CIO THINK TANK
FROM IDG

CIO Think Tank Roadmap Report:

Setting the Multi-cloud Agenda

How can enterprises handle the increasing complexity of multiple clouds – and reap unprecedented benefits? In a series of virtual roundtables, dozens of IT leaders identify obstacles, highlight best practices, and challenge the tech industry to help navigate the road ahead.

In June 2020, CIO held its first CIO Think Tank, a series of virtual roundtables that brought together 30 IT leaders to unpack one of the most important issues in enterprise technology today: managing multiple clouds. The roundtables also included IDC Research Director Deepak Mohan, IDG B2B Editor-in-Chief Eric Knorr, and cloud executives Deepak Patil and Bradd Lewis from Dell Technologies.

The objective of these discussions was to identify the key challenges associated with multi-cloud management and to offer a roadmap for IT leadership — as well as the technology industry — to overcome those obstacles. All participants drew on their own experience and knowledge to describe strategic and tactical approaches to selecting, provisioning, and maintaining multiple clouds for maximum business and IT benefit.

Multi-cloud is so new and evolving so quickly that the panel participants were not in universal agreement about its definition. Yet a consensus emerged: Multi-cloud has evolved to embrace not just multiple public IaaS (infrastructure as a service) and PaaS (platform as a service) clouds, but also private, on-premises clouds. The only substantive disagreement was whether SaaS (software a service) should also be included; most thought it should be.

All 30 participating IT leaders were in the financial industry, where security, availability, and regulatory compliance are paramount (see the Participants list on page 9). With the intent of providing guidance amid constant cloud flux, this report captures and consolidates the thinking of forward-looking IT leaders in a complex multi-cloud world.

WHAT IS CIO THINK TANK?

CIO Think Tank is a unique collaboration showcasing the ideas and expertise of top IT executives, IDC analysts, IDG editors and our exclusive vendor partner. Our goal is to explore and shape the future of emerging technologies. Dell Technologies is IDG's partner on this Multi-Cloud CIO Think Tank. For more on this program go to **www.idg.com/product/cio-virtual-think-tank**.

Motivations for multi-cloud

As IDC's Deepak Mohan stated, for most companies, the two basic reasons to adopt cloud computing in the first place are well known: "Flexibility, which is the underpinning of agility and the ability to map your infrastructure to your business needs at all points in time; and resilience, which is growing in importance as companies increasingly deploy more business-critical workloads and operations based on public cloud backends."

In our multi-cloud world, the leading clouds tend to offer roughly equivalent computing, storage, and networking capabilities. Therefore, the type and suitability of more advanced services may play an outsized role in determining which clouds an organization chooses.

"The thing that's driving adoption of off-prem solutions is … feature functionality that's richer than infrastructure," said Bradd Lewis, a vice president of the financial services practice at Dell Technologies.

Navdeep Singh, vice president of cloud and cybersecurity for the financial services technology firm Fiserv, offered a simple example. "If you're looking for an enormous amount of data transfers, then there is a certain provider that excels in that kind of an offering, versus another that has more high-tech, artificial intelligence, machine learning capabilities," Singh observed.

Mohan Putcha, vice president of digital transformation, architecture, and product strategy at the professional services provider Aon, noted that multi-cloud selection based on services is not always "strategic in nature," particularly when developers are involved. "We have to be native AWS [Amazon Web Services] because of such reasons as their advanced capabilities in analytics," Putcha said. "And we have to be in Azure because, frankly, developers love that ecosystem, and productive developers are probably the best thing."

Then there's the reluctance, in an era of accelerating cloud adoption, to become dependent on one cloud alone. Singh and seven other roundtable participants stated that not being locked into a single provider was a key motivator for going multi-cloud.

The ability to choose among similar cloud services offered by multiple providers based on price was another driver. Chris Gates, CTO for Allstate, went so far as to say he aspired "to opportunistically place workloads wherever I want, almost as a spot market," although he acknowledged that "we're years away from that."

