

Forty Years of Industry Leadership: DST Systems

DST Systems, Inc. this year celebrates 40 years of providing market-leading solutions to the mutual fund industry. In recognition of this milestone, *Money Management Executive* asked DST's senior leadership to identify ways investment management companies can maximize the value they deliver to their stakeholders by leveraging the strengths and resources of a service provider.

This special three-part series looks at how service providers support investment management companies as they seek to manage expenses, improve efficiencies, mitigate risks, distribute their products and help ensure shareholder satisfaction.

Part 1 of the series, about managing expenses and efficiencies, is available at www.dstsystems.com, or in the June 29 issue of *Money Management Executive*. Part 2 of this series focuses on mitigating risks related to security, privacy, operations and regulation.

Managing Risks, Adding Value

Regardless of economic conditions, investment management firms are keenly aware of risks facing their organizations. They are concerned not only with their investment risk strategies, but with their ability to manage operational risks involving security, privacy and regulatory issues. While firms typically have deep risk-management expertise, many find that by working closely with a third-party service provider, they can demonstrate an even stronger risk assessment and management process.

"Firms looking to outsource technology or services should understand how their service provider can help them mitigate

risk," said **Steve Hooley**, president and chief operating officer of DST Systems.

"DST's ability to support risk management begins with a strong corporate culture of risk awareness," Hooley said. "We have the scale to devote technology, people and processes to helping clients mitigate risk. We have robust systems designed to monitor and help protect against threats to critical information. And we deliver standardized processes and automated functions to help reduce the risk of human error. Our clients leverage these strengths in their risk management programs."



Steve Hooley

Privacy, Security and Operational Risk Mitigation

Shareholders have a fundamental expectation that their personal privacy will be protected and that the electronic environment in which their trades are processed is stable and secure.

"Safeguarding privacy, security and stability should be central to a service provider's offering," said **Mark Prasifka**, DST's chief information officer.

Prasifka said that DST reviews both external and internal threats to information security and privacy. External threats to shareholder information can include outsider attempts to break into data storage environments, intercept data transmissions or infiltrate e-commerce or Internet applications. Managing external threats is critical, and some of the main strategies include firewalls, use of encrypted communications lines, as well as public key/private key encryption of files to be transmitted.

"The online environment should undergo an extra level of scrutiny," said Prasifka. "All customer-facing applications within

DST are SSL [secure socket layer] encrypted, and regularly assessed for adherence to security standards and baselines. We also use intrusion detection technology to monitor for extraordinary activity on our network."

Another important security measure is safeguarding portable or remote access to shareholder information. Prasifka noted that DST policy prohibits shareholder information from being physically stored on laptops or other unsecured portable media. He said that remote access should be protected using "strong" or multi-factor authentication, rather than a simple user name and password.

Additionally, it is vital to look at internal risks, such as those that may be introduced within the processing environment. Prasifka said that DST's TA2000® record-keeping platform features internal controls designed to limit access to protected information.

DST defines which individuals have access to shareholder information, as well as specific approval processes for extending additional access. DST's automated business process management tool, AWD®, can mask Social Security and credit card numbers, so that processors have access only to the information they need to do their work. DST also provides clients with audit trails that show who within their shops has access, so they can determine whether user access designations are still appropriate.

Managing Disaster Recovery

The potential impact of a natural disaster, terrorism or human error on shareholder information has driven investment management companies of all sizes to focus greater attention on disaster recovery.

"We view disaster recovery as part of our core transfer agency operations," said **Ed Eiskina**, vice president with responsibility for DST's Winchester Data Center.

To this end, DST has invested in re-

dundant, synchronized recovery facilities in which all critical applications and systems are matched one-to-one with its primary centers. DST utilizes mirroring technologies for its mainframe and open systems platforms, coupled with connectivity through high-capacity, private networks. Because DST owns both data centers, the Winchester Data center in Kansas City Mo., and a recovery data center in St. Louis, Mo., there is no contention for resources. In the event of an incident, DST has recovery time objectives to restart production at full capacity within four hours.

