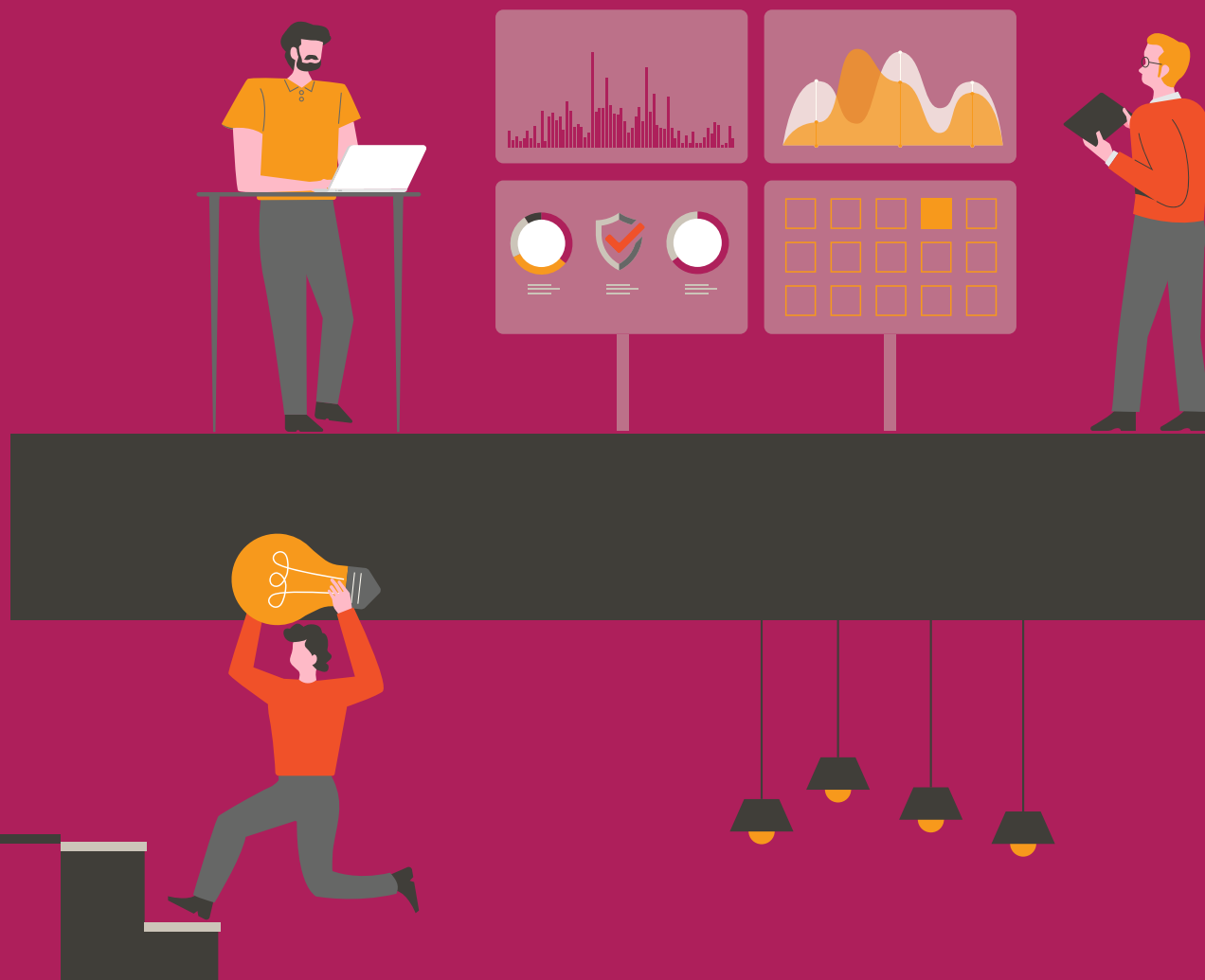# How the Cloud Enables a Secure and Safe Customer Experience Made for the 21st Century

RESEARCH BRIEF

GENESYS™   govloop

Introduction

It's in headlines everywhere: the cloud. Many agencies, large and small, are migrating workflows and email systems to the cloud, and the federal government has encouraged them to do so with mandates, memoranda and even cash incentives. All of the flashy press makes moving to the cloud seem simple, but as agencies know, there's a lot more that goes on behind the scenes.