Another motivator for multi-cloud was, in at least one case, an explicit mandate from the customer.

"The main driver is what our clients are asking for," said Greg Scher, vice president of bank solutions at Fiserv. "We have banks who have an Azure preference; we have banks who have an AWS preference, Google Cloud, and on and on. We don't really get to choose."

Last but not least, some regulations require that organizations keep sensitive data on premises, such as in a VMware-based private cloud.
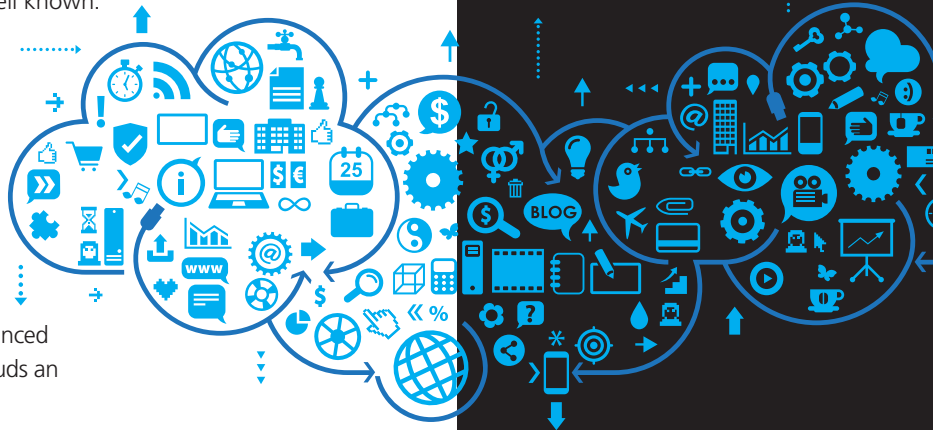
REASONS FOR MULTIPLE CLOUDS

The reasons organizations turn to multiple clouds vary widely. Among the roundtable participants, the motives fall into five categories:

1. A need for specific cloud services.
2. "Bottom-up" cloud demand.
3. Avoidance of lock-in.
4. Cost reduction.
5. Specific customer or regulatory requirements.

USE MULTIPLE PUBLIC CLOUD IaaS PROVIDERS

2019
62%

2018
57%

Source: IDC
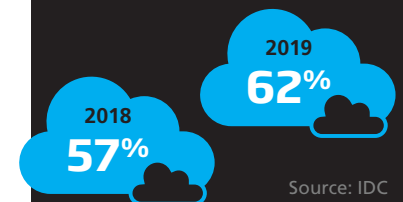
Multi-cloud challenge No. 1:
Governance

Every experienced IT leader knows what it's like to manage disparate systems and platforms. But dealing with multiple clouds — particularly those that include a broad range of PaaS functionality — raises the ante, because they are essentially vast ecosystems of services. Developers and/or lines of business within organizations have been known to go off on their own to build cloud applications or consume public cloud services without IT's knowledge, let alone blessing.

"I hate to use the word governance, because I know that has a negative connotation," said Ryan Brown, chief enterprise architect for cloud at Visa. "I'm not saying to put handcuffs on my developers if they say something new is great in Cloud XYZ, but we need to have some guardrails."

"Look, 'governance' is the right word, but we've also got to play that up against agility," added Aon's Putcha. "I did try, to be honest, to be very heavy handed and governance oriented, and we just didn't move fast, because then we have 20 people with an opinion and a decision by committee, and absolutely nothing took place."

That clampdown was in response to "people going off on their own," which led to wasted money and effort along with the risk of exposing data in unmanaged cloud ecosystems. Today, Putcha has taken a middle path: policy-driven, self-service automation.

"You get to do whatever you want within this space, but we limit the blast radius," he said.

"There's good governance and bad governance," said Richard Wiedenbeck, CIO at the insurance company Ameritas, who, like Brown, prefers to avoid the G-word due to its "negative connotations."

