Strengthening resilience: lessons learnt from the impacts of the pandemic

February 2022

ANALYSIS OF INTERNAL AUDIT REVIEW OUTCOMES

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

EXECUTIVE SUMMARY

With the onset of the coronavirus pandemic, organisations have had to re-think, act quickly, and in many respects change how they have been operating. Throughout the pandemic we have seen a rise in fraud, cyber risk, supply chain disruption and economic uncertainty. These have been coupled with the adoption of homeworking arrangements and the relaxation of certain controls.

Following the initial onset of the pandemic, RSM's internal audit teams continued to undertake reviews, but in a remote setting. Our reviews have focused on our clients' responses to the pandemic and the lessons that were learnt, as well as issues around business continuity, agile and remote working, return to work and mental health. Just like many organisations across the UK, RSM has also had to work its way through the effects of the pandemic and adapt to the new ways of working while continuing to provide quality results for our clients.

Some audit plans were paused during the early stages of the pandemic, but many organisations were keen to restart their internal audit work given the importance of seeking assurance over the controls in place, particularly where new processes had been established at pace.

As part of RSM's approach to categorising internal audit findings, we agree low, medium and high priority management actions with our clients. A high management action is appropriate where there is a serious internal control or risk management issue, and where immediate attention is necessary.

Management actions in focus

As part of our research, we have analysed pandemic-related management actions that were agreed with our clients as part of internal audit reviews during the latter part of 2019/20 and 2020/21, including reviews of actions related to:

- business continuity;
- return to work;
- agile and remote working;
- coronavirus recovery;
- financial management;
- governance; and
- mental health and wellbeing.

This paper highlights the key outcomes from our reviews, and summarises the management actions agreed with our clients.

Overall, we have analysed 289 high, medium and low priority management actions agreed across 70 different reviews with a broad range of clients. Management actions were agreed with 63 organisations across the public and third sectors, and corporate organisations including several financial services businesses.

The 289 management actions covered by this report fall into one of four broad areas:

1. **business continuity;**
2. **secure remote working;**
3. **governance, risk and lessons learnt; and**
4. **people.**

PERCENTAGE OF AGREED MANAGEMENT ACTIONS

NUMBER OF HIGH, MEDIUM AND LOW MANAGEMENT ACTIONS AGREED

It is of note that all of the high-priority management actions that were agreed relate to business continuity and secure remote working. These actions are agreed where urgent attention is necessary as a result of a serious internal control or risk management issue that may lead to:

- substantial losses;
- violation of corporate strategies, policies or values;
- reputational damage;
- negative publicity in national or international media; and/or
- adverse regulatory impact, such as loss of operating licences or material fines.

A medium graded action is used where timely (but less immediate) action is needed as a result of an internal control risk management issue that could lead to:

- financial losses that could affect the effective function of a department;
- loss of controls or process being audited; and/or
- possible reputational damage, eg negative publicity in local or regional media.

We consider each of the four areas noted above in the following sections, concluding with specific sector context drawn from our regular reviews of the risks that sectors face and how these risks have changed during the pandemic.

Key findings

1

The majority of management actions we agreed related to business continuity (101 management actions) across all sectors that were a part of this review. The focus of management actions is on ensuring that plans and policies are reviewed and updated where necessary, and that key members of staff involved in the business continuity plan receive sufficient training.

2

The majority of secure remote working related management actions we agreed were related to security, IT systems and infrastructure, and policies and procedures. Other areas included training, risk assessments and equipment provision. From our reviews, only 12 per cent of organisations could take a substantial level of assurance that the controls in place to ensure secure remote working were operating effectively to manage risks.

3

Reviewing and updating risk assessments was a key area where we agreed management actions and ensured a stronger alignment and communication among boards, committees and other key risk management members regarding the challenges and opportunities created by the pandemic.

4

Very few organisations could have predicted that the pandemic would manifest as it has done, and organisations have had to move quickly to respond. In practice this has likely led to marked changes in risk appetite and often to significant changes in the control environment, as new or revised processes and procedures have been put in place. The need for both effective risk management and to gain assurance over internal controls has been magnified.

5

As hybrid working starts to become the 'new normal', organisations have had to pay particular attention to people; their health, safety and mental wellbeing, as well as their training and personal development. A host of factors should be considered in relation to employee wellbeing, including developing strategies and initiatives to engage and support staff as needed.

