BALANCING THE THREE PILLARS OF IT

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

BALANCING THE THREE PILLARS OF IT

How financial services companies can allocate their IT spending wisely

You may have heard of the 50-20-30 rule. It's a money-management technique that divides your paycheck into three categories: 50% for the essentials, 20% for savings and 30% for everything else.

This guideline of personal finance can be a great model for financial services companies as well, especially when it comes to information technology. However, the categories for IT spending look a little different. The three priorities for financial services companies are IT needs, cybersecurity and technological innovation. And while the exact percentages that organizations allocate to each category can vary—based on the company's structure and business environment—the goal is to balance these three pillars to create the basis for a successful, thriving culture.

PILLAR 1:
Keeping the lights on

PILLAR 2:
Securing IT

PILLAR 3:
Innovation

PILLAR #1

Keeping the lights on

The first pillar addresses basic IT needs. These include essential tasks such as:

- Maintaining proper computing power and data storage
- Managing cloud layers and cloud levels
- Ensuring the stability of a wide area network
- Securing connectivity to the cloud
- Enhancing wireless communication in the company's branches
- Ensuring up-to-date software licensing compliance
- Managing system life cycles
- Maintaining endpoint management and support for all hardware, software and user needs
- Enhancing the remote-work experience

PILLAR #1

Keeping the lights on (Cont.)

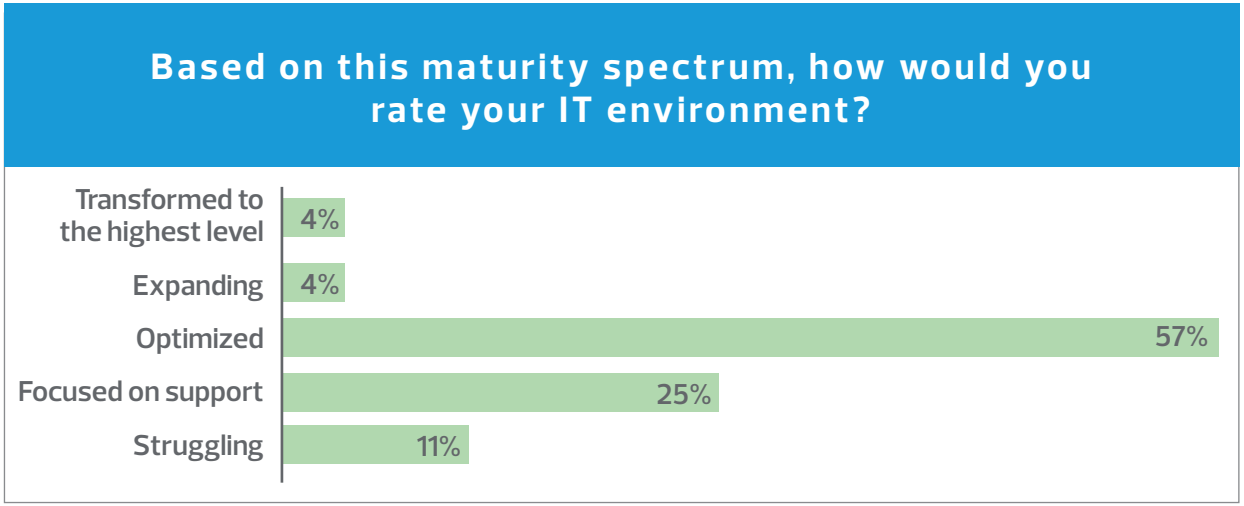
Keeping the lights on, from an IT perspective, is about maintaining a stable, reliable and high-performing IT environment. If a company is performing these tasks well, its systems are seamless and available to all users. Other positive signs include high employee and customer satisfaction, the effective utilization of cloud resources, and the proper management of life cycles and assets. An efficient IT system will reveal itself in positive exam and audit reports, and in the achievement of set metrics.

However, if a company is not performing these tasks well, the signs are unmistakable. The system crashes frequently. Users take minutes, instead of seconds, to log in. Tickets stay open for long periods of time. Legacy debt increases. Customers get frustrated because they can't get into the organization's online system, or they have to wait while employees struggle with their computers.

When issues like this arise, the company's reputation suffers. Its growth is slowed, and IT spending increases without a corresponding improvement in performance.

A recent survey of financial services industry leaders found that a majority believe that their IT environments are optimally running, with a very small percentage stating that their IT systems operate at the highest level. However, over a third of financial services industry leaders admit that their IT environments are either struggling or in support mode.

The first pillar is the foundation of a company's IT system. If that foundation is cracked or wobbly, it becomes impossible to innovate, or even to improve the situation. As such, investing in IT fundamentals is crucial to an organization's overall well-being.