Instead, he said, "We have a sign we put up that says, 'We want to make well-informed, thoughtful and purposeful decisions about technology balancing cost, risk and value.' That's a mantra for everybody. It can't be, 'I just want my thing.'"

> *"You get to do whatever you want within this space, but we limit the blast radius."*
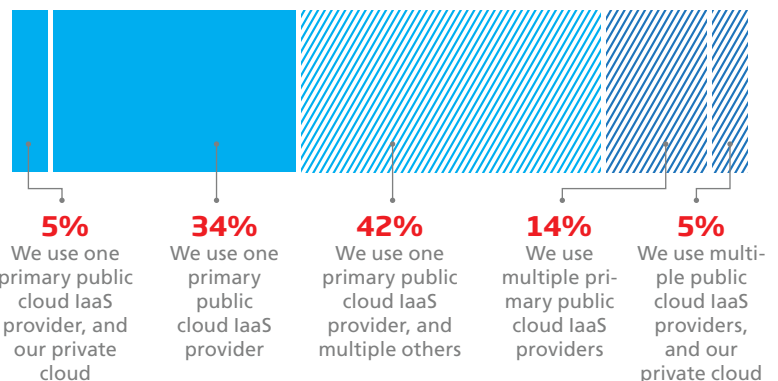>
> — MOHAN PUTCHA[4], Aon

MULTI-CLOUD GOVERNANCE RECOMMENDATIONS

Thomas Sweet, vice president of IT solutions at GM Financial, introduced a phrase the round-table loved: "minimum viable governance." His organization is working toward that goal "with guardrails and setting up a cloud system where, if you go to the cloud, you will have less restraints than if you were to go on-prem." But like Putcha and others, Sweet limits choice through a catalog of approved services. No one in his company, he said, can simply pull out a credit card and pay for a cloud service.

CHARACTERIZING COMPANY'S APPROACH TO USING PUBLIC CLOUD IaaS SERVICES

One primary public cloud IaaS — 81% (87% in 2018)

Multiple public cloud IaaS — 61% (57% in 2018)

5%	34%	42%	14%	5%
We use one primary public cloud IaaS provider, and our private cloud	We use one primary public cloud IaaS provider	We use one primary public cloud IaaS provider, and multiple others	We use multiple primary public cloud IaaS providers	We use multiple public cloud IaaS providers, and our private cloud

Source: IDC

Multi-cloud challenge No. 2:
Interoperability

Every cloud has its own way of doing things, resulting in a lack of interoperability that was problematic for most of the roundtable participants.

Eddie Contreras, chief information security officer and executive vice president at Frost Bank, lamented that "you get these really good vendors, and they have some really good development platforms, but they don't work well with others."

Sankara Ramakrishnan, principal architect at MetLife, agreed: "If you want to move from one vendor's platform with a capability to another vendor's platform … you virtually have to rewrite those applications."

Likewise, FINRA Chief Information Officer Steve Randich has a substantial investment in an AWS analytics implementation that, for practical purposes, can't move anywhere else.

"It would be very difficult for us to take all of our big data processing and 200 petabytes of data and move it over to Azure without major re-architectures and major re-automation and rebuilding our security infrastructure, among many other things," he said.
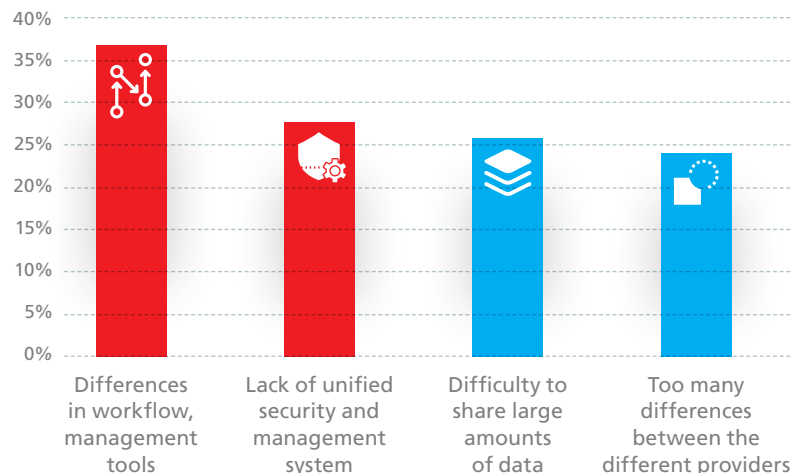
"There is a lack of standardization today," asserted Fiserv's Singh. "I think we all feel and see that. A workload running in an X manner on one cloud platform will run in a different manner on another. If you had standards, that would obviously be a propellant for anybody to get ready to embark on this journey of multi-cloud."

