Information Technology Operations

Introduction to the Role of Technology in Operations

As with most businesses in the modern era, information technology (IT) has played an increasingly important role in the day-to-day operations of alternative investment fund managers in recent years. The impact on technology can be seen on improving the efficiency of traditional fund operations in existing processes such as fund accounting or trade reconciliation. Information technology has also allowed funds to change the ways they do business through the use of automated trading algorithms and near-real-time risk management of investment risks. Increasingly, information technology has evolved to support the growing scope of complex compliance challenges facing alternative investment managers. As we outlined in Chap. 4, examples of this included the use of technology for ongoing compliance monitoring of electronic communications and for data archiving and regulatory reporting. In this chapter, we will focus on some of the more common operational processes in which information technology is utilized.

Information Security Policy

Increasingly, in order to maintain more consistent procedures and policies records from a compliance perspective, many alternative investment fund managers are documenting information technology policies as part of their
overall compliance program. A key focus of this documentation is in the area of information security. Many times, this information may be incorporated into the firm’s compliance manual; however, in some cases a fund manager may develop a stand-alone information security policy (ISP). These policies can cover a wide variety of topics including the following:

- Data protection, retention and disposal
- An overview of data access rights and the process by which employees can request to access restricted data
- Computer and laptop security protocols
- Login password requirements
- Software licensing and usage guidelines
- Data encryption standards and procedures
- Guidelines for the use of wireless networks

Similar to the way that many regulators require registered alternative investment asset managers to perform annual compliance training for employees, increasingly many firms are requiring employees to undergo mandatory information security training. This training is often provided for new employees during orientation as well as more formally throughout the year.

**Information Technology Consultants**

Within the alternative investment manager, the information technology function may be led by an individual with the title of chief technology officer (CTO). In some cases, a fund manager may not maintain an individual with the stand-alone CTO title but, instead, the duties of the CTO would be housed under an individual with another title with operational responsibilities encompassing the information technology function as well as other operational duties. Examples of such titles would be chief operating officer (COO) and chief financial officer (CFO). Depending on the size of the fund manager, they may have a number of in-house staff focused on various aspects of information technology ranging from infrastructure and hardware to software development and support. As with most operational functions today, it is now common for a fund manager to utilize a combination of both in-house and external resources to support the information technology function.

Alternative investment managers utilize information technology consultants in a wide variety of capacities. Historically, many fund managers had a great deal of physical infrastructure hardware such as servers and networking
equipment in their offices. Today, the bulk of alternative investment managers utilize information technology vendors’ off-site cloud-based services, which has significantly reduced the need for this volume of equipment. This often includes a mix of both public and private cloud options to best balance the needs for security and data storage capacity while managing expenses for such services.

Once a fund has been established and is up and running, technology consultants also can provide ongoing services. These services include serving as a helpdesk in the event technology issues should arise and performing ongoing monitoring and maintenance of any on-site hardware in the fund managers’ offices. In some cases, a fund manager may also seek to develop either a customized software to be incorporated into an existing application or a brand new piece of software to perform specific tasks.

While some fund manager do maintain software developers on staff, in many cases fund managers find it more efficient to outsource this work to third-party consultants. An example of this would be a fund manager that wishes to create a software that creates custom reports that can be utilized based on data from an off-the-shelf account system. Additionally, software developers may also perform ongoing updates and revisions to existing software. In many cases, a fund’s information security policy will outline the firm’s specific procedures by which software changes should be requested and initiated, testing should be done, and, finally, the new change should be implemented. In many cases, funds will utilize something called a sandbox testing environment to isolate the newly written code and test it before rolling it out to a live environment. The process and timing of the use of a sandbox would be an example of something that would be covered in the information security policy. Information technology consultants with specialized knowledge of certain systems may also be utilized to work on upgrades of enterprise wide systems. In the alternative investment space, this is often commonplace with complex legacy fund accounting systems.

