CLOUDIFY COMPLIANCE RECORDING

9 Considerations for Moving Compliance Recording to the Cloud

NICE

CONTENTS

Data Considerations

Storing your recordings on-premises or in the cloud

Data residency – where in the world should data be located?

Migration Considerations

User migration from on-prem to the cloud

Legacy system migration on a mass scale

Security & Resiliency Considerations

Achieving compliance recording resilience in the cloud

Securing your data: why the cloud works best

System Configuration Considerations

Single or multi-tenant: what's the best approach?

Ensuring your cloud compliance recording and surveillance work together

Scalability Considerations

The benefits of an evergreen solution

9 Considerations for taking the journey to the cloud

Can you improve business results by moving compliance recording to the cloud?

Today, increasing numbers of financial services firms are turning to the cloud for its efficiency, scalability, and resiliency, and as importantly, the Total Cost of Ownership (TCO) savings it affords. Firms are finding they can easily save 60 to 75 percent in operational costs, simply by migrating from legacy on-premise solutions to the cloud.

With more regulated employees working remotely or in hybrid environments, even firms that previously had no near-term cloud strategy, are accelerating their journey to the cloud.

Thinking of moving your compliance recording to the cloud to improve your business results? In this eBook we offer you 9 key points to consider before making that journey.

In 2021, cloud workload adoption in organizations from the financial services and banking industry stood at 54% in the United States, 52% in Canada, and 48% in the United Kingdom, Hong Kong, and Singapore.

Source:
Cloud workloads by financial services global 2021 | Statista

CONTENTS

Data Considerations
- Storing your recordings on-premises or in the cloud
- Data residency – where in the world should data be located?

Migration Considerations
- User migration from on-prem to the cloud
- Legacy system migration on a mass scale

Security & Resiliency Considerations
- Achieving compliance recording resilience in the cloud
- Securing your data: why the cloud works best

System Configuration Considerations
- Single or multi-tenant: what's the best approach?
- Ensuring your cloud compliance recording and surveillance work together

Scalability Considerations
- The benefits of an evergreen solution

1

Storing your recordings on-premises or in the cloud

One of the first questions that often comes up when firms move compliance capture to the cloud, is 'where will my captured communications be stored?'

"When firms talk about capturing their regulated communications, they want to make sure they are stored appropriately, and how they're stored aligns with regulatory guidelines for their specific trading jurisdictions," said Chad Billing, Financial Markets Consultant, Communication Compliance at NICE. "Depending on where in the world you are, what you're doing and what regulations you're under, you may have very different requirements."

For example, MiFID II requires firms to maintain electronic records of communications, including voice calls and texts, in a WORM-compliant storage medium, as does the SEC and FINRA, under Rule 17a-4. The UK's Financial Conduct Authority (FCA) also requires regulated communications to be stored in a format that can't be intentionally, or accidently, altered or deleted.

Most popular cloud services like Microsoft Azure fulfill this requirement by preserving electronic records in a format that is non-rewritable and non-erasable, for the required retention period. Beyond this factor, firms can also benefit financially from a cloud-first storage approach. Experience shows that firms can save over 80 percent in storage costs alone, simply by moving their recording archives from on-premise to the cloud.

But storing regulated communications in the cloud isn't always a foregone conclusion.

"Moving compliance recording to the cloud doesn't necessarily mean the recording provider always provides the storage," said Billing. "Some customers, as part of their procurement requirements, will mandate that only certain regulated employee communications in specific geographies be stored in the cloud, whereas the remainder are archived on-premise."

"Although it's becoming less of a concern these days, one reason a firm might not elect to use cloud storage is simply 'trust,'" added Paul Cottee, Director, Global Markets Compliance Advisory, NICE. "The firm might be thinking, 'If we store the data on our own infrastructure, we know where it is, and we can control the associated risks - given that in the regulator's eyes we remain responsible for it anyway.'"