> *There is a lack of standardization today, I think we all feel and see that. If you had standards, that would obviously be a propellant for anybody to get ready to embark on this journey of multi-cloud.*
>
> — NAVDEEP SINGH, Fiserv

TOP CHALLENGES WITH USING MULTIPLE PUBLIC CLOUD IaaS PROVIDERS

Differences in workflow, management tools	Lack of unified security and management system	Difficulty to share large amounts of data	Too many differences between the different providers

Source: IDC

Multi-cloud challenge No. 2: **Interoperability** *continued*

Allstate's Gates agreed. "I think there has to be something established for a way to describe what needs to be in place for you to be able to actually place workloads anywhere," he said. "If not, I'm reinventing it every time." Even differences in cloud nomenclature cause problems. "We've got to come up with a way of being able to talk about this or we get caught up in semantics. Oftentimes, you find yourself in violent agreement, but you're talking about two totally different things."

IDC's Mohan saw the interoperability issue as a tension between two extremes. On the one hand, you can maintain a certain degree of portability by restricting yourself to features that are similar across all the clouds. On the other, you can "hypercustomize" applications by "choosing a service which is ideally suited for this particular use case, the implicit assumption being that same service isn't available everywhere else." Unfortunately, such proprietary features also tend to be the cool, new stuff.

That last point was not lost on Sandeep Aich, vice president of cybersecurity and IT risk at Prudential. "As we roll out more and more products in the cloud, we are beginning to realize that native tools for the vendors give better performance, give better features, which also leads to more vendor lock-in," he said.

Sigal Zarmi, head of transformation for Morgan Stanley, did not see the choice between native and relatively generic cloud features as an either/or proposition. "We will have places where customization will be great because we need the efficiency, and we need those services to be embedded," she said. "There are going to be other solutions or workloads where we think we need to be portable … for resiliency purposes or whatever."

> *We've got to come up with a way of being able to talk about this or we get caught up in semantics. Oftentimes, you find yourself in violent agreement, but you're talking about two totally different things.*
>
> — CHRIS GATES, Allstate

MULTI-CLOUD INTEROPERABILITY RECOMMENDATIONS

Several roundtable participants called on the industry to get serious about cloud standardization.

"Cloud providers should start exposing their services as APIs or simply adopt some industry standard so we could adopt these functions" across cloud providers, said Gautam Roy, senior vice president and chief technology officer at the insurance provider Unum. Yet, there was also skepticism.

"I actually don't think we're going to see a lot of standardization from the different cloud providers," said Walt Carter, **chief data officer** and chief information officer for Homestar Financial. **"I don't see them going away from their current strategies of locking us into their services. Any drive toward portability and flexibility is going to have to come from us."**

Regardless, in the immediate term, adopting evolving open-source solutions that work across multiple clouds can help.

"I think the main thing, when we look at designing a solution architecture, is to look at the open source competence as much as we can rather than a specific vendor implementation," said FINRA's Randich.