Data Rooms

Increasingly fund managers utilize technology called data rooms. A data room is an Internet-based storehouse where information can be kept. Today, most data rooms are cloud based. The purpose of a data room is not only to facilitate the storage of historical fund data but also to assist funds in exchanging it with current and prospective investors. In many cases, a prospective investor will be directed by a fund manager to a data room in order to obtain a variety
of pre-investment due diligence materials. On a post-investment basis, an investor may be directed to a data room to pull revised fund materials such as the latest fund risk reports. Information technology consultants often assist fund managers in selecting and utilizing data room solutions.

**Cybersecurity**

While the increased use of information technology among alternative investment managers provides many advantages, there are also a series of new and increased risks associated with its use. One of the biggest risks relates to the area of cybercrime. Cybersecurity can be defined as the risks associated with maintaining the integrity of an alternative investment manager’s information technology infrastructure and data from unauthorized access of theft. When discussing cybersecurity, the first notion that comes to many people’s minds are thoughts of clandestine hackers in remote countries launching virtual attacks again major companies to steal corporate intellectual property or individuals’ credit card numbers. Alternative investment managers are also subject to cyberattacks. They make attractive targets to thieves for a variety of reasons including the wealth of intellectual property they maintain in the form of things such as proprietary trading algorithms, and the sensitive investor information and contact details that they maintain. Additionally, alternative investment managers are very sensitive to the negative effects of reputational damage to their firms that could occur in the event sensitive firm data were to leak and, therefore, might be good targets for cybercriminals to launch ransomware attacks on. A *ransomware attack* is a type of cyberattack where a hacker restricts a company’s access to their own information and requires compensation, typically in the form of cash or virtual currency such as Bitcoin, in exchange for providing them access back or agreeing not to publish the information.

**Penetration Testing**

A penetration test is a way for an alternative investment manager to test for any weaknesses in an information security framework. In many cases, an alternative investment manager will hire a third-party technology consultant that specializes in penetration testing to perform the test. The manager may also perform their own penetration testing as well. The process of performing a penetration test is similar to a regulatory mock audit, except in this case the
goal is to prevent cyberattacks as opposed to prepare for regulatory audits. The penetration testing exercise attempts to simulate the actions of someone with the goal of performing cybercrime. This could either be a third-party individual such as a hacker or be someone from within the firm such as an employee attempting to steal firm data.

Software Patches

Another key element of cybersecurity is ongoing software maintenance. In many cases, when a new version of a software program is released, it is to repair a vulnerability that had been uncovered in a previous version of the software. If a fund manager is slow to update the software with the latest update, often called a patch, then this vulnerability could be exploited.

A historical example of this was the 2017 WannaCry attack utilizing a specific type of ransomware attack called a cryptoworm to exploit unpatched software. In the case of WannaCry and other cyberattacks such as the 2017 EternalBlue attack, a specific type of attack called Botnets was utilized. Botnets are networks of personal computers that are linked together in a clandestine way and then secretly controlled by the hacker to execute the cyberattack. In many cases, the patch process can be automated to pull new patches from software vendors once released. Despite this, automation manual oversight of the process is also recommended in order to ensure that the automated processes do not miss any critical patches. As part of this process, many information technology consultants perform ongoing patch supervision, which will prepare a patch report detailing what patches were updated as well as the date since the last patch of critical software applications. Therefore, it is important for either in-house or third-party information technology consultants to perform ongoing monitoring for software updates and patches.