Agencies have to be mindful of their high-value assets and ensure that the cloud will offer them appropriate security, as mandated by the Federal Risk and Authorization Management Program (FedRAMP), which establishes baseline security standards for agencies' cloud technology.

Therefore, agencies need a clear path to the cloud to avoid a mangle of IT and business objectives, and they need an easy way to evaluate secure, cloud-based solutions. These solutions will lead to numerous benefits. As cloud adoption matures across government, agencies have gradually realized that cloud solutions expand on the security capabilities that agencies had in their legacy data centers and exceed federal standards. From a workforce standpoint, the cloud also makes it easier for employees to access resources, data and systems on demand, and to do so from anywhere and on any device.

By using FedRAMP-certified offerings, agencies can partner with trusted cloud service providers to maintain their IT environment. Having this support frees employees up to focus on higher-priority projects that directly impact customer experience (CX).

In today's digital world, having these cloud-driven capabilities is also the key to driving better engagement with the public and improving CX for all citizens.

To learn how agencies use secure clouds to power CX, GovLoop partnered with Genesys, a leader in cloud customer experience solutions, for this report. We also conducted a survey of 148 government employees knowledgeable about cloud investments in their agency.

In this report, we discuss the current state of cloud in government and the benefits agencies are realizing from the cloud, specifically around CX. You'll learn how security standards can be used to evaluate the strength of cloud solutions and why they are essential when evaluating cloud offerings.
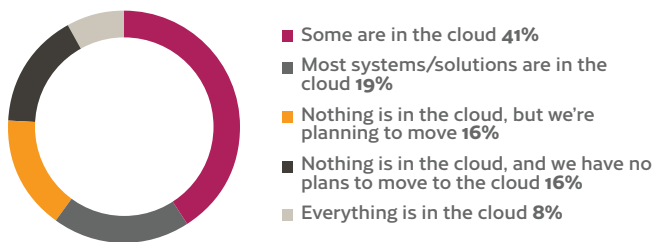
You'll also hear from experts with the Government Group at Genesys — Ian Greene, Enterprise Architect, and Jodi Thompson, Senior Principal Business Consultant — about the best practices agencies can incorporate to maximize the benefit and minimize the risk of cloud technologies.

The State of Cloud Adoption in Government

If you're looking for advice about the cloud, it's coming from every direction. At a high level, the White House announced the Cloud Smart strategy to help agencies find cloud solutions to "streamline transformation and embrace modern capabilities." Congress in 2014 passed the Federal Information Technology Acquisition Reform Act (FITARA), architected to help CIOs escape legacy technology and purchase new technologies. Meanwhile, citizens want a user experience that rivals that of the private sector – one that is timely, intuitive and tailored to meet their specific needs. In many cases, cloud supported these types of experiences.

With all of these potential benefits, many government agencies have been quick to welcome cloud technology. According to GovLoop's survey, however, most are still in the early stages, with 41 percent of respondents saying that some projects are in the cloud, and 16 percent reporting that their agency currently is not using cloud but is planning a cloud migration within the next year. Overall, 68 percent of respondents reported that they had invested in cloud technology, of which 27 percent reported having most or all of their systems in the cloud (See Figure 1).

FIGURE 1: *How would you describe your agency's investment in cloud technology?*

- Some are in the cloud **41%**
- Most systems/solutions are in the cloud **19%**
- Nothing is in the cloud, but we're planning to move **16%**
- Nothing is in the cloud, and we have no plans to move to the cloud **16%**
- Everything is in the cloud **8%**

FIGURE 2: *How would you rate the transition from an internal, cultural perspective?*

- It was OK, we had some bumps in the road but that was to be expected **58%**
- It went well **25%**
- It was not great - we didn't have a lot of buy in **16%**
- It was terrible **1%**

That's to be expected, Greene said, as a mix of business and IT parties within agencies can stir up different views on the cloud.