BUSINESS CONTINUITY

Following the uncertainty associated with coronavirus, organisations have reviewed their business continuity plans and ensured robust procedures are in place. Many organisations would not have had a global pandemic at the top of their risk registers, or even included one at all. While business continuity plans are designed to enable organisations to remain operational, the events that unfolded were far reaching, all-encompassing, and very difficult to navigate. As a result, many organisations have had to live test their disaster recovery arrangements and have incorporated learnings to ensure the robustness of their business continuity plans post-pandemic.

It is clearly essential for organisations to have an emergency plan to enable operational activity to continue, to respond quickly as events unfold, and to mitigate risks and their impacts.

Business continuity management covers risks to infrastructure, cyber operations, employees, business/operational activities and communication. Perhaps unsurprisingly, across all sectors that were a part of this review the majority of management actions we agreed were those relating to business continuity (101 management actions). In particular, the top three areas of management actions we agreed related to reviewing business continuity plans, training, and emergency planning. Other areas included effective testing of the business continuity plan, policies and strategies, impact analysis and disaster recovery.

The majority of management actions were issued to education clients (29 per cent) across seven reviews. However, our data indicates that the social housing sector seemed less well prepared. There were only two business continuity reviews for this sector as part of our analysis, yet business continuity-related management actions made up 16 per cent of the total for social housing.

SECTOR ANALYSIS ON BUSINESS CONTINUITY RELATED MANAGEMENT ACTIONS

- Education
- Social housing
- NHS
- Corporates
- Local government
- Central government
- Charity
- Emergency services
- Financial services

Summary of key themes

As part of our business continuity reviews, management actions we agreed included:

1. Delivering business continuity and disaster recovery training to key members of staff involved in the process, and providing related training to new members of staff with business continuity planning responsibilities as part of their induction.
2. Reviewing policies and strategies relating to business continuity, updating them where needed, and ensuring they are approved by the board.
3. Reviewing and updating business impact analysis and assessments to ensure they are reflective of current working practices.
4. More clearly identifying in business continuity plans the staff and equipment requirement in an emergency, and identifying the alternative arrangements to use should these staff members be absent.
5. Periodic testing of the business continuity plan and incorporating lessons learnt from the testing into the plan.
6. Revising IT business continuity and disaster recovery plans to incorporate a cyber resilience plan that would assist in the event of disaster or disruption to business-critical activities. A testing exercise is also needed to ensure the plan is fit for purpose in the event of disaster or disruption.

For many organisations, reviewing and updating business continuity plans was key to ensuring that, as far as possible, disruption was minimised and that resilience was strengthened. One of the common mistakes many organisations make is to think that resilience can be obtained by simply writing down comprehensive plans and procedures. But having a plan to deal with a major disruption is very different from being able to execute it.

We have seen many plans that suggest moving teams, personnel and operations to alternative locations or premises; that course of action has often been impossible due to the pandemic lockdown measures. In other words, very few, if any, business continuity plans envisaged large-scale home working.

SURVEY SNAPSHOT

Business continuity survey findings at a healthcare client

As part of one of our reviews, we surveyed staff and senior management at a large NHS Trust to understand their knowledge of business continuity plans in their area.

The business continuity survey received 147 responses. From the survey responses it was clear that not all staff knew how or where to locate their local business continuity plan. This is illustrated below.

Whilst this data is specific to one NHS Trust, organisations more generally may benefit from ensuring their business continuity arrangements have been effectively communicated.

SURVEY FINDINGS

- I know how to locate the business continuity plan for my area
- I know how to find central documentation and communications in regard to business continuity

Sector spotlight

The majority of management actions relating to business continuity were in education, social housing and NHS organisations.

EDUCATION

- Business continuity and critical incident policies should be reviewed and approved by the board.
- The IT team should complete the restructure of the IT infrastructure and then update the IT disaster recovery plan to include the new requirements.
- The testing of business continuity arrangements should be formally recorded, with results of the tests and any lessons learnt being reported to the risk management committee.

SOCIAL HOUSING

- The business continuity plan should be expanded to cover other scenarios, as well as the pandemic.
- Ensuring that Incident Management Team meetings cover the review and maintenance of the business continuity plan, and discussions need to take place on how often meetings should be conducted in response to different severity levels.
- A schedule to test the business continuity plan should be designed and implemented. The outcome of these tests will be reported to the board, and where necessary, acted upon.

NHS

- A copy of all local business continuity business plan tests and action plans should be held in a central location.
- There should be an action register to record the outcomes of local and trust wide business continuity plan testing.
- The Emergency Preparedness, Resilience and Response (EPRR) policy should be reviewed and updated to incorporate the lessons learnt from the coronavirus outbreak and how the current EPRR processes and controls can be improved.