Docker containers, along with the open-source container orchestration project **Kubernetes,** which all the public clouds now support, provide a partial solution. As IDC 's Mohan said, **"What you're seeing is that ability or desire to have Kubernetes play the abstraction layer between different cloud providers."**

Dell Technologies' Lewis added that Kubernetes is now supported on the VMware platform, enabling hybrid scenarios in which containerized applications can be moved between private and public clouds.
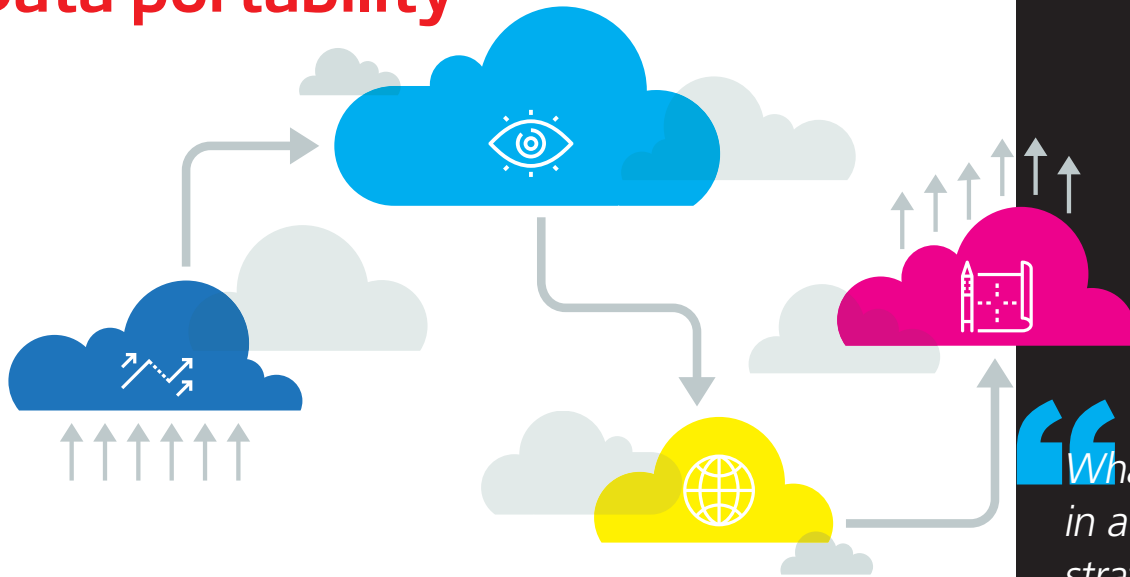
Multi-cloud challenge No. 3:
Data portability

Thanks mainly to open-source applications, application portability is at least becoming feasible. Porting data from one cloud to another, however, is a headache. Part of the problem is the way cloud providers encourage customers to upload data while charging heavily for data going out. The other difficulty is architectural: How do you distribute and synchronize data that might be used for multiple applications across multiple clouds?

"Certainly, that's our biggest pain point," said Kalika Gupta, vice president of IT for Cetera Financial Group. "We have platform providers in our wealth management space. From there, we need to get data, and many times, the data is replicated 10 times over. How do we consume that data in a fashion where we don't have to replicate it in six different systems?" She adds that "how quickly we move data among multiple different providers and platforms" is a high-priority issue that directly affects agility.

"Data governance is huge, huge, huge for everybody," said Visa's Brown.

He went on to describe that, in Visa's business, data by nature flows among different providers and environments in various private and public clouds. Based on his own experience, he raised fundamental questions that applied to many of the participants: "Where does the data live? How can we observe it? When something goes wrong, how can we recover quickly?"

"Data has gravity," Aon's Putcha said. "You are going to end up investing a lot of time managing and securing your data. We don't yet have a solution to move data around."

"The data part is now where the real complexity is starting to run into things," said Dell Technologies' Lewis, "especially in governed and regulated industries, and especially when you're starting to think about the volume of data and also the proportion of cost that a platform typically takes up with the movement of data back and forth. If you want to start to have the true portability of applications, obviously, the data has to go with the application."