PILLAR #2

Securing IT

The second pillar is cybersecurity. This vital component involves:

- Enhancing data protection
- Creating a chief information security officer or chief information officer role
- Establishing a secure access service edge, a cloud-based network infrastructure model that merges networking and security services
- Utilizing a secure security information and event management tool
- Developing incident-response procedures
- Enhancing ransomware protection
- Creating immutable backups
- Preparing for new cyber insurance requirements
- Developing metrics-driven procedures
- Creating testing and audit procedures
- Establishing layered security

PILLAR #2

Securing IT (Cont.)

At its core, cybersecurity is about keeping a financial services company's data from falling into the wrong hands. Organizations are under more threats than ever before, with bad actors determined to gain access to IT systems. Companies need to safeguard their assets, and they often have to do so while working in a dynamic environment. For example, as organizations expand their cyber footprints—by migrating to the cloud, establishing software as a service, creating remote-work systems or adopting other functions—they have to embrace new methodologies to counter attacks.

The Federal Financial Institutions Examination Council's cybersecurity assessment tool for financial services companies can gauge an organization's maturity level when it comes to cybersecurity. Organizations need to take an objective look at their efforts and assess any gaps. Do they have outsourced or in-house security analysts who can analyze events in real time? Do they have built-in automation to take care of alerts and notifications? Are they prepared for ransomware attacks?

Unfortunately, it can be difficult to gauge a company's cybersecurity maturity because most indicators are reactive and not proactively planned. And when it comes to data protection, no news is indeed good news.

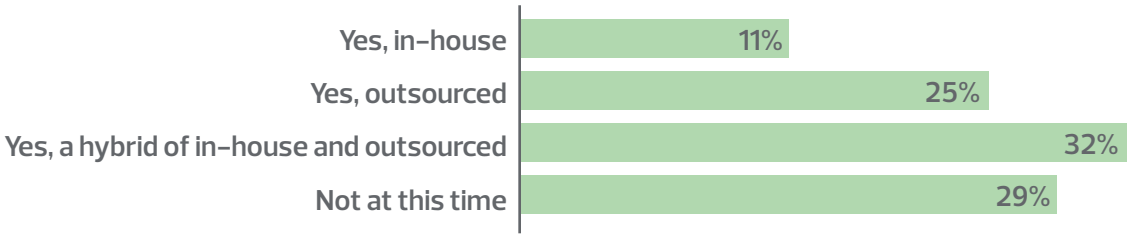
It's far easier to point out when an organization's cybersecurity is flawed. The most glaring sign of inadequate cybersecurity is when an organization suffers critical incidents or data breaches. Just one successful cyberattack can be devastating for a financial services company. The financial loss and reputational damage can be enormous.

However, even if an organization has fended off hackers and avoided data leaks, serious problems might be lurking that can be identified only through a regulatory audit or exam. Or companies might make the mistake of leading with risk instead of technology, creating an IT environment that is so locked down that users cannot do their jobs efficiently.

The good news is that financial services companies are taking the issue seriously. According to a recent survey of financial services industry leaders, more than two-thirds of organizations have access to a security analyst, either through in-house staff, a managed service provider or a hybrid of the two.

But the bad news is that there is no such thing as perfect cybersecurity. Financial services companies need to constantly assess this second pillar to ensure that they are investing in adequate protections for their data.

Do you have a security analyst today?



PILLAR #3

Innovation

The third pillar is technological innovation. This involves continually evaluating people, processes and technology to accomplish an organization's business strategies. Trends in innovation include:

- Enhancing the user experience
- Personalizing the customer experience
- Creating more effective data decision-making
- Assessing embedded banking
- Maturing the application stack into high-performing assets
- Establishing facial-recognition procedures
- Enhancing collaboration
- Creating virtual branches
- Assessing cryptocurrency
- Establishing fintech partnerships
- Enhancing environmental, social and governance concepts
- Assessing artificial intelligence options
- Creating opportunities for automation and integration

PILLAR #3

Innovation (Cont.)

Studies have shown that organizations that grew during the last recession were technologically superior. They established the importance of innovation ownership and got more of their employees onboard—not just executives and IT personnel. Financial services companies that want to create a culture of innovation must strive to help their workers find ways to perform their jobs better, faster and more efficiently through technological improvements.

But how do companies know if they are promoting innovation? For starters, the organization's employees will have the tools to do their jobs well, whether they are in the office or working remotely. In such organizations, human error is rare, because automation decreases the odds of a catastrophic mistake. Also, customers will feel that the company is easy to work with, and can quickly meet their needs.

