Essential Strategies for Secure Administration: Proactively Managing Risk

Karen Malone October 8, 2024

As administration becomes more complex and regulatory landscapes more demanding, fund managers must adopt a proactive approach to risk management.

Secure administration is about more than just responding to regulatory requirements; it involves building resilient systems, safeguarding data and ensuring that operations run smoothly across the board. By focusing on these key strategies, fund managers can enhance operational security while also addressing potential risks in a structured way.

1. Risk Assessment and Due Diligence

Administrators must prioritise a robust risk assessment framework to help fund managers identify vulnerabilities, whether in cybersecurity, third-party interactions, or internal operations. Regular risk evaluations are essential, enabling administrators to support fund managers by pinpointing areas that need attention.

One of the most pressing concerns is cybersecurity, as the frequency and sophistication of cyber-attacks continue to rise. Administrators implement secure systems to prevent data breaches, ensuring that fund managers' sensitive financial information remains safeguarded.

In addition to cybersecurity, administrators must ensure comprehensive due diligence for regulatory compliance. Keeping fund managers informed and up-to-date with evolving regulatory frameworks is essential to avoid penalties and align with the requirements of bodies such as the SEC and FCA. This ties into regulatory risks, ensuring compliance strategies are continually reviewed and adapted to meet new regulations.

By continuously reviewing their own systems and developing strategies to prevent, detect and respond to threats, administrators can ensure that fund managers remain secure and compliant with industry standards.

2. Data Governance and Cybersecurity Vigilance

Administrators must establish and maintain robust data governance policies to ensure that the data they manage for fund managers is accurate, accessible and secure. These policies should evolve as both security needs and data management systems change over time to ensure the ongoing protection of critical information.

Additionally, cybersecurity vigilance is not just about policy but active oversight. Administrators need to regularly update security systems, educate staff on recognising cyber threats and implement quick-detection systems for breaches. This protects against technology failures and enhances operational resilience.

By investing in scenario analysis and stress testing, administrators can help fund managers understand how their portfolios and administrative systems might respond to adverse conditions. This allows administrators to mitigate risks and maintain operational stability during a crisis.

3. Organisational Flexibility and Change Management

Internal changes, whether personnel shifts or broader organisational restructuring, can significantly affect a fund's operations. Administrators play a key role in ensuring that such changes are managed without disrupting fund managers' day-to-day operations.

Implementing clear change management strategies ensures that any transitions within the administration framework do not negatively impact the fund's security, operational integrity, or compliance with third-party and regulatory processes.

4. Managing Third-Party Risks: Ensuring Control Over Outsourced Services

Administrators often rely on third-party service providers to handle essential tasks, but this practice introduces risk. Administrators must manage these third-party risks by conducting thorough due diligence on all external vendors, ensuring that they meet strict compliance and security standards.

Establishing clear service level agreements (SLAs) is critical. These agreements hold third-party providers accountable, while regular assessments of their security practices help prevent data breaches and ensure consistent operational performance. Administrators' oversight of third-party providers ensures that fund managers can trust the quality and security of outsourced services.

5. Technology and Automation: Enhancing Efficiency While Mitigating Risk

While administrators leverage technology and automation to enhance efficiency, they must be aware of the risks these systems introduce. System outages or malfunctions can lead to operational disruptions, making it crucial for administrators to develop comprehensive business continuity and disaster recovery plans.

Regular testing of these plans ensures that they are effective, helping fund managers remain prepared for any technological disruptions. Administrators must balance the benefits of automation with strong risk management frameworks to maintain operational security while continuing to streamline processes for fund managers.

Best Practices in Administration: Ensuring Security and Compliance

To enhance operational security, Waystone implements robust frameworks and processes that focus on compliance, data integrity and technology resilience. By prioritising security, fund managers can maintain the trust of their investors and ensure the long-term stability of their funds. As the demands of the investment landscape grow, it is crucial for administrators to adapt to these changes and safeguard against risks through strategic oversight and operational diligence.

Karen Malone, Global Product Head - Administration Solutions, emphasises the importance of information security and operational due diligence. "*As administration becomes increasingly complex, savvy managers must ensure that they stay ahead of industry challenges. At Waystone, we consistently review our processes and controls to safeguard both our clients' interests and those of their stakeholders*." This commitment to security is reflected in Waystone's ongoing efforts to enhance risk management strategies and ensure that they deliver industry-leading services.

If you have any questions or would like to sign-up to receive our communications, please contact Karen Malone or your usual Waystone representative via the below.

Contact Us →