KEY QUESTIONS FOR ORGANISATIONS TO CONSIDER

Does your organisation have assurance that business and critical incident policies have been approved by the board?

Do you have assurance that the business continuity plan reflects the lessons learnt from the pandemic?

Has business continuity training been rolled out to all key members of staff involved in the process, and to new members of staff with business continuity planning responsibilities?

SECURE REMOTE WORKING

Since the beginning of the coronavirus lockdown at the end of March 2020, many organisations have had to rapidly adapt to a large proportion of their workforce working entirely from home. Technology continues to facilitate the success of virtual working, and digital transformation has been a big focus for organisations, with the pandemic accelerating investment in all things digital. The world has harnessed the opportunities technology provides us, for example virtual meetings. There have been some benefits, including reduced costs, time savings, and beneficial environmental impacts. However, the pandemic has also offered opportunities for criminals to launch sophisticated and dangerous cyber- attacks.

The Chartered Institute of Internal Auditors' (IIA) annual analysis of the top business risks faced by organisations across Europe were cybersecurity and data security (79 per cent), regulatory change and compliance (59 per cent) and digitalisation, new technology and AI (50 per cent).

RSM's survey of the views of Heads of Internal Audit mirrored the findings presented by the IIA's analysis. It showed that cybersecurity was rated as the second-highest challenge for internal audit functions in 2021, the second-highest risk for the business, and the most selected area for inclusion in internal audit plans for 2021. The risks associated with data privacy and management were also rated highly by our surveyed Heads of Internal Audit.

Cybercrime is, of course, nothing new. But increased levels of connectivity, remote working, reliance on technology, and automation means the risk of attack is rising rapidly.

The pandemic has made many organisations more vulnerable to cyber-attacks because of:

- relaxed or more informal control environments;
- revised processes and procedures; and
- changing employee workforce profiles.

Remote and hybrid working are becoming the new normal, so organisations have had to carefully review policies and implement new ways of working to address some of the concerns around information security risks. It is more important than ever to ensure there are no technical barriers to effective working outside of the office environment.

The majority of secure remote working related management actions we agreed were related to security, IT systems and infrastructure and policies and procedures. Other areas included training, risk assessments and equipment provision.

From our reviews, only 12 per cent of organisations could take a substantial level of assurance that their controls to ensure secure remote working were operating effectively. This illustrates that many organisations have significant room to improve their IT control environments to:

- ensure data security;
- manage cyber-crime threats; and
- enhance IT operational effectiveness.

Find out more by browsing our report:
The Real Economy: Cyber Security — breaking the kill chain on The Real Economy **website** hub.

SURVEY SNAPSHOT

DO YOU KNOW HOW TO WORK SECURELY IN A HOME ENVIRONMENT?

A secure remote working survey shared with one of our emergency services clients received 1,025 responses. It showed that while the majority of respondents knew how to work securely in a remote setting, just under 20 per cent did not.

YOU FIND YOUR EMPLOYER'S INFORMATION SECURITY AND REMOTE WORKING POLICIES FRIENDLY AND EASY TO FOLLOW AND UNDERSTAND

When asked about the policies relating to secure remote working, over half of respondents 'strongly agreed' or 'agreed' that the employer's information security and remote working policies were easy to follow or understand.

However, interestingly a significant proportion of respondents stated that they 'don't know.'

Management actions — and questions to ask in your own organisation

Security

- User accounts with no password expiry date should be reviewed.
- In future, all machines where the security software showed as 'Not Protected' are properly accounted for and the justification for them being not protected should be adequate and formally documented.
- A risk analysis should be conducted to take into account the potential impact of unavailability of security logs in the event of an incident, to determine if further capacity for security logs is required.
- Firewall rulesets should be formally documented and reviewed on a periodic basis to ensure these offer the best possible security.

IT systems and infrastructure

- Management should identify the most critical and at-risk areas in the organisation's IT network and schedule an annual penetration test to assess its vulnerability.
- Ensuring that unsupported servers are segregated from the network (where possible), and that they are upgraded to supported solutions.
- All processes and procedures (eg standard build) need to be kept up to date to ensure these are an accurate representation of the IT environment and can be followed.
- A formal patching policy should be established to define how patching activities are performed across the IT estate.