"Local privacy regulations can also cause firms to be wary of the cloud when data is stored outside of the firm's four walls, simply because it's no longer physically under the firm's security and supervision," added Cottee. "This can cause even more concerns for the firm if the cloud data center is in another country."

Whatever a firm's justification for cloud or on-premise storage, it's important for a firm to know that their chosen compliance recording system is agile and flexible enough to adapt.

NICE addresses this concern through its **NTR-X** compliance recording solution by offering multiple options.

"Our **NTR-X** platform as a Service (SaaS) solution, **NTR-X Cloud**, leverages the Microsoft Azure cloud for WORM-compliant archiving," said Billing. "But of course, if clients want to store their recordings on their own on-premise non-rewritable and non-erasable storage or other archive devices, these are capabilities we've built into our SaaS compliance recording platform as well."

> "When firms talk about capturing their regulated communications, they want to make sure they are stored appropriately, and how they're stored aligns with regulatory guidelines for their specific trading jurisdictions."
>
> **Chad Billing**,
> Financial Markets Consultant,
> Communication Compliance at NICE

CONTENTS

Data Considerations

Storing your recordings on-premises or in the cloud

Data residency – where in the world should data be located?

Migration Considerations

User migration from on-prem to the cloud

Legacy system migration on a mass scale

Security & Resiliency Considerations

Achieving compliance recording resilience in the cloud

Securing your data: why the cloud works best

System Configuration Considerations

Single or multi-tenant: what's the best approach?

Ensuring your cloud compliance recording and surveillance work together

Scalability Considerations

The benefits of an evergreen solution

2

Data residency – where in the world should data be located?

If you plan to store captured data and recordings in the cloud, there's also the question of where it can be located.

When you are storing data on your firm's own premises, it's pretty clear cut. Moving to the cloud can add complexities, because where data is recorded and stored becomes a function of multiple factors.

"What's right for one firm may not be right for another," said Billing. "We recognize that a one-size-fits-all approach to data residency just doesn't work in today's world."

"If a firm is interested in going the fully-managed cloud route, there are of course regulatory considerations they need to be aware of, which vary by territory," added Cottee.

Large multinational financial services firms may be subject to multiple data privacy requirements, depending on the regions they operate in. "The world's a big place," said Billing. "When you consider that there are 195 sovereign nations in the world, different countries are going to have different requirements about whether data can be captured, and within what geographical boundaries it can be stored."

For starters, can employees' conversations even be recorded? In many territories some form of consent is required from at least one of the parties to the conversation. This can usually be achieved by an appropriate disclosure, such as a clause in an employment contract or customer agreement.

Another question that crops up – can recordings be sent to and stored at an off-shore data center? In most cases the answer is 'yes,' with caveats. Many territories require the subject's consent. Others permit transfer to territories with 'equivalent' or 'appropriate' controls over personal data. Still others only allow transfer subject to an official license, permit or notification. Cottee says, "Again, obtaining an employee's consent via the employment contract is usually a good first step."

And what about firms located in multiple territories? Here it can get a bit trickier. Consider for a moment the recorded communications of a firm with traders employed in, for example, Singapore, London, and New York. The traders' communication recording files are sent to a data center in Bangalore for storage, and perhaps some level of processing. The resulting data is then accessed and examined by a surveillance officer in Toronto. The firm needs to consider the regulatory implications for each location, at each stage in the process.

For this reason, it's essential when moving to the cloud, to work with a cloud solution provider that has a solid understanding of these regulatory impacts.

Aside from all of this, while the cloud can create added complexities, it also gives firms an avenue to address them. With cloud compliance recording, firms have the flexibility to stand-up a solution in virtually any geographical location where they need data to be recorded, and reside.

"We run our **NTR-X Cloud** solution in Microsoft Azure, which provides a multi-region, multi-location deployment capability that gives customers free reign to choose the right region based on their needs," added Billing. "So we can provide customers with a cloud compliance recording solution that aligns with their unique regulatory, and regional data governance requirements."

