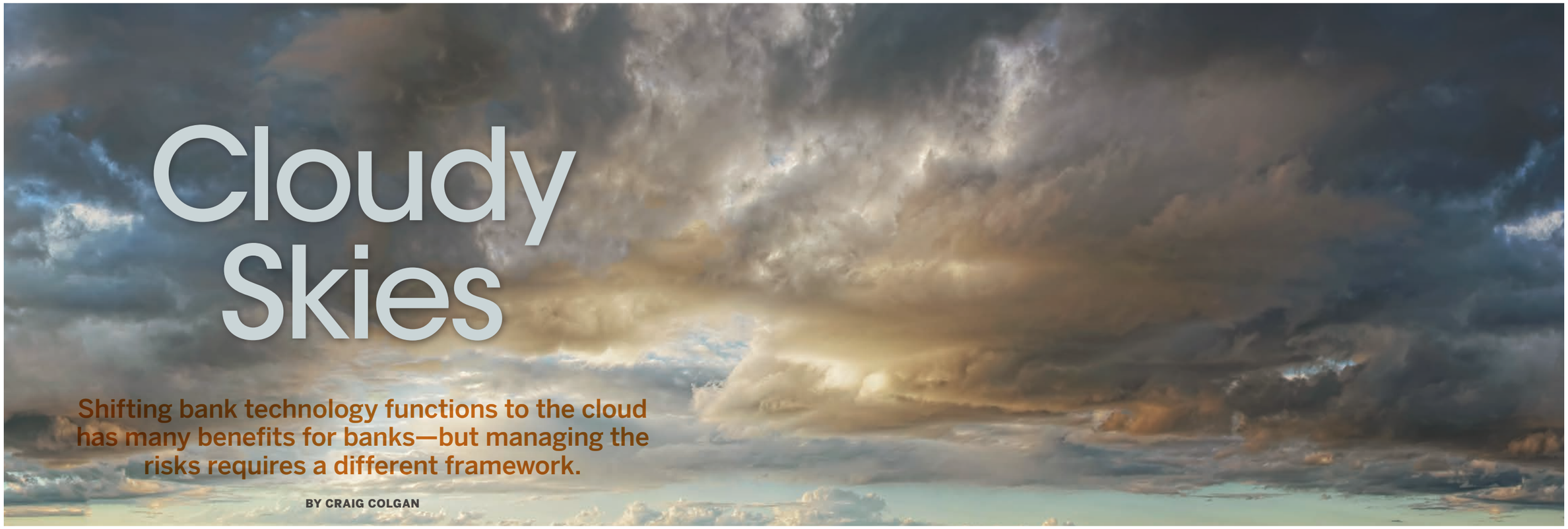

Cloudy Skies

Shifting bank technology functions to the cloud has many benefits for banks—but managing the risks requires a different framework.

BY CRAIG COLGAN

The day before Kish Bank in central Pennsylvania planned to break ground in October on a $10 million building it calls an innovation center, the bank's president and COO reflected on all that went into what is an enormous project.

And on all that is ahead.

"It's been a long process to this point," says Greg Hayes, president and COO of the $850 million bank, headquartered in Belleville with executive offices in State College. And the building may not even be the major piece.

"Once this is built, then it's on to more planning and to implementing," he adds. "It's a big change. Team members who work out of this facility are going to support a more digital but still very physical and very relationship-based local experience." Hayes talks frequently about finding better ways to serve his customers, and about refining "digital but physical" branch-of-the-future models.

Kish Bank is making a major commitment to next-generation banking. To fuel these changes, the bank is migrating multiple systems to cloud-based solutions. These include hardware infrastructure, productivity software, core platform, even a phone system. Those main cloud providers for the new Kish Bank include Amazon Web Services, Microsoft Teams and Office 365, data backup and recovery solutions, and for its core banking CSI.

"This enables our employees to meet the needs of our clients basically from anywhere at any time through faster, more reliable technology that is easier to get to and more intuitive to use," Hayes says.

Bankers from across the country reach out to him and to his team regularly, inquiring about how all these changes are progressing. The topic of many of the questions: risk. Hayes starts his answer by pointing to his bank's DNA and then to the perpetual monitoring culture that has become second nature.

"We've been strategic planning for 38 years," Hayes says. "Our cloud journey is actually part of a much larger strategy that reimagines our entire technology approach. Every year we are identifying these threats and these opportunities. It will be great when this part of it all comes to fruition. But really, it's never going to stop."

Partnering to solve the culture clash

Economist Tyler Cowen says the U.S. is on the verge of "a golden age of financial innovation." Increasingly for many banks, of just about all sizes, that golden path forward means committing valuable resources—such as time, dollars, and personnel—to cloud.

Cloud service providers offer outsourcing of computing infrastructure and data storage, but also convenience, expertise, specialized personnel, flexibility and what IT experts call "resilience." Moreover, cloud services increasingly promise to execute and deliver quickly on a host of needs and applications and enhancements requested by banks. Other advantages: greater access to advanced analytics and artificial intelligence tools.

SEBOS/SHUTTERSTOCK.COM

So what's the holdup? One problem is that only one in four banks has a defined cloud strategy in place, according to Accenture research. Another problem is that the banking industry, while a leader in cybersecurity, faces distinctive risk across additional zones when it comes to cloud banking. And the service providers are finding themselves on the hot seat in Washington, learning to interact with regulators in a way that is much more familiar to the supervised financial sector.