“Effective disaster recovery is more than just having the facilities in place. A key component of effective disaster recovery is testing,” said Eiskina. “We commit to testing at least eight times a year—but we generally test dozens of times a year. Disaster recovery is not an afterthought. It is ingrained in the day-to-day management of our systems and applications.”

Having a disaster recovery model in place helps investment management companies meet regulatory obligations and maintain service levels and investor confidence, according to Eiskina.

Regulatory Risk

In addition to security and operations risks, investment management firms are concerned with risks related to regulatory issues. Keeping up with a dynamic regulatory and legal landscape poses significant challenges. Service providers should demonstrate a commitment to helping firms remain compliant with current regulations and legislation.

Part of that commitment is reflected in the way service providers structure their approach to compliance, said **Jeff Cook**, DST’s director of regulatory compliance.

“Compliance support is not a part-time responsibility,” said Cook. “It’s a key function that requires senior management and a staff to implement initiatives.”

DST maintains a regulatory compliance staff, as well as a separate regulatory services team and a transfer agent control group. The regulatory compliance staff

monitors regulatory and legislative activity and works to identify systems and operations requirements. The regulatory services group executes technology development, while the control group implements operational practices and procedures within DST’s full-service transfer agency. This segregation of functions demonstrates that helping clients with compliance remains a development and operational priority, according to Cook.

Another example of a service provider’s regulatory commitment is its approach to interpreting and acting upon regulations and legislation. Investment management firms must not only understand what the new regulations and laws entail, but also have a well-considered strategy for addressing them through business processes and technology solutions.

DST’s Regulatory Compliance Advisory Group, or RCAG, is a forum comprised of regulatory and operations professionals from DST and its client companies. The RCAG works to interpret regulations and legislation, evaluate system impacts and look for consensus on how to implement compliance solutions.

“For each regulation, there may be multiple interpretations or solutions, so it is important to have a broad cross section of the industry represented on the DST RCAG,” said Cook. “Bringing together clients that represent a wide variety of fund sizes, business models and priorities enables us to consider various probable interpretations of a given regulation.”

Service providers can deliver another level of regulatory support by representing their clients’ perspectives as regulations are proposed and considered. DST speaks to the needs and priorities of clients on task forces and committees with industry organizations such as the **Investment Company Institute (ICI)**, **National Investment Company Service Association (NICSA)** and **Security Traders Association (STA)**.

“We are solicited to represent the views of our large and diverse client base as these organizations draft responses to regula-

tory proposals,” said Cook. “For example, we are represented on four ICI committees that are evaluating and making recommendations regarding the new mandatory cost basis reporting law.”

Investment managers can look to their service provider to support their fund board and chief compliance officer (CCO), as well. Since the implementation of SEC Rule 38a-1, the relationship between service providers and fund boards has become increasingly important. DST works to support fund boards’ due diligence processes in overseeing regulatory compliance.

“By demonstrating compliance with certain rules, we assist our clients in meeting third-party service provider due diligence requirements,” said Cook. “When the **Federal Trade Commission (FTC)** came out with its ‘Red Flags’ rule, for instance, we developed an identity-theft prevention program that demonstrated compliance, which enabled our clients to perform their service provider due diligence.”

Leveraging Scale And Strength

Robust risk assessment and mitigation are critical to investment management companies’ goals of maintaining privacy, security and stability, as well as regulatory compliance. Firms that keep operations, including risk management, entirely in-house must devote significant resources to building and maintaining the teams, technology and processes needed to meet these requirements.

“Risk management can be expensive and pose operational challenges. Working with a service provider can alleviate the burden of maintaining operations that are separate from a firm’s core competencies,” said DST President and COO Hooley.

“By leveraging the scale, technology and operational expertise of a long-standing industry leader, these firms will likely be in a much better position to protect and provide value to their shareholders,” he said.

MIME

888.DST.INFO ■

Investment Management Solutions ■ International Shareholder & Investor Recordkeeping
Brokerage Subaccounting Solutions ■ Business Process Management Solutions ■ Healthcare Solutions ■ Wealth Management Solutions