The solution also allows firms to configure their own retention and access policies, to ensure that data: 1) is being protected, 2) can only be accessed by authorized individuals, and 3) can only be removed from archive storage when a specific policy (regulation) dictates.

> "If a firm is interested in going the fully-managed cloud route, there are of course regulatory considerations they need to be aware of, which vary by territory."
>
> **Paul Cottee**,
> Director, Global Markets Compliance Advisory, NICE

CONTENTS

Data Considerations
- Storing your recordings on-premises or in the cloud
- Data residency – where in the world should data be located?

Migration Considerations
- User migration from on-prem to the cloud
- Legacy system migration on a mass scale

Security & Resiliency Considerations
- Achieving compliance recording resilience in the cloud
- Securing your data: why the cloud works best

System Configuration Considerations
- Single or multi-tenant: what's the best approach?
- Ensuring your cloud compliance recording and surveillance work together

Scalability Considerations
- The benefits of an evergreen solution

3

User migration from on-prem to the cloud

How do you migrate potentially thousands of users to the cloud?

Another consideration in migrating to the cloud is how to make sure you continue to record everyone who needs to be recorded. A bank may employ tens of thousands of regulated employees spread across the far reaches of the globe, who all need to be recorded.

With more financial services firms now embracing hybrid work environments and unified communications platforms like Microsoft Teams (which requires cloud recording) this concern is coming to the forefront more often.

"At NICE, we've devised a migration capability where we can bring regulated users across in groups or regions from the legacy recording system to the cloud in a very, very risk averse way," said Billing. "So for example, a bank may have a NICE on-premise solution for recording Cisco users, but now those same regulated employees are using Teams and need to be recorded in the cloud. We can seamlessly ingest all of that user profile data into the cloud system."

Steve Logan, Director of Product Management, NICE, explains how. "Each regulated user might have a number of profiles in the legacy recording system that are used to trigger recording for different communication platforms and devices. Essentially these profiles can be migrated and linked to the same user in the cloud. This saves firms a tremendous amount of time by not having to do this work manually, and ensures that the regulated users' communications on the new platform, in this case Microsoft Teams, will be flawlessly recorded in the cloud."

> "Essentially all user profiles can be migrated and linked to the same user profile in the cloud. This saves firms a tremendous amount of time by not having to do this work manually, and ensures that the regulated users' communications on the new platform will be flawlessly recorded in the cloud."
>
> **Steven Logan**,
> Director of Product Management, NICE

CONTENTS

Data Considerations
- Storing your recordings on-premises or in the cloud
- Data residency – where in the world should data be located?

Migration Considerations
- User migration from on-prem to the cloud
- Legacy system migration on a mass scale

Security & Resiliency Considerations
- Achieving compliance recording resilience in the cloud
- Securing your data: why the cloud works best

System Configuration Considerations
- Single or multi-tenant: what's the best approach?
- Ensuring your cloud compliance recording and surveillance work together

Scalability Considerations
- The benefits of an evergreen solution

4

Legacy system migration on a mass scale

One of the biggest things that strikes fear in moving to the cloud is the risk of losing data.

Unlike many commercial enterprises, financial services firms are highly regulated. Beyond a requirement to simply record, they are also required to retain captured communications for varying extended periods of time.

For example, the SEC and FINRA require recordings of communications to be retained for six years. MiFID II mandates the same for up to seven years. And the FCA requires calls to be retained for at least five years, even longer if the regulator requests it.

What does this mean? Essentially, beyond just migrating any new recording of regulated users to the cloud, you need to migrate their historical communications as well.

"It varies from customer to customer, but most firms keep their recordings longer than required by regulation," said Logan. "So this could be twenty years or more worth of data."

"If you're going to buy a cloud solution for compliance recording, you need to consider more than just the calls you're going to record in the future," added Billing.

