own judgement on the risks affecting the Service and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised.
- The control of application systems is not included within the IT General Controls review.

FOR FURTHER INFORMATION CONTACT

Suzanne Lane, Senior Manager

Suzanne.lane@bakertilly.co.uk

01908 687800

rsmuk.com

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 11 Old Jewry, London EC2R 8DU. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM UK Consulting LLP, RSM Corporate Finance LLP, RSM Restructuring Advisory LLP, RSM Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP, RSM Employer Services Limited and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are members of the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. Baker Tilly Creditor Services LLP is authorised and regulated by the Financial Conduct Authority for credit-related regulated activities. RSM & Co (UK) Limited is authorised and regulated by the Financial Conduct Authority to conduct a range of investment business activities. Whilst every effort has been made to ensure accuracy, information contained in this communication may not be comprehensive and recipients should not act upon it without seeking professional advice.

© 2015 RSM UK Group LLP, all rights reserved