Policies and strategies

Management should assess, review and update where necessary the following policies:

- OneDrive policy settings that allow for the sharing of links to information on OneDrive and who they can be shared with;
- IT Security Policies and the Social Media Policy to ensure they are understandable for staff;
- IT Usage Policy to reflect the current IT environment; and
- Remote Working Policy and Information Security Policy and Internet and Email Policy are updated to include the organisation's security requirements and procedures to follow when working remote.

Other areas

- Periodic cyber-security training should be provided for staff to raise awareness of the cyber-security threats they face and how to secure their working environment in a remote setting.
- A checklist for staff that can be used to verify whether staff have adequate equipment/home environment to facilitate working from home should be developed. Information should also be collected to identify what office equipment, remote access and software is needed.
- Routine spot checks need to be undertaken on completed risk assessments to ensure that they are reviewed and updated timely.
- An online assessment for all staff who work remotely to assess their home environments should be developed. A training package should also be designed to support remote working staff.

KEY QUESTIONS FOR ORGANISATIONS TO CONSIDER

Does your organisation have assurance that there is an effective and suitably robust IT infrastructure in place so that staff are able to work from home securely?

Are all policies relating to secure remote working up to date and easily accessible to staff?

Do you have oversight of your equipment and current records of where your IT assets are?

TECHNOLOGY: ENSURING ROBUSTNESS AND SUITABILITY

Technology will need to be factored into new and amended plans to ensure that both existing and new technology infrastructure can withstand another change in circumstance or continued remote working.

As more businesses move towards cloud-first and software as a service models, there will be a greater reliance on the robustness of technology infrastructure and on technology partners to provide reliable managed services and support.

Look out for our in-depth paper highlighting outcomes from our secure remote working and operational resilience reviews.

Key factors for consideration:

IT strategic plans that underpin future business planning, including digital transformation and introduction of emerging technology such as AI and RPA.

Reliance on key third parties, their financial and operational stability, and their continued ability to support the business.

Robustness of IT disaster recovery processes, including regular testing exercises.

To find out more, please visit
Business continuity management | Coronavirus: adapting to change | RSM UK

GOVERNANCE, RISK AND LESSONS LEARNT

Clearly, the pandemic has changed the way boards and committees operate, with decisions made remotely and with a particular focus on crisis management. While this has placed new demands on board and committee members, we have seen some positives emerge, such as enhanced efficiency as more people attend meetings virtually.

Until the pandemic, governance meetings have changed little since the start of the 20th century. Board and committee meetings have reflected this traditional model, even though how business is done and how we communicate has transformed beyond recognition. The pandemic has provided an opportunity to reflect on how we deliver governance and oversight in the longer term as we embrace both virtual and face-to-face meetings.

Few organisations would have predicted the pandemic to take hold as it has, and in response, organisations have had to move quickly, leading to changes in risk appetite. As new or revised processes and procedures have been put in place there have been significant changes to the control environment. This has magnified the need for effective risk management as well as the need to gain assurance over internal controls.

The August 2020 issue of the Global Institute of Internal Auditors' (IIA) Tone at the Top, 'The Board's Role in an Evolving Internal Audit Plan,' notes that risk assessments and audit plans will likely be very different in a post-pandemic environment. The IIA also states that the 'director's role in supporting development of an effective and responsive audit plan must account for changes in the speed of emerging risks, the disruptive impact of technology, and the ability of internal audit to provide effective independent assurance.'

A large proportion of the management actions we agreed as part of our reviews related to risk management and risk assessments. In particular, these related to reviewing and updating risk assessments and ensuring a stronger alignment and communication among boards, committees and other key risk management members on the challenges and opportunities created by the pandemic. As risk appetite may have changed during the pandemic, organisations also need to understand what their risk tolerances are now and, in addition, continue ensuring that risk registers (along with associated controls and assurances) are routinely updated.

From any crisis there are, of course, opportunities and learnings. Since March 2020 we have undertaken several 'lessons learnt' reviews, and we have agreed management actions related to wider organisational governance and risk management.

Management actions — and food for thought

Coronavirus lessons and responses

- Evaluate what went well during each wave of the pandemic as well as areas for improvement. The findings can be incorporated into working practices to help ensure the organisation is in a good position to meet any future challenges.
- Identify critical information that should be reported and reviewed by the governing bodies. This will enable effective reviews and decision-making, considering the changes in priorities and challenges as a result of the pandemic.
- Consider the effectiveness of governance processes and ensure lessons are applied to future incident management.