"Fortunately, NICE makes it easy for firms to take all of their existing recordings and seamlessly bring them into the cloud."

This is accomplished using built-in software migration tools that allow an on-premise recorder to be connected to a cloud recorder so recordings can be natively ingested through a sustainable, monitored and measured process.

Logan says this can be done in two different ways, based on the firm's specific preference for archiving historical content (recordings), and associated meta-data used to search for calls. One option would involve migrating meta-data to the cloud, while maintaining the actual audio recordings on-premise. A second option would be to migrate both to the cloud.

Firms that are migrating from one NICE solution, say **NTR**, to another NICE solution, **NTR-X Cloud**, can achieve either result seamlessly with NICE's assistance and migration tools. The software runs a check to look for damaged files or fragmented data first, then automatically copies meta-data and voice recordings from the on-premise archive to the cloud archive, while reconciling records for assurance that everything was successfully replicated over.

> "Fortunately, NICE makes it easy for firms to take all of their existing recordings and seamlessly bring them into the cloud."
>
> **Steven Logan**,
> Director of Product Management, NICE

CONTENTS

Data Considerations
- Storing your recordings on-premises or in the cloud
- Data residency – where in the world should data be located?

Migration Considerations
- User migration from on-prem to the cloud
- Legacy system migration on a mass scale

Security & Resiliency Considerations
- Achieving compliance recording resilience in the cloud
- Securing your data: why the cloud works best

System Configuration Considerations
- Single or multi-tenant: what's the best approach?
- Ensuring your cloud compliance recording and surveillance work together

Scalability Considerations
- The benefits of an evergreen solution

5

Achieving compliance recording resilience in the cloud

In financial services, compliance recording isn't a nice-to-have; it's imperative.

For this reason, resilience is another key consideration. You want to make sure your system is recording all of the time, and if it stops for any unforeseen reason, that there are fail-safe back-up mechanisms built in. This holds true whether you're recording on-premise or in the cloud, although some would argue that the cloud makes attaining resiliency much easier.

One important feature to look for is redundant (also known as 2N) capture where every call is recorded simultaneously, in parallel, by two systems.

To eliminate single points of failure, and add resiliency, one might also consider replicating recordings across two geographically distributed enterprise-grade cloud data centers.

Cloud providers like Microsoft Azure also offer built-in resiliency with regular backups of data (archived across multiple zones), and load balancing.

Additionally all software updates and security patches can be handled by the cloud provider outside of business hours to mitigate any possibility of service disruptions.

When it comes to recording certain types of communications, like Microsoft Teams, additional fail-safe mechanisms can also be implemented at an integration (API) level.

Microsoft Senior Teams Technical Specialist, Pete Woodhams explains: "When a user that has a compliance recording policy assigned to them makes a call in Teams, or receives a call, a recording bot is invited by the Teams service into that call or meeting prior to it taking place. We can have multiple bots available, so we're not just reliant on a single bot. If one bot became unavailable for whatever reason, additional bots can be available to participate so you've got a resilient approach."

"One of our recent enhancements we've added is the ability to auto-scale," said Billing. "That basically means in a busy time, the bots automatically scale up, and then when it gets quieter, the bots automatically scale down."

"Through our integration to the Microsoft Teams Graph API, a firm can also implement a policy that says, 'if a bot is unavailable, then the user cannot complete the call,'" added Billing. "This is a protection mechanism that ensures that if you have a regulated user, who has to be captured, but isn't being captured, he shouldn't be able to complete the call. As a trader, this enables me to confidently use Teams to work from anywhere. I know if I can complete a call, that a record of the call has been generated, and the business is protected."

