# Five Strategies For CIOs to Stay On Top Of The Game

## These practical, clear strategies will enable CIOs to stay on the leading edge

**The Chief Information Officer (CIO) plays a vital role in federal agencies. They are accountable for managing IT spend worth billions of dollars, and the decisions they make impact how successful a business is in leveraging technology. To be truly effective, CIOs know they must keep the function running at its best. Yet according to the US Government Accountability Office's (GAO's) most recent figures, three-quarters of those who take up a CIO role are gone within three years. What gives? And how can these numbers spell success for either federal agencies or the individuals involved?**

Turnover can occur for various reasons—a change in administration, retirement from federal service, the lure of higher-paying jobs in the private sector or a security breach. If the role was not challenging enough, the pandemic-driven move to being a digital-first organization with most staff working remotely forced CIOs to be even more agile and innovate on the fly. But when it comes to CIOs getting fired, the common yet vague accusation of having been "ineffective" covers a multitude of potential issues.

These myriad causes, many of which may sound subjective or seem to stem from external considerations, impact the multifaceted CIO position. To help you navigate this complex, dynamic terrain, we've used our long-term experience and insights from working with federal agencies and commercial sectors, as well as input from GAO's survey report, and other metrics, to reveal the most common challenges CIOs face. We've also devised strategies for resolving these problems, keeping you at the top of your game. In the following pages, we unpack the five key things CIOs must address to excel in this important position.

Step 1

# Implement Comprehensive IT Governance

Leading in the information space is not just about technology, but also in how the business is run. Today's federal CIOs contend with much higher stress levels and more demands than ever before. They face unrelenting pressure to improve internal customer satisfaction and to deliver higher quality technology initiatives within compressed timeframes. They are also expected to drive enterprise process improvements while reducing costs and redundancy.

Added to these strains, federal agency departments and business units are continuously moving forward with higher-dollar projects, many of which gained urgency during the pandemic. Unfortunately, much of this activity is occurring in silos.

Inadequate, siloed information and processes impede a CIOs ability to make decisions, streamline operations, monitor accountability, sustain value, and address common 'pain points,' such as:

- Fragmented governing bodies that do not drive the achievement of strategic goals and objectives.
- Lack of an enterprise communication strategy to keep responsible parties 'engaged' and apprised of governance objectives, performance measures, and outputs.
- No overarching enterprise architecture aligned to agency objectives that serves as a blueprint for IT decisions and enforces technology standards and platforms.
- Inability to identify, manage, mitigate, and report on risks at an agency-wide level.

As the GAO report noted, CIOs struggle in articulating these challenges to executives. Some lacked the appropriate oversight to proactively make timely, informed decisions on at-risk projects, which, while unfair, ultimately led to termination. But with USGS estimates suggesting that poor IT governance can cost a company 15% to 20% of its operating budget, no agency can afford to get this piece wrong.

## How Can You Establish A Comprehensive It Governance Program?

- Cultivate relationships to encourage better information sharing and communication to facilitate a 360-degree view of the business.
- Foster a collaborative culture instead of just treating business stakeholders as consumers.
- Evaluate current management controls and IT governance structures.
- Consistently analyze investment risks prior to green-lighting projects and monitor those risks throughout the project lifecycle.
- Select the IT governance framework (e.g., ITIL) that best aligns to strategic objectives, and determine the desired maturity level.
- After implementation, continue to measure performance against the framework. A trusted partner with expertise in this process can provide invaluable, unbiased support throughout.

**With pressures around evolving technologies and business demmands for quicker implementation, you must foster and maintain collaboration with business owners across the organization while ensuring IT governance processes are clear & effective.**

Step 2

# Prioritize Strategic Planning

CEOs don't always understand the value of a CIO, in large part because these two crucial C-suite roles often fail to connect around mission priorities, investments, and business objectives. The burden falls on the CIO to demonstrate the worth of their value proposition, and excellence in strategic planning initiatives may well be the best way to do so. Also, without continuous strategic planning and monitoring, a CIO will likely foster other dysfunctional relationships, placing them at odds with business and mission support-oriented stakeholders.

Planning for success involves a myriad of factors. While most CIOs do have a plan, a considerable number of strategic plans are:

1. Outdated
2. Not entirely consistent with the agency's mission
3. Lack continuous performance monitoring and reporting mechanisms
4. Lack internal stakeholder input and buy-in, and
5. Lack a tactical implementation roadmap.

Furthermore, as COVID-19 revealed all too clearly, many agencies also desperately need tailored tactics to cope with potential global crises, with one survey from the onset of the pandemic identifying close to 40% of companies as being devoid of such a plan.

