



# A CFO'S GUIDE TO MANAGING TECHNOLOGY, IT SOLUTIONS, AND RISK

*By Thomas H. Douglas*




**Every business is a technology company.** No matter your industry, vertical, area of expertise, location, or the age of the company, every business must have technology in place not only to operate but also to achieve success. Yet many businesses fail to see IT for what it is: a key driver in achieving that success. This is because many business leaders do not know how to leverage IT effectively to drive strategy and outcomes. As a CFO, this is especially important, and the goal of this document is to help you be successful.

Budget management requirements for technology are constantly changing and becoming more challenging. The budget has to move as fast as the technology does within the business community. And that's not even accounting for cybersecurity risk management, productivity management, cloud services, depreciation and amortization management, business continuity plans, and compliance requirements. In other words, you have a lot to accomplish to ensure success is achieved. The good news is that following this guide's best practices will help.






# CFO Control

A photograph of three business professionals in a modern office setting. A man with glasses and a beard, wearing a green and black plaid shirt, is seated on the left, holding a white document. A woman with long dark hair, wearing a denim jacket, is seated in the center, looking at a document with a colorful circular chart. A man with a beard, wearing a maroon shirt, is seated on the right, looking towards the woman. They are all engaged in a discussion.

One concept we believe is fundamental in any SMB is CFO control. That means that the levers are aligned so that the CFO and other decision-makers have control over the budget and that "the budget does not control them." This is extra important with IT management. Unfortunately, many businesses don't have this control in place. Often, this happens because an organization simply doesn't realize the costs and controls related to cloud expenses. An organization will make a big move to a cloud or hosted service with the belief that high Capex costs will go away, only to find out that Opex costs soar out of control. This happens because many cloud solutions are based on utilization, often referred to as a utility expense. The more you use, the more the costs increase. The problem is multiplied when an organization doesn't fully understand how to best leverage the features and services in the cloud environment, resulting in waste and overspending. This can cost an organization tens or even hundreds of thousands of dollars per year.





When it comes to technology, one of the premier responsibilities of a CFO is to ensure controls and cost management capabilities are in place. Doing this keeps costs manageable. We have helped customers quickly exit a bad cloud design because the costs turned out to be three or even six times higher than anticipated. A cloud readiness assessment should be performed to prevent that type of situation and ensure there are no surprises. In addition, a detailed evaluation of the agreement with the provider should be performed.



# Technology Planning

A JMARK best practice is to have a five-year technology plan in place for every client. This plan includes every component on the network, such as workstations, laptops, servers, network equipment, security, software licenses, renewal management, internet and communication, wide area network (WAN), warranty extensions, and beyond. The plan is broken up by quarter so that on the day a component goes into use, the organization already knows exactly when it will be pulled and replaced. Combined with getting clarity on expense versus amortization, planning in this way allows you to know exactly what the budget will require, which ensures that there are no surprises.

Nothing is more frustrating than when an IT provider or department head springs a major expense (like a server) on a business without proper planning. For this reason, the plan should always include application upgrades, business expansions (like a new location or acquisition), and normal lifecycle management, as well as manufacturer end-of-life schedules. By aligning IT plans and lifecycle management with the responsible parties in IT, you can determine what to expense, what to depreciate, and what should be accounted for over a given period.





It's important to realize that IT costs actually increase when an organization tries to push the lifecycle schedule too far. Productivity problems and frustrations grow with an aged technology infrastructure. Not to mention that in the fourth year of operations, workstations begin to experience problems at a higher rate, and in the fifth year, these issues begin to bloom into significant challenges.

At JMARK, we call this aspect of IT management the "business of IT." Whereas the "operations of IT" refers to the day-to-day performance of an environment, the business of IT is knowing the cost schedule, best-in-class spending requirements, and other factors. Formally, we describe the two as follows:







## The Operations of IT

*This is the day-to-day delivery of IT services that ensures an organization can maximize its technology investment to enable people to maximize their productivity. This is accomplished through helpdesk services; security; server, network, and workstation management; backup and business continuity strategies; application and data management; patch management; firmware; and vendor update management.*

## The Business of IT

*This is the strategy employed to ensure that the technology design meets the mission of the organization and aligns those outcomes with the budget and lifecycle management plans. Done properly, this should result in investments being appropriately made to ensure the organization is not put at risk through underspending, wasting of resources, or overspending. This involves aligning the right design, resources, and capabilities so that the technology advances the organization toward its objectives.*

You can find out more about these two areas by reading this [\*article\*](#).





# Risk Management

Another critical responsibility for the CFO is to manage the risk of the business. Creating clarity and accountability for this is more than mandatory, as the IT environment typically houses intellectual property—or what we describe as "the future of the business." While accounts receivable is a historical record stored within the IT environment, the future of the business is stored in the documents, applications, plans, proposals, templates, patents, work products, and much more.

Every organization must manage risk. For some, this includes worker's compensation and safety; for others, professional liability insurance. But for all, it includes IT risk and cyber liability. Risk management plans should include protections from ransomware, data loss, failures, natural disasters, fires, water damage, vendor failures, and other possible catastrophic events. Oversight and clarity in this arena are the key responsibility of a good CFO.

To learn more about business continuity plans, please see this [article](#).



# IT People Management

A CFO is often responsible for the people or organization that manages IT. This daunting task can actually be quite rewarding. One secret to managing these resources is mitigating people issues and risk management by focusing on outcomes.

A good CFO should require that IT perform well in both the business and operations sides mentioned above. This can only occur by working with an IT delivery solution that is of a higher operational maturity. Unfortunately, an "IT guy," homegrown department, or small, immature partner will never have the capability to perform at a high maturity level. This is influenced by market conditions, threat awareness, access to resources, access to subject matter experts, and adequate time to mature the solutions and processes needed to deliver desired outcomes consistently. In contrast, a mature partner works proactively and guarantees outcomes, which, at the end of the day, are the only thing that matters when it comes to IT. "Effort" doesn't earn a prize.






As a part of good IT oversight and management, a few key things need to be in place:

- **Business continuity management:** This should include the tracking of all security events, backup and restore activities, replication management, testing and verification management, and much more. These activities are the key to ensuring risk is properly monitored.
- **Tracking:** Every issue, change request, addition, and modification should be tracked. This doesn't just include the issue, but also the time taken to resolve it. Every minute of every day should be accounted for within IT.
- **Configuration management:** All components of IT should be accounted for in a configuration management system. This includes the necessary information to redeploy a device should the design of the component be lost. This is especially true for servers, network devices, firewalls, and database management.
- **CSAT (customer satisfaction) results:** As a part of good IT management, users should have the ability to rate their support experience, using a consistent rating method with the ability for plain text feedback.
- **SLA management:** Service level agreements are a way to measure how well an IT support structure is achieving expectations. All IT issues should have measurable expectations to ensure IT is performing satisfactorily.







All these items (and any others you deem necessary in your company) should be reviewed on at least a quarterly basis. By having a formal review process, you can ensure that IT is operating at a high level and can identify risk areas, frustrations, and any other trends that may require further attention.

If you would like to find out how JMARK makes all of this much easier so you can focus on your organization's financial performance, please [click here](#). We'd love to help!