Board operation

- An annual report should be presented to the board, outlining any instances that triggered the business continuity plans and any near misses.
- Where a decision has been taken via email between meetings, confirmation of it should be in the minutes of the following meeting to be formally approved as part of the standing agenda item.
- The actions identified in the previous meeting should have a status update to confirm whether they have been completed and formally recorded in the minutes.

Risk management

- Risk assessments for current and emerging threats to business-critical activities should be reviewed and updated. Additionally, a dedicated risk owner should be allocated for each risk identified.
- Risk assessments should only be marked as completed with evidence to support the review being undertaken or appropriate communication to reject the risk assessment taking place.
- Organisations should update relevant coronavirus risk assessments and include reference to Display Screen Equipment (DSE) and homeworking to ensure that this has been considered in line with the Health and Safety Executive guidance.
- Organisations need to assess the risks relating to the pandemic, document mitigating controls and provide assurance to the audit committee that this risk is being effectively managed.

As part of our risk management culture reviews, between January 2020 and April 2021 we shared 20 surveys with senior management and board members across a wide range of sectors including healthcare, education, central and local government, social housing and charities. We put the following two statements to survey respondents, and the majority of them were positive about the way risks are being dealt with by senior management and the board:

THE BOARD PROVIDES CONSISTENT, COHERENT, SUSTAINED AND VISIBLE LEADERSHIP IN TERMS OF HOW THE ORGANISATION EXPECTS PEOPLE TO BEHAVE AND RESPOND WHEN DEALING WITH RISK

Percentage of 530 respondents

SIGNIFICANT RISKS ARE IDENTIFIED AND BROUGHT TO THE ATTENTION OF SENIOR MANAGEMENT AND THE BOARD

Percentage of 486 respondents

Some of our clients furloughed staff (as did RSM), particularly during the initial phase of the pandemic. Consequently, we have undertaken several furlough-specific reviews where we had agreed management actions.

KEY QUESTIONS FOR ORGANISATIONS TO CONSIDER

Does your organisation have assurance that risk assessments are frequently being reviewed and updated where necessary?

Has your organisation applied lessons that were learnt as a result of the pandemic to ensure you are able to meet any future challenges?

PEOPLE

As hybrid working starts to become the 'new normal', organisations have had to pay particular attention to people; their health, safety and mental wellbeing as well as their training and personal development. A host of factors should be considered in relation to employee wellbeing, including developing strategies and initiatives to engage and support staff.

Home working means that employers have an extended obligation to ensure that their employees are safe, and have a suitable workstation at home. As we move towards a long-term 'hybrid' working model, and for many people home working may become a permanent arrangement, it is good practice for employers to consider the Health and Safety Executive guidelines. A workspace should have a full health and safety risk assessment.

Management actions

Regarding people, we have agreed internal audit management actions regarding the need for:

- organisations to keep reviewing the support in place to ensure the health, safety and wellbeing of staff and take appropriate action where required. This includes raising staff awareness of the health and wellbeing resources available;
- homeworking health, safety and security self-assessment checklists to be completed;
- staff to complete the DSE assessment to ensure that they have a suitable working environment and, if necessary, they are able to request further equipment to improve their working space;
- health and wellbeing information and support for staff to be publicised and accessible;
- organisations to actively monitor coronavirus-related absences and provide support where required; and
- the Health and Safety Policy to be updated to include the processes for assessing risk for vulnerable persons.

Mental health and wellbeing

We all recognise the importance of wellbeing and mental health. Be it the nature of work undertaken, or working differently – perhaps in a remote setting – we all face personal challenges. In trying to understand these challenges, employee engagement is vital, as it allows employers to gauge whether measures put in place are effective and whether there is room for improvement. Following the onset of the pandemic, it is important to recognise how this has impacted mental health. Encouraging employees to maintain a positive work/life balance is key.

Managers regularly checking in with team members can help prevent feelings of isolation. Normalising conversations on employee wellbeing and having systems and tools in place to handle this is recommended. For example:

- offering benefits such as an employee assistance programme (EAP);
- introducing and embedding mental health first aid throughout the organisation; and
- ensuring absence management policies and procedures relating to mental health support the timely referral of employees to specialist health where appropriate.

SURVEY SNAPSHOT

An occupational health survey issued to one of our emergency services clients found that **almost a third** of respondents were not aware of the EAP service.

At a large NHS Trust, we asked 171 people whether there were effective channels in place to identify wellbeing concerns. In using data analytics tool sentiment analysis, just **11 per cent** of employees were positive in their response.