Furthermore, the General Services Administration (GSA) reported that agencies are implementing cloud migrations in real time. Cloud-based solutions are serving 95 percent of federal email inboxes, and four federal agencies added more inboxes to the cloud from August to December 2018.

Not every agency has embarked on the cloud journey as of yet, however, and for those that don't, culture is often the barrier to adoption.

Transitioning to the cloud is only effective if agencies have clear plans and preparations. As cloud is a significant investment, it should be approached with an all-hands-on-deck mentality to prepare all of the staff to deal with the shift. Unfortunately, that is not usually the case in practice.

Most agencies that have gone to the cloud – 58 percent – encountered some bumps along the path of adoption, and 17 percent of respondents said that the transition was "terrible" or did not go well. While challenges might be expected, 25 percent of respondents had successful buy-in culturally to the cloud changeover (See Figure 2).

Many factors influence the success of cloud migrations, but it's often easy to blame shortcomings on an aging workforce or employees – which is misguided. Instead, there are certain techniques that agencies can implement to allow cloud adoptions to go over smoothly.

That includes preparing staff for a dramatic change to the way that agencies process data and manage systems. Oftentimes, a disconnect between the IT and business communities within agencies can create friction involving the move to cloud.

In addition to communication, there needs to be a clear purpose for cloud adoption. If leaders fail to identify cumbersome workflows and procedures before moving
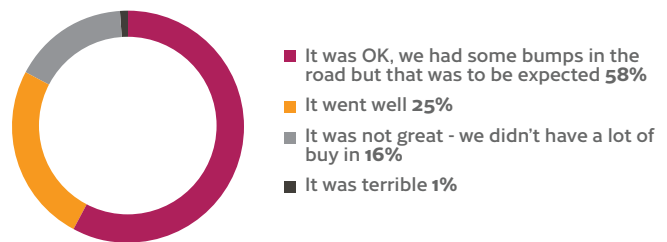
to the cloud, then agencies can entrap their workforce in a new system with the same inefficiencies as beforehand – putting themselves through a dramatic cultural shift without even achieving what was intended. With a clear path for rollout, however, cloud technologies can save agencies time and free up resources that will improve CX.

"Cloud migrations are about best practices and business outcomes," Greene said. "The focus of IT departments has gone from dedicating resources to managing a system, physically making sure the system is working, and from doing some work on the CX side to all their resources going toward customer experience."

How traditional agencies operate

*The federal government often spends **75 percent or more** of its IT budget on operations and maintenance. Legacy systems continuously stall out and soak up valuable IT resources. As agencies seek to invest in and improve their CX, the cloud can unlock new capabilities while also providing them with the funds and time to invest further.*

Government's Top Cloud Challenges

Although agencies can struggle to equip their workforce culturally for cloud adoption, that's not the primary concern of most who haven't adopted cloud yet.

Agencies that fail to correctly vet their cloud solutions can be left stranded. After enduring intensive and laborious migrations, agencies that disregarded the compatibility of their applications or the employee training side are likely to meet the same outcomes as they did beforehand. Even after moving to the cloud, agencies can be left with an expensive tab and the same stagnant CX internally and externally.

"If you invest in cloud and simply replicate the status quo, you're not going to see many benefits," Thompson said.

While agency leadership often dictates whether cloud will be the next step, only 9 percent of respondents said cloud was not a priority (See Figure 3).