Excellence in strategic planning opens up space to flourish in every area of the enterprise. But unfortunately, many current technology investments are not meeting the desired ROI for the organization, nor driving improved outcomes for your customers, employees, and the public at large.

The standard components of a thorough strategic plan include many steps on the journey from development to execution. Expert oversight encompassing both business and technology is often beneficial throughout this complex process. Such collaborations can produce compelling, tangible evidence for the proficiency of the sitting CIO, without which they risk being seen as expendable.

## How Can You Ensure Success In Strategic Planning?

Review and revise the current CIO strategic plan with an eye toward bringing together stakeholders, emphasizing collaboration, value, and results, and, specifically:

- Improving management of IT as a business.
- Leveraging leading technologies and capabilities to enable the future of core mission programs while advancing operational effectiveness and efficiency.
- Operationalizing strategic initiatives into a tactical implementation roadmap.
- Identifying opportunities to drive comprehensive IT transformation to enhance capabilities, collaborate with the business, reduce cost, increase agility, and improve customer service.

**Align with your customers, especially the leaders of the business, to strategically impel both overall mission and day-to-day priorities, responsibilities, and performance expectations.**

## Step 3

# Be Proactive About Security

In any sector, a major security incident almost guarantees a CIO will need to start updating their LinkedIn profile. Federal security breaches took on a different resonance during the pandemic, with almost everyone working remotely and vast swathes of the population having to access government relief assistance programs online. A recent Interpol report warned of a 569% growth in malicious domain and website registrations from February to March 2020 alone. Such trends are expected to continue, increasing in variance and sophistication over time.

Moving forward, CIOs will need to be more innovative when it comes to information security to support agile responses to evolving attacks and unprecedented crises, to protect working-from-home tech and data, and to safeguard their jobs. Strengthening cybersecurity is an integral responsibility as well as a mandated duty for federal CIOs. Yet many fall short in this regard. Fortunately, it's possible to do better.

## How Can You Get Ahead of Potential Security Issues?

- Develop a comprehensive cybersecurity program to address policy, processes and technology to strengthen the security posture of the organization.
- Implement a strong asset management program to ensure you know and track everything in your environment.
- Establish a strong relationship with your mission and business organizations to develop a Cyber Resilience Program to be sure you are adequately protecting your High Value Assets.
- Partner with the Chief Information Security Officer on priorities and investments to ensure the resources you are allocating are protecting the most important company assets.
- Assess key aspects of information security:
  - Ensure current security controls in place are aligned to the organizational and federal standard security framework (e.g., NIST Cybersecurity Framework and Improving Critical Infrastructure Cybersecurity Framework).
  - Invest in improved Governance, Risk and Compliance processes and tools ensuring you understand third-party risk as well.
  - Align processes, standard operating procedures and tools to the agency's enterprise risk management framework.
  - Implement and strengthen "defense in depth" solutions to ensure a layered detection and prevention approach.
  - Implement a proactive vulnerability patching program and a continuous monitoring program for malicious behavior.
  - Employ state of the art Identity and Access Management programs to ensure people, technology and data access are authenticated.
  - Implement a robust cybersecurity employ training program-90% of all breaches result because of human error.
- Implement a data governance strategy for data security, ownership, compliance, and stewardship, particularly in mission-critical applications and areas that collect and store sensitive Personally Identifiable Information. Establish a great relationship with your General Counsel to ensure you understand Data Privacy regulations which vary by country and U.S. State.
- Work with your C-suite & CISO to establish and exercise an incident response plan. More likely than not you'll need to enact it and learning how to do respond in the middle of a crisis is less than ideal.

**The central role security plays in your—and your agency's—continued success means you need to leverage analytical, technological, relational, & other tools for a robust and highly adaptable program.**

Step 4

# Address Common IT Workforce Issues

IT is a high-demand, well-compensated skill in the public and private sectors. So agencies, and CIOs in particular, struggle to recruit and retain employees with these valuable skill sets. Workforce scarcities extend beyond critical IT areas, such as cybersecurity and cloud computing, to mission support functions that enable effective execution of IT investments.

In all these instances, CIOs end up relying more on contractors, leaving the organizational culture of shared goals and values on the sidelines. And while the common CIO believes their job centers on technology, employees believe leaders drive culture, which in turn drives behavior, morale, performance, and customer service.

Recent exigencies in government and global health crises have highlighted the importance of human relationships and ongoing training. According to the Federal CIO Council's May 2020 Future of the Federal IT Workforce Update, agencies must improve their recruiting, hiring, training, and retention-promoting practices to spur innovation, boost flexibility, and drive worker satisfaction.