Vendor Cybersecurity Analysis

As outlined in Chap. 5, alternative investment managers work with a wide variety of third-party service providers. These service providers maintain their own information technology infrastructures and are also subject to cybersecurity risks in the same way that the fund managers they provide services too are. Increasingly, before beginning a new relationship with a service provider, fund managers are devoting more efforts to analyzing the cybersecurity protocols in place at vendors. A large motivation for this is the increased regulatory
scrutiny that has been placed in this area. Under regulations such as the European Union’s General Data Protection Regulation (GDPR), fund managers can be held responsible for data breaches that take place at vendors under certain conditions. An example of how this would work in practice would be if a hedge fund manager works with a third-party administrator. If the administrator was subject to a data breach where the personal information of the hedge fund’s investors was stolen, then under GDPR the hedge fund would have obligations to notify these investors of the breach and may also be exposed to financial penalties under the regulation. To be clear, in this example the hedge fund had nothing to do with the attack at the fund administrator, yet they still have obligations and potential liabilities because of it. Due to the potential for scenarios such as this, fund managers have developed a number of approaches to assess cybersecurity risks at vendors during the onboarding process. The specific steps taken by the fund manager in this regard often include the following:

- Sending the vendor a questionnaire to complete regarding their cybersecurity preparedness
- Conducting on-site or remote interviews with a vendor’s in-house information technology personnel
- Evaluating the use of standard deterrence technology such as firewalls, analyzing the backup and storage of sensitive data
- Analyzing the use of any third-party information technology consultants
- Understanding if the vendor has a plan in place should a data breach occur

Business Continuity and Disaster Recovery

Business continuity planning and disaster recovery (BCP/DR) refers to the procedures and policies an alternative investment manager has in place in the event of a material business disruption. This business disruption can be temporary in nature or more long term. Examples of short-term business disruptions may include the temporary failure of Internet connectivity from a fund manager’s office, a short-term power outage that causes a fund manager’s office to lose electricity, and a small fire or a plumbing incident that causes employees to be out of the office for a day or two. Longer-term business disruptions are usually related to disaster-type events such as weather events like Hurricane Sandy and the 2019 Novel Coronavirus (COVID-19), which we referenced in Chap. 4.
Due to the vital nature of a fund manager being able to continue to manage investments and communicate with investors during times of crisis, BCP/DR planning has become increasingly an important part of a firm’s operations. Oftentimes, the information technology function of an alternative asset manager is tasked with coordinating the implementation of BCP/DR plans. Oftentimes, in practice the work of the technology function in this regard is performing in coordination with other parts of the firm including the investment function and the compliance department. Many firms also develop a stand-alone business continuity and disaster recovery committee that is responsible for overseeing the implementation of BCP/DR plans. Compliance is also usually integral toward assisting the firm in developing a document known as a business continuity and disaster recovery plan.

Financial regulators are also increasingly requiring that alternative investment managers develop written BCP/DR plans. In the United States, the Securities and Exchange Commission (SEC), with regard to Rule 206(4)-7, outlines in part:

> We believe that an adviser’s fiduciary obligation to its clients includes the obligation to take steps to protect the clients’ interests from being placed at risk as a result of the adviser’s inability to provide advisory services after, for example, a natural disaster or, in the case of some smaller firms, the death of the owner or key personnel. The clients of an adviser that is engaged in the active management of their assets would ordinarily be placed at risk if the adviser ceased operations.

Similarly, the National Futures Association (NFA) Compliance Rule 2-38 outlines that funds registered with the NFA are required to adopt business continuity and disaster recovery plans. Similarly, the UK’s Financial Conduct Authority (FCA) Handbook in section SYSC 3.2.19 outlines that:

> A firm should have in place appropriate arrangements, having regard to the nature, scale and complexity of its business, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption. These arrangements should be regularly updated and tested to ensure their effectiveness.

The development of a BCP/DR plan usually addresses a wide variety of aspects of a firm’s plan for continued operation. One of the key areas that many asset managers plan for in the event of a business disruption is a way for employees to stay in touch and communicate when they cannot be physically
present in the office. Plans in this regard often include instructions for employees to pass on information via email or through phone calling trees, alternative web portals that can be utilized to access the firm’s systems remotely through virtually secure access, emergency contact details for employees, instructions for how to continue trading for approved employees from outside the office and instructions for how to use methods of communication such as video conferencing technologies. The following is an example of a sample language that would be contained in a BCP/DR plan with regards to a fund manager’s communication plan in the event of a business disruption:

The firm will communicate with employees via a communications tree. This tree includes several different means of communication including phone numbers (mobile and home) and individual employee personal email addresses. Additionally, in the event of a disruption, all firm staff will be required to attend a virtual conference call at 10:15 am, Monday through Friday. The information for this conference call is as follows:

   Participant Access Code: 55555
   Conference Dial-In Number: (555) 555-5555

   All employees have a listing of cellphone and home phone information electronically and in hard copy. Additionally, senior management each maintains a detail list of contact information for all material vendors in hard copy and electronic format at their residences.