> *What I'd like to see in a multi-cloud strategy from our cloud providers is some mechanism for enabling movement of data in a way that's not punitive to us financially.*
>
> — GREG SCHER, Fiserv

MULTI-CLOUD PORTABILITY RECOMMENDATIONS

The roundtable strongly agreed with a blunt statement from Fiserv's Scher. "What I'd like to see in a multi-cloud strategy from our cloud providers is some mechanism for enabling movement of data in a way that's not punitive to us financially," he said. "I think that would actually incentivize us more to share things, to leverage best of breed."

Multi-cloud challenge No. 4:
Security

Differences among clouds also can hamper effective data security. No one is concerned about the resilience of the major clouds in the face of attack. The variations in security controls from cloud to cloud, however, can increase the risk of a data breach, because a company's internal security model needs to be emulated on each cloud in a different way. Along the way, cloud customers need to observe differences in regulatory compliance across different geographies.

For Fiserv's Singh, the challenge is clear. "In a multi-cloud environment, how do we ensure that our overall security fabric that we have at an enterprise level gets mapped to the distributed workloads across various geographies?" he asked. "Also, at the same time, what is that consistent and repeatable manner with which our associates — or anybody, for that matter — are accessing those environments?"

"We have billions of dollars of transactional data as it relates to the mortgages coming through the Freddie Mac system," explained Bhavini Amin, vice president for single-family business services at Freddie Mac. "For us, information security is our number-one priority, so we need to use the right controls, the strong processes internally to make sure that we can take advantage of a multi-cloud strategy."

For Manish Desai, senior information risk officer for BNY Mellon, the emphasis is on compliance across multiple clouds. "We look at this from a data residency perspective and from a regulatory standpoint," he said. "We know that the regulatory regime is getting more and more strict. That is where the focus is."

At Frost Bank, Contreras is focusing on privacy mandates. "I think that's going to help us understand what some of our expectations are from a risk perspective," he said. "So, when you're in a cloud, when you're geolocated or when you're sharing data, privacy [should be considered] at the design stage."

> *For us, information security is our number-one priority, so we need to use the right controls, the strong processes internally to make sure that we can take advantage of a multi-cloud strategy.*
>
> — BHAVINI AMIN, Freddie Mac

MULTI-CLOUD SECURITY RECOMMENDATIONS

The ideal multi-cloud security scenario is clear. Jeff Farinich, vice president of infrastructure and security for New American Funding, said that a definition of success would be to "allow the different IT groups and business teams to put a workload in any cloud environment they want with the same security policies, and then be able to move that workload around as needed."

Farinich may need to develop that solution on his own, however, given that cloud providers seem unlikely to standardize their security controls anytime soon. Meanwhile, Aon's Putcha recommended that IT leaders involve the security folks in a multi-cloud strategy from the get-go.

"Invest heavily in partnering with your privacy organization, your cybersecurity organization," suggested Putcha.

Paul Hamman, senior vice president of cybersecurity at the bank holding company Truist Financial, took that a step further. "If we haven't run the service through our service adoption framework where we start to provide patterns on how to use the service securely and also map it over to controls for compliance reasons, then we essentially disable the service," he said.

Multi-cloud challenge No. 5:
Cloud management solutions

The complexity of maintaining multiple clouds with all their intricacies and differences can be exhausting. So why not consolidate all of that management in one place?

"The panacea … is to have that single pane of glass and know that, when I'm building this application, that I can move that workload to where it makes the most sense," said Visa's Ryan Brown.

Unum's Gautam Roy echoed that sentiment. "We need governance, control, monitoring, and security to be abstracted to a single pane of glass so that we can use it seamlessly across various clouds," he said.

Paul Hamman at Truist Financial has had a similar dream for some time. "I was thinking about this eight, nine years ago, when we were first starting out, that it would be great if I could have something that automatically moved my workload to whoever was providing the cheapest virtual machine."