> "When a user that has a compliance recording policy assigned to them makes a call in Teams, or receives a call, a recording bot is invited by the Teams service into that call or meeting prior to it taking place. We can have multiple bots available, so we're not just reliant on a single bot. If one bot became unavailable for whatever reason, additional bots can be available to participate so you've got a resilient approach."
>
> **Pete Woodhams**,
> Microsoft Senior Teams Technical Specialist

CONTENTS

Data Considerations
- Storing your recordings on-premises or in the cloud
- Data residency – where in the world should data be located?

Migration Considerations
- User migration from on-prem to the cloud
- Legacy system migration on a mass scale

Security & Resiliency Considerations
- Achieving compliance recording resilience in the cloud
- Securing your data: why the cloud works best

System Configuration Considerations
- Single or multi-tenant: what's the best approach?
- Ensuring your cloud compliance recording and surveillance work together

Scalability Considerations
- The benefits of an evergreen solution

6

Securing your data: why the cloud works best

When it comes to adopting new technology, especially cloud-based technology, security is a prime concern.

And this is one reason financial services firms have been historically slow to turn over their data to outside cloud providers.

"How are you going to protect me?' is one of the first questions out of the gate when we engage in cloud conversations," said Billing. "When data is not stored on the customer's premises they are not in control of protecting it. There's also an element of trust required that if they give us the proverbial keys to the kingdom, we, as the cloud solution provider, will protect their data, in a very secure manner. There's a huge element of trust involved."

In spite of the perception of cloud being less secure, the reality is on-premise systems can be equally, if not more vulnerable. For example, servers can be mis-handled by disgruntled employees, or not adequately updated to fight off newly-emerging cyber security threats.

Data security in the cloud, on the other hand, is handled by the cloud provider, and managing the cloud is all they do. The implication is this: when you consider a cloud compliance recording solution, the cloud provider's approach to security is key.

The NTR-X Cloud platform

Working with our cloud partner, Microsoft Azure, NICE's approach to securing data in the cloud is multi-faceted. The **NTR-X Cloud** platform is built securely from the start, following secure software development life cycle (SSDLC) processes.

The **NTR-X Cloud** application runs on cloud infrastructure powered by Azure, which is used and trusted by more than 95 percent of Fortune 500 companies. System components that process and store customer data reside in private networks within the Azure cloud (with customer-dedicated databases, storage space and virtual machine resources), preventing any possibility of data commingling or cross-client access.

Furthermore, network security restricts inbound and outbound network traffic into and out of Azure to specific designated destination and ports, as defined in the network security group rules.

Customer data is secured both in transit and at rest. All traffic into and out of the NICE cloud network infrastructure is encrypted, as well as all data at rest. Access to the **NTR-X** application is also encrypted using transport layer security TLS 1.2.

Access to stored data is only possible through the **NTR-X** application, subject to two-factor authentication, based on Active Directory Security Groups and granted roles-based permissions. Added security can be achieved through IP white-listing, and optional site to site VPN established between the data center and customer. Logical access controls also strictly limit access to customer data to designated support personnel with limited privileges.

Data is also secured through physical access controls. Microsoft Azure datacenters adhere to a broad set of international and industry-specific compliance standards, including ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2, as well as country- and region-specific standards (e.g. Australia IRAP, UK G-Cloud, and Singapore's MTCS). Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to mandated security controls.

NTR-X Cloud also leverages automated systems to monitor and alert on the occurrence of any irregular event. NICE maintains a global incident response team to handle any unforeseen events, in accordance with pre-established security policies and protocols.

While cloud compliance recording is just taking off in the regulated financial services realm, it has been a mainstay for enterprise contact centers for years.

One final takeaway

To ensure the security of your data in the cloud, look to solutions providers with cloud experience. With 12-plus years of cloud experience, over 3,000 cloud customers deployed, more than one million cloud users, and in excess of 20 billion interactions recorded in the cloud annually, NICE's track record speaks for itself.

CONTENTS

Data Considerations
- Storing your recordings on-premises or in the cloud
- Data residency – where in the world should data be located?