Another item typically covered in BCP/DR plans is the designation of an alternative location from which employees may continue operations. This could include designating a formal location, known as a disruption gathering location. This is a location where employees would be directed to go in the event of a business disruption where the fund manager’s office could not be accessed. The following is a sample excerpt from a BCP/DR plan with regards to the language that would commonly be seen in relation to a fund manager’s office closure and remote working of employees:

In the event of a significant business disruption that necessitates an office closure or evacuation, employees will utilize employee residences as alternate physical work locations. All employees either have desktop computers and/or laptops set up at home that are used for remote access. Currently each employee can access the firm’s network (including all applications) from home via secure virtual private network (VPN).

The firm has made the determination that mission critical business processes can all be supported effectively by a remote workforce with access to the Internet and telephony services. In the event of a significant long-term business disrup-
tion or outage of the firm’s facilities, it will be the determination of the manage-
ment as to whether or not the procurement of alternate physical workspace for
use on either a temporary or long-term basis will be made.

BCP/DR plans also typically address the ways by which data will be
archived so that in the event of a business disruption it would be accessible.
Today it is considered best practice for fund managers in most situations to
typically archive data on as close to real-time basis as possible. As noted above,
in modern alternative investment fund managers the majority of data is stored
off-site via the cloud; however, some firms may still use physical on-site back-
ups as well for legacy reasons. In addition to data backup plans, BCP/DR
plans will also typically detail the ways in which data can be accessed remotely
in a secure way such as via a Secure Sockets Layer (SSL) connection.

Some of the other important considerations that should generally be
addressed when evaluating what a BCP/DR should cover include the
following:

- Are BCP/DR plans based on any industry certifications or guidelines?
- Are BCP/DR focused on a small list of specific events or do plans cover
  multiple scenarios?
- What does the plan cover in regards to outages of telephony and
  Internet loss?
- When a BCP/DR plan requires updating, who oversees updating the plans?
- Is separate office space maintained where employees could continue opera-
  tions? If yes, how many seats are in such locations? If not, are employee
  expected to work from home?
- In the event that the fund manager has more than one office, what is the
  plan for employees from the different office to support each other to coor-
  dinate recovery efforts?

Earlier in this chapter, we discussed the role of information technology
consultants and the cloud in supporting data archiving. The storage and access
to data in the event of a BCP/DR event is another key consideration that is
important to BCP/DR plans. Two key questions that should be considered
when designing a BCP/DR plan with regards to data management are: How
would employees be able to access data remotely and is this data storage and
access secure? Another key consideration is the time frame involved in under-
going a data restoration. For example, if a disaster event occurs during the end
of quarter when investor statements are due and it takes the hedge fund five
days to perform a full data restore of their fund accounting system, this would
likely cause a delay in the production of the fund manager’s net asset value calculation and subsequent investor statements.

When a business disruption or a disaster event does occur, many funds then undergo a post-crisis evaluation to determine what lessons were learned from the event. In this way, the firm can determine what deficiencies may have been present in their current BCP/DR planning and how those weaknesses could be improved upon going forward. In many cases, failures of BCP/DR plan implementation come about not due to the failure of technology but rather due to human oversight.