The far more important barriers to cloud adoption were (See Figure 3):

- Lack of funding 23%
- Lack of in-house knowledge on cloud services 32%
- Security concerns about cloud technology 36%

So, what are those security concerns that respondents identified as the biggest barrier to adoption? Much of them tie to the other primary issues, specifically a lack of knowledge about cloud. As IT departments can be bound to the legacy technologies they maintain, a foreign cloud service may seem like starting at square one.
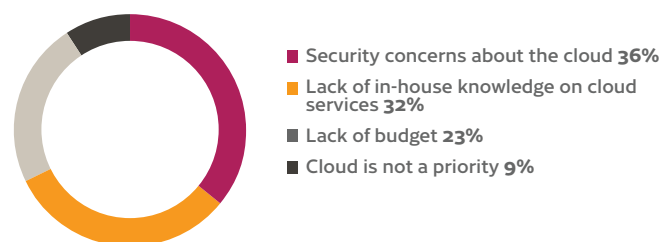
Although legacy systems require constant upkeep and maintenance, security teams can feel like they have greater visibility because they can see and touch physical servers. But these systems take on more vulnerabilities as they become outdated.

These barriers to cloud adoption used to be even greater. Before moving from on-premise hardware and software to cloud-based services, entire IT departments would have to be brought in to evaluate a cloud provider's solution and compare it to the agency-specific Authority-to-Operate (ATO) – a formal sign-off from agency senior officials to permit a cloud transition. Kickoff meetings could take hours, while testing and acquisition timelines could drag on much longer.

Without ways to easily check the fit of a cloud solution, agencies could either feel forced to adopt solutions that did not fit their needs or be left without an appropriate IT solution at all. As such, legacy systems would shackle CX services, which would have limited capabilities because of outmoded on-premise hardware. Agencies, investing heavily in operations and maintenance, would then lack the funds to adopt new, upgraded CX solutions because of their tie to legacy technologies.

FIGURE 3: *If your agency is not currently using cloud solutions, what is your biggest barrier to adoption?*

- Security concerns about the cloud **36%**
- Lack of in-house knowledge on cloud services **32%**
- Lack of budget **23%**
- Cloud is not a priority **9%**

How FedRAMP Answers Chronic Security Questions

FedRAMP was signed December 2011 and was established to streamline how agencies purchase new solutions by holding cloud assets to federal security standards. The program operates with a two-fold analysis of how agencies should secure cloud-based data and information: by certifying solutions, and then offering levels of security clearance for cloud service providers.

FedRAMP requires that agencies comply with National Institute of Standards and Technology (NIST) and Federal Information Security Management Act (FISMA) security standards when housing services on the cloud, which means that they have to find cloud service providers to match these standards. While agencies have to pass FedRAMP compliance checks, FedRAMP also provides agencies a way to easily measure and evaluate cloud service offerings.

An intergovernmental Joint Authorization Board (JAB) manages FedRAMP. The JAB is made up of chief

information officers from GSA and the Defense (DoD) and Homeland Security (DHS) departments. Vendors have to meet increasingly rigorous requirements to secure more valuable assets, so that low-level, small agency data is not held to the same security standard as high-level DoD data.

Although FedRAMP compliance is mandated governmentwide, the program is still not well understood by all agencies. One reason is a lack of intra- and interagency communication about FedRAMP, Thompson said.

The best use of FedRAMP happens with top-down, consistent leadership and with synchronization between the IT and business communities of an agency. Considering the 3 percent who marked themselves as experts, or the 15 percent who marked themselves as confident in FedRAMP knowledge, the program can be more easily understood when the different offices and bureaus within an agency can communicate with one another (See Figure 4).

"They know FedRAMP is a requirement," Greene said. "They've been told they have to have it, but agencies don't entirely understand what it does for them."

That could explain why 35 percent of respondents said their agency considers all solutions regardless of FedRAMP compliance. The vast majority (65 percent) indicated that their agency either required or preferred FedRAMP compliance from cloud service providers (See Figure 5).

Understanding exactly what FedRAMP is can crucially reduce acquisition costs and time. If cloud service providers can lay out their security credentials in an easy-to-understand way, such as through FedRAMP impact levels, then agencies can instantly gain an understanding of their new security system. Therefore, leadership can focus on what cloud providers enable for CX, instead of fretting over what security will be required.

"They see the benefits of the customer experience as having the most current, digital and innovative technology available at their fingertips, versus it being a siloed solution," Greene said.