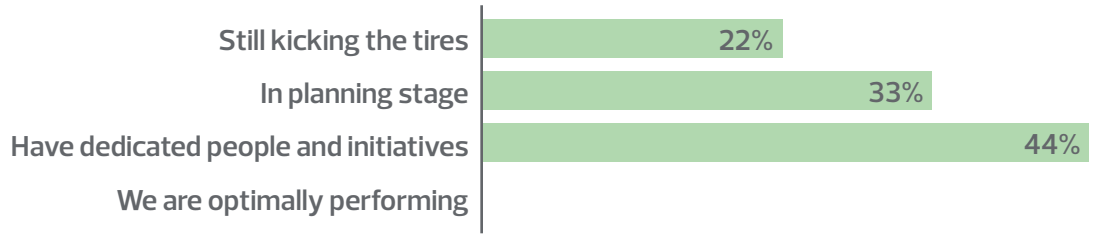
In contrast, an organization that is struggling to keep up with technological innovation will have employees who complain about the inadequacies of the IT system. Often, an organization with subpar IT does not have staff members who are dedicated to transforming the business through innovation. In such cases, customers will not give multiple chances to companies with glitchy systems or confusing interfaces.

Unfortunately, a recent survey of financial services industry leaders found that most organizations have not progressed past the planning stage when it comes to innovation. In fact, less than 1% of respondents state that they are optimally performing within the field of innovation.

This is problematic, because companies that do not innovate are closing themselves off to new revenue streams even while shrinking margins are driving the need to find more efficiencies. In addition, competition among financial services companies never wavers, so organizations that fall behind are unlikely to catch up. Furthermore, maintaining a culture of innovation is critical in the current tight labor market. After all, people who have their pick of jobs are unlikely to choose a company that makes it difficult to be productive or that doesn't offer the latest technological tools.

Therefore, establishing a culture of continued improvement is not optional for financial services companies. Innovation is a necessity.

Where is your bank on its innovation journey?



The importance of a **road map**

To keep the three pillars balanced, it is essential to plan. This involves identifying strategic goals, available resources and the nuances of the business environment. Once these crucial components are pinpointed, leaders must map the digital journey that their organizations have to take.

Soon after this road map is created, financial services companies should track their IT spending, not just with regard to budgeting and return on investment, but with an eye on the three pillars. For example, is the organization spending most of its money just to keep the lights on? Or does a large chunk of the budget go to innovative applications, even while users have trouble performing basic functions? If a financial services company is spending very little on cybersecurity, can it strive to erase legacy debt, and then use the savings to bolster data protection?

Again, the exact percentage that an organization allocates to each pillar is not set in stone. But leaders who know the signs of high performance—relative to each pillar—are well-positioned to figure out these crucial details.

Regardless of the specifics of each role, it is important for leaders to hold themselves and others accountable. Without accountability, the best plans for optimizing an organization's IT performance end up sitting in a desk drawer, untouched and forgotten. It is no accident when a financial services company succeeds in transforming its IT performance. The act of going to the next level is an intentional one.

Of course, like most aspects of good governance, balancing the three pillars requires a team effort to achieve the best results. A breakdown of roles is as follows:

- **Board of directors.** Board members are instrumental in developing an overall strategy and securing funding for high-performing IT functions. They also review audit and exam findings, which is a vital function.
- **Financial services company management.** By virtue of running the day-to-day operations, management is indispensable when it comes to improving IT performance. Managers provide a stable foundation for users and influence the organization's culture, which can be the difference between changes getting accepted or stagnation being allowed to rule.
- **IT department.** Obviously, the people who work most closely with an organization's IT platform will have a large impact on how that platform functions. The members of the IT department are the first line of defense and the organizational experts when it comes to performance.
- **Business units.** The members of the business units help drive technology based on their voice. They serve as internal customers of the IT department, and their insights into what works and what doesn't can guide important decisions.
- **Risk department.** Personnel in the risk department often establish formal procedures, such as creating an information security office. They also analyze risk and compliance assessments, and liaise with the IT department.
- **All employees.** It's often said that everybody's job is sales. But in today's climate, everybody's job is also cybersecurity. The easiest way for hackers to corrupt systems is through employees, so it is critical for workers to remain knowledgeable and vigilant about data protection. Employees can also drive innovation and provide guidance about how IT should interact with customers.