True, multi-cloud management solutions already exist. But Jeff Farinich at New American Funding has looked at several commercial offerings — including Morpheus, CloudBolt, and Flexera's Optima — and has found that "each of those products has some gaps, and there's no great solution."

Allstate's Chris Gates sees the need for better multi-cloud management solutions as well, although he wonders about scale. "I think there's a lot of small to medium-sized businesses that would benefit heavily from having that service," he said. "Larger enterprises, I think, just have to figure out how to take responsibility."

> *I think there's a tremendous opportunity for software vendors to really step up their game and build the CMP [cloud management platform] of the future that really does solve these multi-cloud problems.*
>
> — MATT MCCOMAS
> GM Financial

MULTI-CLOUD MANAGEMENT RECOMMENDATIONS

The roundtable participants were divided on the viability of third-party, multi-cloud management solutions.

Matt McComas, devops engineering leader at GM Financial, issued a direct challenge to the industry: "I think there's a tremendous opportunity for software vendors to really step up their game and build the CMP [cloud management platform] of the future that really does solve these multi-cloud problems. I still feel like it's sort of up for grabs."

Others see a risk in vesting so much responsibility in another third party. "The thing is that, as soon as you go to a cloud broker, you've now done exactly what you were trying not to do with doing a multi-cloud, which is vendor lock-in," said Truist Financial's Paul Hamman.

"I was thinking the same thing," said Cetera's Kalika Gupta. "Now, you've taken this whole thing for which you should have inherent capability in-house for a large corporation, and you've outsourced it to a third-party provider thinking everything will be fine. But how do you know?" she asked. "Now you're locked in — or maybe you're held hostage, if there are just one or two providers in that space."

Homestar Financial's Walt Carter gets the last word. "I think we've got to find our own way to — if not a single pane of glass to look at all of these different structures — then we've got to be comfortable with multiple panes of glass, because I think that management responsibility for those workloads is all up to us."

Participants

Paul Hamman, SVP, Cybersecurity Architecture, Strategy, Digital Transformation, and Cloud Security, Truist

Gautam Roy, SVP and CTO, Unum

Chris Gates, CTO, Allstate

Kalika Gupta, VP IT, Cetera Financial Group

Lee Ann Murray, CIO, Global Wealth and Asset Management, John Hancock

Bhavini Amin, Vice President, Business Services, Freddie Mac

Navdeep Singh, Vice President, Infrastructure Engineering, Fiserv

Mohan Putcha, Vice President, Enterprise Architecture & Digital Strategy, Aon

Richard Wiedenbeck, SVP & CIO, Ameritas Mutual Holding Company

Tom Sweet, VP of IT, GM Financial

Ryan Brown, Chief Enterprise Architect — Cloud, Visa

Ash Shah, Global Technology Lead, EY

Dana Jackson, Chief Technology Officer, Legg Mason

Manish Desai, CyberSecurity — Senior Information Risk Officer, BNY Mellon

Anandaraj Velmurugan, SVP, CIO, Salem Five Bank

Sunil Dayal, Head of Innovation & Fintech Sumitomo Mitsui Banking Corporation

John Marshall, Assistant Vice President, Credit Suisse

Michael Brady, CIO/CISO, LeaderOne Financail Corp

Sandeep Aich, VP, Prudential

Manik Patil, VP, Modernization, AIG

Sankara Ramakrishnan, Principal Architect, MetLife

Matthew Copelin, CIO — UK/Europe, WR Berkley

Edward Contreras, EVP/CISO, Frost Bank

Gregory Scher, VP Business Platform Technology, Fiserv

Walt Carter, Chief Digital Officer & CIO, Homestar Financial Corp

Matt McComas, VP DevOps Center of Enablement, GM Financial

Steve Randich, EVP and CIO, FINRA

Sigal Zarmi, Managing Director & Head of Transformation, Morgan Stanley

Jeff Farinich, VP of Infrastructure and Security, New American Funding

Raj Pillai, Vice President, Cloud & Enterprise Platform Services, Aon Corporation