As CIO, it's your job to ensure your current workforce is on-point with sufficient staff numbers, as well as the necessary skill sets and competencies needed for success.

## How Can You Develop A Preemptive Workforce Plan?

With the appropriate in-house talent, in tandem with a trusted advisor, perform the following five workforce-enhancing tasks:

- Review present roles to identify critical skills and competencies.
- Develop a workforce strategy focusing on employee engagement, diversity and inclusion, retention, and training.
- Perform an inventory of in-place training to identify gaps and ensure alignment with current technical skill requirements.
- Evaluate the IT hiring manager role and related processes.
- Review the current organizational structure, including open and funded position vacancies, against the CIO strategic goals and objectives.

**Remember, building and empowering your workforce is just as important as investing in technology.**

## Step 5

# Choose Contracts Wisely

Clients always seem to want the next new thing. Your staff is barraged with the latest products, which may not reflect what truly works for the business in the long term. Failures—over budget, with little or nothing delivered—are often in the news. In fact, The Economist has already branded 2021 as "a bad year for government software."[viii] And during the pandemic, the rush to satisfy demand increased the pressure on federal CIOs to choose quickly or risk depriving people of basic necessities.

While IT spending on investments, vendors and contracts has increased—federal IT spending is budgeted to top $92 billion in fiscal year 2021[ix]—the operating budget within the CIO shop has long remained the same. Additionally, CIOs typically grapple with several forces that underly disappointing contract choices, execution and fulfilment:

- Systems implementation contractors often generate substandard SLAs.
- Federal Contracting Officer Representatives/Contracting Officer Technical Representatives may produce inconsistent RFPs/RFQs and lack the capacity to properly evaluate responses.
- COTS systems implementers typically develop requirements that are biased toward a particular platform or solution rather than centering on the requirements or needs of the business.
- Deficient IT operations contracts provide insufficient resources to support the necessary work.

### What are the key aspects of effective vendor management?

A vendor agnostic, objective approach is invaluable to distinguish between a valuable addition to your enterprise's technology toolkit and a bad fit. In any such endeavor:

- Stop automatically awarding contracts to the lowest bidder. You get what you pay for—and the agency CEO doesn't get fired when you're over budget, you do.
- Closely analyze contract-award processes and the quality of SLAs with vendors and system integrators.
- Conduct an unbiased analysis of 'configurable' tools and alternatives encompassing the full spectrum of pertinent agency business needs.

**To be sure to award contracts that serve both you and the business, take concrete steps to evaluate and choose wisely, integrating the appropriate constructive factors into the process.**

Guidehouse
Outwit *Complexity*

For more information,
please contact:

**Robert McNamara**
Partner, IT Strategy
rmcnamara@guidehouse.com

**Brian Williams**
Associate Director, IT Strategy
bawilliams@guidehouse.com

The federal CIO peer group shares many unique opportunities to enhance the business. Its members also face an array of well-documented risks, any one of which can get them fired or in hot water. The CIO who proactively addresses and mitigates these five challenges will increase their probability for lasting tenure, while also contributing to peak business performance.

Working with a skilled partner can help in detecting such problems and generating unbiased, objective, quantifiable, effective ways to solve them.

**If you are looking to make progress in any or all of these five areas, Guidehouse can help you move forward with confidence, whether through holding a targeted IT workforce strategy assessment, developing your IT Strategic Plan or collaborating on a more comprehensive IT Governance program.**

1. https://www.gao.gov/products/gao-18-93 https://www.gao.gov/products/gao-18-93
2. https://www.gao.gov/products/gao-18-93
3. https://www.usgs.gov/products/data-and-tools/data-management/value-data-management
4. https://www.prnewsonline.com/crisis-survey-CSA-practice
5. https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of cyberattacks-during-COVID-19
6. https://www.federalregister.gov/documents/2018/05/18/2018-10855/enhancing-the-effectiveness-of-agency-chief-information-officers
7. https://www.cio.gov/assets/resources/Future_of_Federal_IT_Workforce_Update_Public_Version.pdf
8. https://www.economist.com/united-states/2021/03/18/despite-high-profile-failures-government-tech-is-slowly-improving
9. https://www.statista.com/statistics/506409/united-states-federal-it-expenditure/

## About Guidehouse

Guidehouse is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology, and risk consulting. We help clients address their toughest challenges and navigate significant regulatory pressures with a focus on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that prepare our clients for future growth and success. The company has more than 10,000 professionals in over 50 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit: **www.guidehouse.com.**