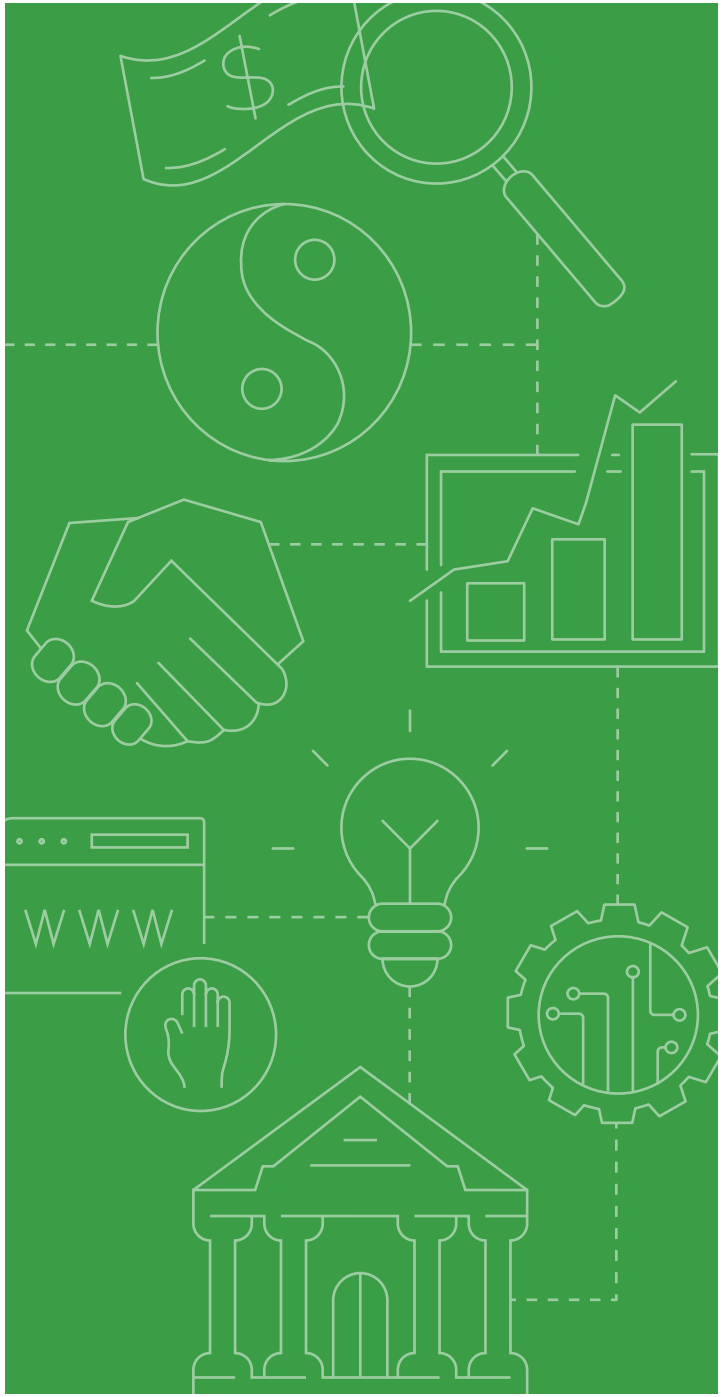
Achieving balance

For companies to unlock the full potential of their IT platforms, it is vital for them to balance all three pillars. Focusing too much on any one area, to the exclusion of the others, will lead to dysfunction, inefficiency and frustration.

Just as balancing essentials, savings and extras is important in personal finance, it is also essential for companies. IT fundamentals (the first pillar) are the essentials, cybersecurity (the second pillar) are savings and innovations (the third pillar) are wants. Thinking about it this way makes it clear that companies must have a robust IT foundation and strong data protection before they tackle innovative applications.

Companies can start this process by analyzing their needs, breaking down their IT budgets and allocating their spending to the pillars that need the most support. A strategic road map is necessary, and all employees have a part to play in achieving harmony among the competing IT functions.

Balancing the three pillars means maintaining a high-performing IT environment, while ensuring that data is secure and that innovation can thrive. A financial services company that strives for this balance creates a culture where both employees and customers feel their needs are being met, and builds a solid foundation for success.



Outsource your needs

RSM US LLP is a next-generation managed services provider that's ready to guide your financial institution through its digital transformation. Our sophisticated financial institution technology solution can help you optimize your technology usage and safeguard your organization by offering secure cloud solutions.

We provide rapid onboarding and a deep talent bench that has unmatched industry and technology experience. We'll introduce you to best practices and provide 24/7 access to IT services. And, if you need them, we offer strategic advisory, regulatory and technology services.

For more information, visit RSM's managed IT services for financial institutions hub.

VISIT HUB

+1 800 274 3978
rsmus.com

eb-nt-mts-fs-0422

RSM