FedRAMP can help agencies bypass the standard weeks of security checks that occur outside of implementation. Greene said that for agencies that have embraced the program, they have already lined up their authority to operate (ATO) orders in accordance with FedRAMP

standards. Of course, agencies always have the option to require a higher level of security from vendors than what is mandated by FedRAMP for their data.
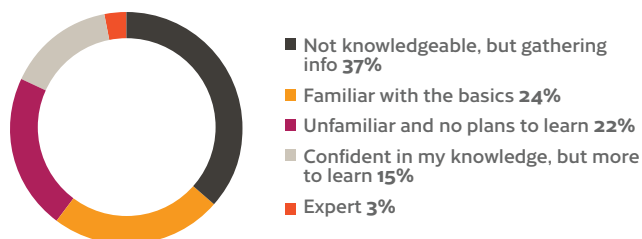
Greene also sees more adoption of FedRAMP. He has noticed more and more agencies are demanding their solutions be compliant – and he estimates that two years ago, only 10 percent of agencies would have required FedRAMP solutions. Thirty-seven percent of respondents said their agencies require FedRAMP-compliant solutions now. Greene said that in the next year, he expects even more agencies will depend on it as the gold standard, and that number could jump as high as 45 percent (see Figure 5).

"We're seeing it pop up in places that it's not technically even applicable, but they're asking for it anyway," Greene said. "We see small state agencies still requiring vendors to comply with FedRAMP."
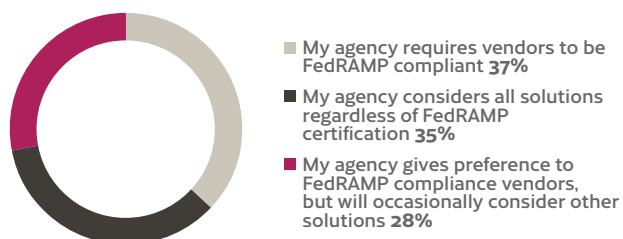
As we've seen, agencies recoup time and money that they save from FedRAMP. So, what can they do from there? That energy can be circled back into mission goals, such as CX.

In the next section, we'll explore the cloud's many agencywide benefits.

FIGURE 4: *How familiar are you with FedRAMP?*

- Not knowledgeable, but gathering info **37%**
- Familiar with the basics **24%**
- Unfamiliar and no plans to learn **22%**
- Confident in my knowledge, but more to learn **15%**
- Expert **3%**

FIGURE 5: *How does FedRAMP impact the cloud solutions you invest in?*

- My agency requires vendors to be FedRAMP compliant **37%**
- My agency considers all solutions regardless of FedRAMP certification **35%**
- My agency gives preference to FedRAMP compliance vendors, but will occasionally consider other solutions **28%**

The Benefits of Cloud and How to Direct Resources at Mission Goals

An ideal cloud transition requires the right people, the right industry partner and the right implementation strategy. But most of all, a smooth transition needs to start with a defined goal.
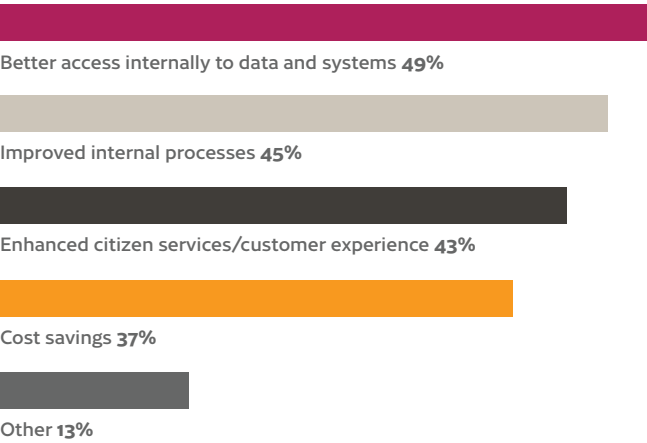
The benefits accrued from cloud technology are vast and highly dependent on agencies' goals. Of government respondents, 45 percent enjoyed improved internal processes, 49 percent received better access to internal data and systems and 37 percent saved costs by using cloud services (See Figure 6).