Migration Considerations
- User migration from on-prem to the cloud
- Legacy system migration on a mass scale

Security & Resiliency Considerations
- Achieving compliance recording resilience in the cloud
- Securing your data: why the cloud works best

System Configuration Considerations
- Single or multi-tenant: what's the best approach?
- Ensuring your cloud compliance recording and surveillance work together

Scalability Considerations
- The benefits of an evergreen solution

7

Single or multi-tenant: what's the best approach?

Another consideration for moving compliance recording to the cloud is whether to select a solution that uses a single or multi-tenant approach.

In a single-tenant cloud environment, a financial services firm is allocated dedicated applications, databases, and servers. In a multi-tenant cloud solution, the company may share these resources to run and manage their application.

A Compunnel Digital blog offered this analogy: "The best way to visualize the difference between single-tenant and multi-tenant SaaS solutions is to think of the architecture like housing options. With single-tenant, imagine that each business has its own custom 'house' or SaaS product. Every aspect of their product is completely customized to fit their needs, and their data is securely siloed in its own space for added protection. Multi-tenant, on the other hand, is more like an apartment building, wherein each business has a similar space and service level within one SaaS product, but with their own personalized experience and security."

In commercial applications, multi-tenancy can provide a cost advantage, but any cost advantage can have diminishing returns for regulated financial services firms, which tend to be very risk averse.

"Multi-tenancy on the whole is good for the service provider, but has a far bigger downside for a regulated firm," explained Logan. "The only potential benefit to the customer is if the service provider passes the cost savings along. But what's the risk? If my data could be potentially compromised, the negatives are much higher. This is why we are seeing more and more RFPs requesting a single-tenant approach."

According to Billing, there are other practical reasons for going the single-tenant route.

"Because **NTR-X Cloud** is a single-tenant system, it means that we can run the system in the way that is right for the customer," he said. "The service that we're providing in the cloud is geared specifically for financial firms, which operate during specific hours and require recording to be operational at all times. In a single-tenant world, the customer can exclusively choose when to shut down the system to do an upgrade or maintenance."

Now contrast this to a multi-tenant system. If you've got a hundred different banks on one recording system in the cloud, and the cloud provider needs to shut down and restart the recorder to complete a system-wide upgrade, one bank can't just say 'No, I don't want you to do that.' By being part of a shared system, individual companies lose some degree of control on how the system is managed. In regulated environments where recording is a need-to-have, this can introduce unacceptable risk.

Bruce Bolcer, VP of Enterprise Engineering at IPC Systems (another technology and service leader powering the global financial markets) agrees with this approach. "In order to provide our clients control over their cloud-based solutions, we build up and provide a hosted infrastructure that is completely dedicated to them. They have control over when we're providing upgrades, and overall, much greater control over their environment. We're managing and operating the trading communications service for our clients and delivering customizable SLA options to meet our customer's needs. We're not changing their environment without their advance knowledge, and we coordinate with them on any upgrade cycles. They have full involvement and full control."

> "In order to provide our clients control over their cloud-based solutions, we build up and provide a hosted infrastructure that is completely dedicated to them. They have control over when we're providing upgrades, and overall, much greater control over their environment."
>
> **Bruce Bolcer**,
> VP of Enterprise Engineering at IPC Systems

CONTENTS

Data Considerations
- Storing your recordings on-premises or in the cloud
- Data residency – where in the world should data be located?

Migration Considerations
- User migration from on-prem to the cloud
- Legacy system migration on a mass scale

Security & Resiliency Considerations
- Achieving compliance recording resilience in the cloud
- Securing your data: why the cloud works best

System Configuration Considerations
- Single or multi-tenant: what's the best approach?
- Ensuring your cloud compliance recording and surveillance work together

Scalability Considerations
- The benefits of an evergreen solution

8

Ensuring your cloud compliance recording and surveillance work together

Playing nice in the sandbox.