A classic example of this is that of an alternative investment manager whose office becomes inaccessible due to a business disruption. The manager would have a robust BCP/DR plan in place. As part of this plan when such a business disruption were to occur, employees would work from home. The BCP/DR plan includes detailed instructions by which employees can securely access the firm’s network under a work-from-home situation. The problem is that when an employee sits down to access the network, they realize they do not know their login password. Let us further assume that they do not have the phone number or email of the IT department or consultant, since it is stored on the computer. This failure of the BCP/DR plan, therefore, has nothing to do with the technology in place but is a result of simple human oversight. This example highlights the importance of not only drafting and implementing detailed BCP/DR plans, but also the need for testing these plans on a regular basis. When such tests are implemented, often issues such as an employee forgetting their login password become more apparent than merely by performing technology-based tests of plans. The following is sample language from an example of BCP/DR plan with regards to testing and plan updates:

The fund manager anticipates that updates to the BCP/DR plans will take place whenever there are material changes to fund operations. Additionally, the BCP/DR committee will audit and review this plan on at least an annual basis for accuracy. Plan testing will be performed both in-house and by the firm’s external information technology vendor. Formal testing will occur on at least an annual basis however, management recognizes the need and benefit for more frequent testing as well and will endeavor to do so at their discretion. Annual testing will include power and internet failover simulations as well as file server failure simulations. Training will also be conducted for each employee with regards to BCP/DR plans. Management will utilize the results of testing to improve BCP/DR planning at least annually. Additionally, on at least an annual basis employees will be required to attest that they have read and understand the firm’s BCP/DR plans.
It should also be noted that similar to the vendor oversight of cybersecurity efforts, increasingly alternative investment managers are focused on the BCP/DR plans of their service providers. A key reason for this is that a disruption in the services provided by a key service provider, such as a prime broker, could directly impact the ability of the fund to successfully continue investment operations. Similarly, a business disruption at a service provider such as a fund administrator or auditor could impact a fund manager’s ability to distribute investor statements and audited financials in a timely manner.

Big Data in Alternative Investment Operations

The term big data refers to the process of using special computing applications to facilitate the analysis of very large sets of data in order to reveal trends and patterns. Alternative investment managers produce a great deal of data. Some of this data is stored and organized very accurately, such as data related to executed trades or the net asset value of a fund historically. Other types of data might not have been organized or even stored at all. An example of this would be the number of near-miss compliance violations with regards to a fund manager’s gifts and entertainment policy, or the times a particular broker was unable to locate a bid for a particular security. Increasingly, fund managers are realizing that there is value in better tracking and organizing all of this data with a particular emphasis on fund operations.

A key motivator for this change in recent years has been increased pressure from financial regulators to better track and report on certain data such as fund risk exposures. Registered funds in the United States, for example, are also asked to calculate relatively newer metrics than they had in the past such as Regulatory Assets Under Management (RAUM). This calculation of these types of metrics requires access to more and better data. Additionally, investors in funds have increased the frequency and depth of their initial and ongoing operational due diligence requests. These requests have resulted in funds needing a better understanding of their data. It is also important to note that some funds have also incorporated the use of big data analytics as well as artificial intelligence–related solutions to big data problems on the investment side of their business as well. These efforts have also resulted in more insights with regards to areas such as identifying potential compliance challenges on the investment side with more lead time as well as more insightful risk management strategies.
Chapter Summary

This chapter discussed the role of technology in alternative investment manager operations. The chapter began by outlining the role and items typically covered in information security policies. Next, we discussed the role of information technology consultants and the range of duties they typically perform for fund managers. As part of this conversation we discussed the software development life cycle including the process for change management and sandbox testing. We then discussed the role of data rooms in archiving and distributing management company and fund information. Next, we outlined cybersecurity trends with regards to fund operations including the role of penetration testing, software patches and vendor cybersecurity analysis. We concluded the chapter with a discussion of business continuity and disaster recovery planning and the role of big data and artificial intelligence in alternative investment operations. In the next chapter, we will discuss a variety of other additional functions and tasks that are important to fund operations.

Note

1. See M. Bowden, “The Worm That Nearly Ate the Internet,” The New York Times, June 29, 2019