No matter why they went to the cloud, 43 percent were able to offer better CX or citizen services, a top three priority. As nearly every agency has an end focus on improving customer experience, such as reducing wait times and improving service functions, they need new solutions (See Figure 6).

Agencies, often held back by legacy systems, might expect cloud to pay immediate dividends in some of these categories. Data visibility, for example, improves when cloud technologies can raze decades-old silos between different departments, which in turn can increase collaboration and communication. Fewer costs can also be anticipated when government can offload expensive hardware that requires repairs, staff and energy, and instead buy IT as a service via the cloud.

Customer experience is improved on both ends by the other rewards of cloud as well, because cost savings trickle into agency missions and improved data tears down expensive barriers to analysis. But better CX also requires a concerted effort on behalf of agency leadership when considering cloud technologies.

FIGURE 6: If your agency is using cloud products and services, what benefits have you reaped so far? Please select all that apply.

Better access internally to data and systems **49%**

Improved internal processes **45%**

Enhanced citizen services/customer experience **43%**

Cost savings **37%**

Other **13%**

When asked, 65 percent of government employees said that customer experience is a priority at their agency (See Figure 7). Of those, 55 percent said cloud played a "very significant" part in their CX efforts. Another 37 percent said cloud was a "somewhat significant" element of their CX efforts (See Figure 8).

That's no surprise. While cloud technologies present unexplored possibilities of all kinds to agencies, CX in particular can be unlocked by going off-premise. Social media monitoring and chatbots can be introduced to agencies' CX strategies when agencies move from legacy systems to dynamic cloud environments.

"They see that cloud will enable them to keep pace with the expectations of citizens," Thompson said. "If I can do it in the private sector, why can't I do it in the public sector?"

In interactive voice response systems, cloud-based speech recognition and collapsed menus can dramatically reduce process times. All the while, agencies are able to monitor their systems with up-to-date, precise data. For many, this represents a major improvement.

Legacy systems can leave agencies blindly selecting applications and CX strategies, without having the means to evaluate whether they're meeting their goals. Worse, they might receive negative feedback at the end without

being able to diagnose the problem.

The right cloud solution can solve that.

"That analysis actually helps dovetail into the enhanced CX [and user experience] portion of it, because the best way to improve a system is to measure it," Greene said.

FIGURE 7: *Cloud computing is often a key driver of better customer experiences (CX) in government. Is CX a priority at your agency?*

■ **Yes 65%**
■ **No 35%**

FIGURE 8: *If yes, how significant is cloud to your CX efforts?*

■ **Very significant 55%**
■ **Somewhat significant 37%**
■ **Not significant 8%**
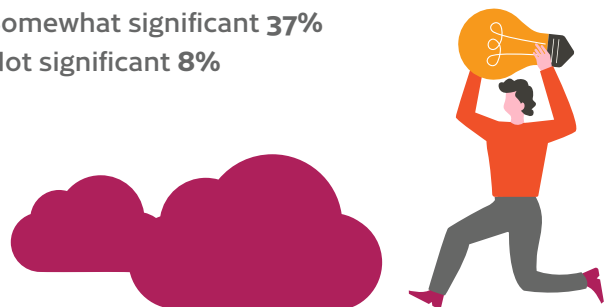
Why Improving CX Is Important, and How to Do It Securely

With cloud, agencies can also rotate their focus from constantly repairing and maintaining obsolete – albeit familiar – legacy systems to projects that directly impact citizens, furthering the benefits of cloud technologies. For example, when an IT department can direct its attention to adding new online features, reducing wait times in call centers using analytics or enhancing a digital service, customer service markedly improves.