Recording and record-keeping of voice, video, chat, email and more, is required around the globe for compliance. But for financial services firms subject to regulations, captured interactions are essential for surveillance too.

By leveraging holistic surveillance solutions, firms can analyze communications, alongside trade and lots of other data, to detect and prevent market abuse and conduct risk, reconstruct events, and better understand the intent behind trader actions.

But to get to this point, the systems need to work together.

If your firm is sourcing compliance recording and surveillance technology from different vendors, this can add confusion, operational complexities and delays.

For starters, firms that take the multi-vendor route need to create and manage their own integration, or hire a third party, which means managing multiple vendors. And when you introduce different vendors into a project, this can also sometimes create unintended friction, especially if they are competitors working in the same space. Then there's the inevitable finger pointing when something goes wrong.

“Data integrations are hard,” said Steve LoGalbo, Director of Compliance Product Management for NICE. “Having a single vendor with an end-to-end solution simplifies this process and eliminates costly data integration. It also ensures that compliance capture and surveillance work hand in hand and seamlessly together.”

Toward this end, NICE offers an end-to-end, fully integrated cloud compliance suite that bridges communications capture and surveillance. **NTR-X** and **SURVEIL-X** are both offered as SaaS solutions which also means that firms can benefit from faster deployment, and lower infrastructure, operational, training and maintenance costs, as well as hassle free upgrades, seamless scalability, and improved resiliency and security.

“A single vendor approach means there's inherent software interoperability,” added Billing. “The two systems will natively work with each other because they've been designed and coded to be able to do that. On the other hand, multi-vendor solutions that require custom integrations, introduce risk.”

According to Logan, an end-to-end approach also makes it easier to implement future upgrades and enhancements, because cross-solution design and testing ensures changes to one solution won't negatively impact the other.

And, not having to do integration work inhouse has an added benefit. It enables financial services compliance professionals to focus on what they do best.

“No compliance professional wants to spend time focusing on the inner workings of technology,” said Billing. “At the end of the day, the only thing they want to do is to be able to get the information out of their compliance system in a timely fashion, to be able to satisfy an investigation.”

Surveillance of all captured interactions is essential for regulated firms

By leveraging holistic surveillance solutions, firms can analyze communications, alongside trade and lots of other data, to detect and prevent market abuse and conduct risk, reconstruct events, and better understand the intent behind trader actions.

CONTENTS

Data Considerations
- Storing your recordings on-premises or in the cloud
- Data residency – where in the world should data be located?

Migration Considerations
- User migration from on-prem to the cloud
- Legacy system migration on a mass scale

Security & Resiliency Considerations
- Achieving compliance recording resilience in the cloud
- Securing your data: why the cloud works best

System Configuration Considerations
- Single or multi-tenant: what's the best approach?
- Ensuring your cloud compliance recording and surveillance work together

Scalability Considerations
- The benefits of an evergreen solution

9

The benefits of an evergreen solution

In today's rapidly changing world, you need the agility and speed to adapt overnight.

Maybe it's new regulations, adding more locations or regulated employees, or adapting to the new technologies that employees use to communicate.

With on-premise compliance recording, these changes may require your firm to re-provision existing infrastructure, or purchase, install, test and certify new hardware and software. Some firms employ a virtual army of trained, knowledgeable staff to manage and certify recording system upgrades (even for the smallest security patches and software updates). This can be a huge resource drain.

Firms that move their compliance recording to the cloud find the cloud makes all of these things easy.

There's no need to stand-up new on-premise systems, or install hardware and software. Patches and updates are deployed and tested in the cloud environment by the cloud provider, and much faster. Ultimately, this means your firm can realize the benefits of new, innovative features and capabilities sooner.

Additionally, the cloud provider retains teams of skilled employees (DevOps, security, networking experts, and so on) to fully manage all aspects of your daily recording operations in the cloud. This takes the load off you.

This ability to adapt and scale quickly is one of the key benefits of **NTR-X** Cloud.