When asked, 'Do you feel your mental health has been impacted significantly during the coronavirus pandemic?,' just **7 per cent** gave anecdotal responses that were considered to display 'positive' sentiment.

For more information on each of these areas, please visit:
The intersection of COVID-19 and mental health | RSM Global

Environmental, social and governance

In some respects, coronavirus has amplified environmental, social and governance (ESG) concerns. Putting sustainable and responsible practices at the heart of the business is fast becoming a pivotal requirement for regulators, investors, and other stakeholders — especially after COP26. While profit will always and inevitably be a key indicator of success, it can no longer be the only benchmark. In relation to the environmental aspects of ESG, reducing travel will support many pledges made to become carbon zero within the next ten years and climate positive after that.

People are the most important asset of any business, and they sit at the core of the 'social' pillar of ESG. When developing an ESG strategy, or rethinking how your business impacts society, it is crucial to consider all your stakeholders' interests, from investors to employees. This will help secure a sustainable and inclusive future for your business, which is fundamental to an ESG strategy. The key things to consider for your social impact and value strategy are working conditions and employee relations and welfare.

Find out more on ESG on the **RSM's website**.

KEY QUESTIONS FOR ORGANISATIONS TO CONSIDER

Has your organisation developed hybrid / flexible working policies that both support staff and reflect business needs?

Has your organisation considered ways in which it will support Net Zero and tackle climate change?

Has your organisation begun its ESG journey, and have you considered your ESG maturity?

CONCLUSION

The challenges from the coronavirus pandemic have been evident across the diverse sectors we work with. We have seen enormous pressures for some of our clients, and many navigated them remarkably well. A myriad of learnings presented themselves throughout the pandemic, particularly in terms of a more ready embrace of technology, a fresh commitment to resilience and collaborative working, and a renewed focus on work/life balance. These learnings will continue for many organisations as we move into a recovery period.

Coronavirus has had a significant financial impact on many organisations. Although the government has put in place numerous measures to support businesses, some firms will continue to face the long-term effects of the pandemic.

Organisations have had to consider their future business models, shift to effective remote working, review how services are delivered, and bring forward enhanced digitalisation plans. All of this has resulted in an increasing need for assurance over a portfolio of risks that are not necessarily new, but where the likelihood of those risks occurring have increased significantly.

To understand what others are thinking and how organisations are responding to this challenging and evolving environment, RSM surveyed Heads of Internal Audit in the UK on their views about the challenges of coronavirus, the future changes for internal audit functions, and how organisations are managing risk and preparing for a potential UK SOX reporting environment.

The survey showed that the top three most significant challenges that arose for internal audit teams during the pandemic were:

1. providing assurance over key business areas when the business has other competing priorities;
2. maintaining visibility and presence while working remotely; and
3. retaining the ability to execute overseas work.

Providing an entirely remote internal audit service has presented challenges that we at RSM have not been immune to. Yet, throughout the pandemic we have worked closely with our clients to ensure we continue to provide assurances over key business risks.

The pandemic has impacted how organisations have addressed the management actions that were agreed with internal audit. There are also clear areas where internal audit functions will need to direct their focus to support businesses in 2022 including, for example, efficient risk management and routinely monitoring business continuity plans.

Audit plans will continue to remain agile. RSM has adapted – and will continue to adapt – our ways of working to respond to the needs of our clients. Many organisations will now be deciding which processes and procedures that were adopted or revised during the pandemic will remain in the longer term, and whether they will require assurance as to whether the controls in place are operating as intended.

FURTHER INFORMATION

Richard Smith
National Head of Risk Assurance and Public and Third sector
M: +44 (0)7398 168 960
E: richard.smith@rsmuk.com

Mark Jones
Head of Internal Audit, Risk Assurance
M: +44 (0)7768 952 387
E: mark.jones@rsmuk.com

Risk Assurance Technical Team
Research and author
E: technical.ra@rsmuk.com

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 50 Cannon Street, London EC4N 6JJ. 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 Corporate Finance LLP, RSM UK Restructuring Advisory LLP, RSM UK Risk Assurance Services LLP, RSM UK Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP, RSM Northern Ireland (UK) 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 licensed by 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. RSM UK Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317, to undertake reserved and non-reserved legal activities. It is not authorised under the Financial Services and Markets Act 2000 but is able in certain circumstances to offer a limited range of investment services because it is authorised and regulated by the Solicitors Regulation Authority and may provide investment services if they are an incidental part of the professional services that it has been engaged to provide. 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.

© 2022 RSM UK Group LLP, all rights reserved.