The biggest pain points of CX are telling examples of why the right cloud strategy can solve chronic issues for agencies. Respondents identified the following pain points (See Figure 9):

- Data silos 39%
- Disparate CX solutions 32%
- Gaps in IT security 46%
- Lack of leadership/buy-in 37%
- Lack of budget 47%

The cloud directly addresses budget, which can divert hardware costs to software, but the 46 percent of respondents who cited gaps in IT security can also refocus their attention.

FedRAMP can appease those for whom security is a pain point for CX. Comparing FedRAMP certifications and impact levels to their ATO requirements, agencies can rid themselves of traditional security burdens. That effort can be refocused toward CX.
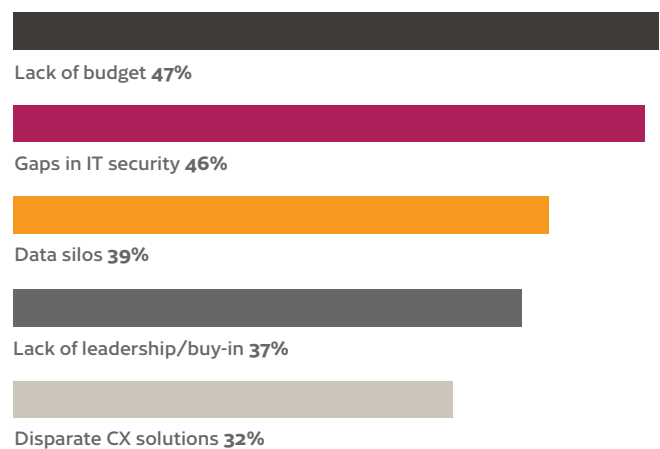
Finding a FedRAMP solution, agencies not only get the power of the cloud, but they can reallocate spending that would have gone toward IT security.

Greene said that as long as agencies are familiar with the FedRAMP impact level they need, security discussions are simple. A majority of respondents (54 percent) said that their CX strategy requires that they host or share sensitive data (See Figure 10).

With the right solution in place, however, agencies not only can ensure the quality and protection of their data, but they can make use of it across multiple platforms. Communicating data across departments can streamline customer service by creating profiles of information for each user.

"For example, if someone is applying to child support services, that's a financial conversation," Thompson said. "But if they're also applying for public assistance, there needs to be an adjustment made. And these two departments, though separate, need to speak and be aware of each other."

FIGURE 9: *What are your biggest pain points when it comes to improving CX? Please select all that apply.*

Lack of budget **47%**

Gaps in IT security **46%**

Data silos **39%**

Lack of leadership/buy-in **37%**

Disparate CX solutions **32%**

FIGURE 10: *Does your current CX strategy require you to host or share sensitive date?*

- Yes **54%**
- No **46%**
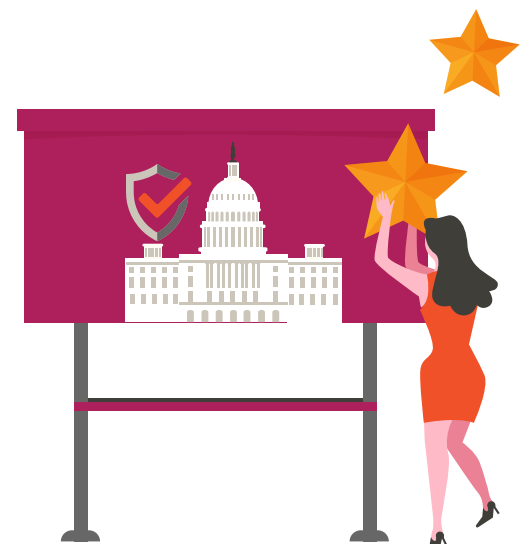
Crafting the Right Cloud Strategy for CX

While some environments are better prepared for cloud transitions than others, there are tips that apply across agencies for finding the right solution to improve CX. Cloud solutions shouldn't be generalized or templatized, however. They have to be case-tailored. Here are three best practices for finding a secure cloud solution with the tools to improve CX.

Define your goals and reasons for moving to the cloud.

It can be difficult to articulate exactly why the cloud can help, but just because everyone else is doing it doesn't mean it's right for your agency. Have an educated discussion about CX goals and areas for improvement, and if there are problems of backload, data-sharing and system optimization, then the cloud might be right.

