Compliance Best Practices For Working from Home

Tanya Raj and Manish Mohan Raj

Uncertain times call for unusual measures. As we have seen in the past few weeks, with the fast-developing situations around a global pandemic, businesses across the world are being called to relook at their working models. There is a need now, more than ever, to ensure that a business is fully functional, with minimal to no impact on work. With a large proportion of the workforce being asked to work remotely, there are obvious compliance concerns that crop up.

Compliance plays an integral role in supporting a firm's policies to meet regulatory requirements. As the Financial Conduct Authority (FCA) states on operational resilience, "Firms should take all reasonable steps to meet the regulatory obligations, which are in place to protect their consumers and maintain market integrity. The firm should establish appropriate systems and controls to ensure it maintains appropriate records, including call recordings if required." Here, we aim to list certain compliance best practices for employees to adhere to when working from home, executing a business continuity plan (BCP).

Confidentiality

Each company's data is its intellectual property, and maintaining confidentiality during a BCP situation is of utmost importance. The use of company-approved systems and virtual desktops helps mitigate risk. During business disruptions, therefore, it is imperative to reiterate the importance of employees using only company-approved systems. It is easy to lose track of compliance requirements during a business disruption; hence, it is critical that compliance programmes are robust and diligence is heightened during such times.

- There should be clear guidance provided on using the company's email system versus personal email systems
- Employees should refrain from sending company documents to personal email addresses
- Employees should not conduct any company business via personal email accounts
- Any exception would require approval from the respective employee's managers and the Compliance and Information Security teams

Regulatory requirements

It is also imperative that employees who are required by regulation to, for example, conduct business via recorded phone lines do so. These are mandatory rules put in place to mitigate risks of conflict of interest, inappropriate trading practices, and market manipulation. To adhere to such requirements during a BCP event,

- There should be clear guidance on the appropriate use of personal phone connections
- Employees can be provided with company-approved equipment to be installed at home to continue making business-related calls
- If company-approved equipment cannot be provided, the Compliance team should act as a chaperone on business-related calls

Ring-fencing

Employees should also be mindful of other best practices when working from home:

- It is important to understand that working from home implies “home”; company business should never be conducted from cafes, internet hubs, airports, libraries, or other public spaces
- When at home, the working area/screen should be ring-fenced from other members of the family to avoid inadvertent leakage of confidential information
- No material should be printed at home, unless employees have explicit remote printing approval from their respective managers, and the Compliance and Information Security teams
- Team and client calls should be treated with the same confidentiality as in the office environment, and the “don’t ask, don’t tell” policy should be practised
- When in doubt, and before taking any steps, employees should check in with their respective managers or the Compliance team

While the above mentioned steps are basic to setting up a robust compliance programme during a BCP event, it is critical that the Compliance team ensure employees have been provided with adequate training on privacy and confidentiality, and a set of specific guidelines, to effectively and efficiently work from home. The effectiveness of a company’s programme and adherence to regulatory obligations will be tested by its resilient compliance structure and effective ongoing monitoring.

We believe COVID-19 will have a deep impact on how we do business around the world. During these testing times, the Compliance team needs to continue to take all steps to prevent market abuse risks and enhance review and monitoring programmes to abide by both the letter and the spirit of the law.

Here is where Acuity Knowledge Partners can help you navigate through these challenging times. With our focused set of offerings in the areas of Corporate Compliance, Forensic Analysis, Compliance Testing, Monitoring Programmes, Risk Trend Analysis, and Risk Mitigation, we customise and design reviews dedicated to mitigating your firm’s risks, keeping the latest regulatory expectations in mind. We believe a well thought-through approach – from initial analysis to end

documentation and recommendation – will provide you with a holistic view of your business's risks and build its resilience to any threat.

To help our clients navigate both the people and business impact of COVID-19, we have created a dedicated hub containing a variety of topics including our latest thinking, thought leadership content and action oriented guides and best practices.

About Acuity Knowledge Partners

Acuity Knowledge Partners is a leading provider of high-value research, analytics and business intelligence to the financial services sector. The company supports over 400+ financial institutions and consulting companies through a team of over 4,000+ subject matter experts who work as an extension of the clients' teams based out of various global delivery centres.

We empower our clients to drive revenues higher. We innovate using our proprietary technology and automation solutions. We enable our clients to transform their operating model and cost base.

contact@acuitykp.com | ***acuitykp.com***