In April, Federal Reserve examiners surprised staff at an Amazon Web Services facility in Richmond, Va., the *Wall Street Journal* reported. The examiners were allowed to review certain documents but did not remove any. The episode "points to a culture clash between government and big tech," which has been far less regulated than the financial sector, the paper reported.

Other culture clashes are not uncommon as cloud banking arrangements expand—for smaller banks in particular. Paul Benda, ABA's SVP for risk and cybersecurity policy, worked with a small bank recently that told him about the problem it was having getting a major cloud provider to provide information for some basic regulatory filings.

"It's a formal document the bank needs to present to the regulators to show they are doing due diligence with third-party providers," Benda says. "The attitude from the cloud provider was: 'Why do I have to fill out this thing for *you*?' From the bank's perspective the provider's attitude was, 'we don't need you. Especially since you are a small bank'." The bank got the information it needed eventually, but it took several months, Benda says.

> **"Our cloud journey is actually part of a much larger strategy that reimagines our entire technology approach. Every year we are identifying these threats and these opportunities. It will be great when this part of it all comes to fruition. But really, it's never going to stop."**
>
> *—Greg Hayes, Kish Bank*

ABA SVP Paul Benda testifies on cloud service providers before the House Financial Services Committee.

Firms called shared assessment providers, recently started by banks, aim to solve some of this confusion, by providing processes to simplify regulator-required vendor reporting, assessment and validation.

Benda recently testified before the House Financial Services Committee and offered hope for a positive way all parties can better address risk issues in cloud banking. "We believe there is potential for financial institutions, CSPs and regulators to collaborate on a best practices model to provide standardized terms and conditions that provide financial institutions access to required audit and control data," he told the panel. "The challenges in this space are complex, and we believe that every stakeholder wants to ensure that the security of these critical systems is maintained and at the same time innovation is not hindered."

Ben Wallace—a former banker and partner at Summit Technology Group, a firm assisting banks on their cloud projects, including Kish Bank—says he is seeing more meeting of the minds from implementation to regulatory awareness to risk management at all levels between cloud service providers and banks. One motivator for CSPs: reputation risk exposure from news coverage of major data breaches.

"While they have no responsibility or obligation, [major CSPs are] now beginning themselves right on their own accord to look at your infrastructure" and offer advice on ways to mitigate risk and maximize performance, Wallace says. "I think what we are starting to see is they are trying to help these customers. Because these cloud providers are seeing best practices, for all concerned, and even though there is no legal obligation, they are more and more trying to be good stewards."

Congress is beginning to notice as well. Two House members recently requested that the three leading CSPs—Amazon Web Services, Microsoft and Google Cloud—be designated as systematically important financial market utilities, so they could be regulated under Title VII of the Dodd-Frank Act. How this all could affect banks themselves remains unclear.

The monitor culture has arrived

Bank leaders and decision makers may have to occasionally cut through some lingo to figure this out.

The thing to avoid: "Disparate risk methodologies across multiple traditionally siloed risk functions."

The thing you want: "A robust risk governance framework."

These are the very specific words of Paul Sussex, digital and financial services cloud leader at EY Americas. Having worked with financial services clients for a quarter century, Sussex says banks must first broaden the way they think of risk when considering cloud services. "As banks start to enable more critical business use cases with cloud technologies, they need to refine their risk management capabilities across multiple fronts," Sussex explains.

"Monitor the service provider," adds Scott Sargent, an attorney and head of the financial services group for the law firm Baker Donelson, which advises banks on major cloud contracts. "This is where banks are the most vulnerable. If the service provider is providing a crucial component, many banks think that they monitor the service provider every day by just seeing the process work as expected. It is important to monitor contract performance and service level agreement, but not looking beyond that is a dangerous trap and it can cost the bank."

> **"As banks start to enable more critical business use cases with cloud technologies, they need to refine their risk management capabilities across multiple fronts."**
>
> *—Paul Sussex, digital and financial services cloud leader at EY Americas*

Sargent suggests asking: What if a disaster struck the service provider? Does the provider have adequate insurance coverage? How does the provider audit itself? For high-risk or critical vendors, visit the provider's facilities, he suggests. Finally, contracts should be evaluated by a lawyer who is familiar with applicable vendor management rules and guidance.

One of Kish Bank's largest risk hedges is simply how the bank's entire upgrade project is conceived and then executed.

Hayes calls his bank's new cloud arrangement "hybrid," in that it is composed of both on-premises versions of virtual servers and desktops, as well as a hosted public cloud-based version. "So if the future of cloud does not play out or we have *unforeseen* risks, we can migrate easily back to an on-premises solution," Hayes said. "Or if we find that cloud is much easier to manage, much more effective and efficient, we can utilize the on-premise solution as a backup and go full cloud solution."

Other risk mitigating steps Kish Bank has taken include shorter-term contracts with providers. This might mean higher costs in the short term, he admits, against the upside of the flexibility to get out or move to another provider. Staffing is a risk too, as decisions about just which tasks and responsibilities are to be outsourced will become a continual challenge.

Kish Bank's cyber and information security program also gets a complete refresh through the use of real-time automated reporting and alerts to ensure that threats to customer information and systems are identified and eliminated.

"It's that technology sophistication that's driving a more mature cybersecurity program," Hayes says. "You can't do one without the other."

Craig Colgan is a staff writer at the ABA Banking Journal.

Greg Hayes (holding shovel, right) breaks ground on the Kish Innovation Center.