According to Microsoft's Woodhams, "The ability to deploy new services, new applications from the cloud to the user really helps to drive the pace of deployment and adoption. We're in a cloud-first world, and applications are evergreen. We see it in Teams, the ability to deliver new features quickly and transparently without any intervention makes a real difference not only to the user experience but also in reduced management overhead."

But even though the benefits of cloud are fairly well understood, there is one thing that firms can overlook. The cloud is fantastic for its adaptability, but you also need a great foundation to build on.

Communications recording means different things to different people. A solution that was designed for contact centers, even if it's deployed in the cloud, is likely not well-suited to compliance recording.

Compliance recording solutions are built from the ground up to address the specific needs and regulatory requirements of financial firms. This means as you embark on your cloud compliance recording journey, it's also important to look for companies that are well-entrenched in financial services (from both a technology and regulatory knowledge standpoint), so you can stay a step ahead of emerging and future requirements.

The cloud can make upgrades and enhancements easier, but what you can achieve through the cloud is a function of who you choose to do business with.

Billing explains it this way: "You want to make sure that your expectations on software upgrades and functionality are in line with who you are as a business, and what you expect to get out of your compliance recording system, not just today, but over the next 12, 24, 48 or even 60 months."

CUSTOMER EXAMPLE

Global Asset Manager BMO Deploys NICE Cloud Compliance Recording

THE CHALLENGE:

BMO GAM is global investment manager that delivers service excellence to clients across five continents. Upon shifting to a remote workforce in 2020, BMO GAM needed to continue meeting regulatory requirements around recording omnichannel communications for regulated employees now working from home.

THE SOLUTION:

To solve this challenge, BMO deployed NICE's certified Cloud Compliance Recording solution for Microsoft Teams across its business in Europe, the Middle East and Africa (EMEA).

> "As we transitioned to Microsoft Teams to support our remote workforce, we needed to implement a compliance recording solution quickly. NICE's fully managed, cloud-based, software-as-a-service offering for Teams compliance recording enabled us to accelerate our adoption of Microsoft Teams. We were also able to free our staff from time-consuming activities like handling security patches, upgrades and other platform management tasks, which are now fully managed by NICE."

Scott Wilson,
Director, Infrastructure & Operations at BMO Global Asset Management

NICE

NICE Financial Markets Compliance

NICE is a leading financial compliance solution provider, serving more than 90 percent of the largest investment banks globally. NICE's compliance solutions assist customers in the capture of trade conversations and trades, analyzing them for potential risk, and correlating trade conversations with trades for trade reconstruction. The company's compliance solutions make automated and intelligent holistic trade compliance programs possible and enable FSOs to more efficiently comply with regulatory requirements, including MiFID II, MAR, FX Code of Conduct, Dodd-Frank and future directives.

NTR-X is the world's first and only, fully-integrated, cloud-ready, next-generation, omni-channel compliance recording and assurance solution. Offering simplified compliance for a complex world, NTR-X captures all modalities of regulated employee communications – traditional, unified and mobile – in a single platform. If your firm is looking for a simpler way to lower compliance costs, extend unified communications to your regulated workforce, ensure complete compliance assurance, centrally manage your global compliance recording estate, and pave a future path to the cost savings, security and scalability of the cloud – NTR-X is the answer.

www.nice.com/compliance

Download the Brochure on Cloud Compliance Recording

About NICE

With NICE (Nasdaq: NICE), it's never been easier for organizations of all sizes around the globe to create extraordinary customer experiences while meeting key business metrics. Featuring the world's #1 cloud native customer experience platform, CXone, NICE is a worldwide leader in AI-powered self-service and agent-assisted CX software for the contact center – and beyond. Over 25,000 organizations in more than 150 countries, including over 85 of the Fortune 100 companies, partner with NICE to transform – and elevate – every customer interaction.

www.nice.com