"It's all about the best practices and the business outcomes when you move to cloud," Greene said. "It's no longer a thing about the system."

Although cloud's potential is powerful in government, an agency's capabilities and pain points also constrain it. In homing in on specific use cases for cloud adoption, agencies can approximate what the benefit of cloud adoption might be.

Consider all stakeholders and different perspectives.

Cloud solutions come in all shapes and sizes, so it's important to have an idea of what you might want. Engaging all interested parties is good policy from the start, as it prepares and energizes the workforce. Cloud migrations represent a fundamental shift in workflows and personnel management, and while new capabilities are welcome, oftentimes bumps do come along with the process.

Business leaders who decide that cloud can accelerate mission progress need to communicate with IT along the way and clearly define milestones for CX and the end goal in their strategy.

Agencies also should understand what level of security they need to meet, based on the sensitivity of their data. FedRAMP levels exist for a reason, and it's important to map your security needs back to those baseline requirements and determine if additional measures

should be taken. If the aim of cloud adoption is to improve CX, then the maximum amount of time and funding resources generated by cloud investments should be redirected toward CX.

Find the right technology partner.

While the cloud represents a technological change, it also embodies something more: a new way of doing business. Agencies that go to the cloud must have a clear direction and invest in employee training and workflow transformation, or they risk adopting a technology that fails to address their crucial needs.

Partnering with the right cloud service provider will assist agencies in the process. By alleviating the security requirements of the migration, the industry partner can show agencies where to redirect their attention.

One advantage of the cloud is the incorporation of advanced metrics. Cloud service providers should be able to review these with agencies during their cloud journey, to explore possibilities for future efficiencies and treat any problems that might come along the way.

By analyzing the incremental gains and losses of a CX, strategy, agencies can be sure to maximize the power of cloud technologies.

How Genesys Helps

Genesys is a leading provider of customer experience solutions in government. With fluid and compatible cloud-based platforms, Genesys can eliminate longstanding silos in customer service and enable the newest technologies. Offering advanced analytics, Genesys helps its customers track the success of CX campaigns and products.

"We go the extra step," Thompson said. "We're encouraging the client and collaborating with them to look ahead and determine what they're trying to achieve, versus simply replicating the status quo."

In terms of security, Genesys can offer FedRAMP/DoD-certified Impact Level Four security. Impact Level Four means that the cloud service provider is approved to work with unclassified, sensitive data – including military data.

Providing assistance throughout the cloud journey, Genesys supplies its government partners with use cases, best practices and lessons learned from managing CX experiences.

Conclusion

Customer experience has undergone a technological revolution, and cloud is powering it. With guidance from the White House and acts of Congress, adoption of the cloud will continue to proliferate across government, and that's good news for CX. By harnessing cloud capabilities, CX solutions are up to date for the mobile and social media era.

Agencies need to do their research to find answers, and fortunately, there is help along the way. FedRAMP provides a measuring stick for service providers, and agencies can compare what they need with FedRAMP compliance and impact levels.

The right service providers will also assist cloud journeys with cultural and technical instruction, while shouldering the security responsibilities. Then, agencies not only have the technological capabilities to deal with CX; they have the time and resources as well.

The public sector has consistently earmarked CX as a top priority, and with cloud, agencies can serve citizens like never before.

GENESYS™

govloop

About Genesys

Genesys® powers 25 billion of the world's best customer experiences each year. Our success comes from connecting employee and customer conversations on any channel, every day. Over 11,000 companies in 100+ countries trust our #1 customer experience platform to drive great business outcomes and create lasting relationships. Combining the best of technology and human ingenuity, we build solutions that mirror natural communication and work the way you think. Our industry-leading solutions foster true omnichannel engagement, performing equally well across all channels, on-premise and in the cloud. Experience communication as it should be: fluid, instinctive and profoundly empowering.

To learn more, visit www.genesys.com | @Genesys

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop