CDS

Chromatography data systems: Current cloud coverage

Authors

Brian Alliston, Product Marketing Manager Chromatography Software, Thermo Fisher Scientific

Keywords

Cloud computing, Software as a Service, SaaS, Infrastructure as a Service, IaaS, Cloud security, GxP compliance, Validation, CSV, Chromatography Data System, CDS, Chromeleon

Summary

With the increasing use of cloud services in both regulated and non-regulated organizations the deployment of Chromatographic Data Systems (CDS) in the cloud has become more commonplace. Science based industries worldwide are taking advantage of cloud-based Infrastructure as a Service (IaaS), streamlining operations, and providing a competitive edge.

This White Paper will discuss the benefits and challenges of implementing, migrating, and operating 'CDS' in the cloud, what advantages a cloud deployment can provide to your IT department and why some organizations are reluctant to move to the cloud. It will also provide a summary of the current options for a migration or a new deployment of Thermo Scientific[™] Chromeleon[™] Chromatography Data System (CDS) in the cloud.

Introduction

You may not realize that you use the cloud every day. Services like video streaming, online shopping, web-based email, photo storage, and smart speakers are all cloud-based and in regular use.

Business usage continues to increase and, in an article published August 2021, Gartner, the technology research and consulting company, predicted that global enduser spending on public cloud services would exceed \$480 billion dollars in 2022, an increase of 22% from 2021.¹

thermo scientific

FLEXERA[™], a supplier of IT management solutions, reported that "public cloud adoption continues to accelerate, 55% of enterprise workloads are expected to be in a public cloud within 12 months" – by mid-2022.²

What is the cloud?

You may have seen the meme 'There is no cloud, it's just someone else's computer'. A bit of an oversimplification, but essentially true.



Cloud computing can be defined as the on-demand delivery of IT resources over the internet. Chromeleon CDS is cloud-ready and can be deployed in IaaS environments where you rent computing capacity, storage, and networking resources on-demand with pay-as-you-go pricing.

There are many different Cloud Service Providers (CSP) and Thermo Fisher Scientific have partnered with Amazon Web Services (AWS) to develop Chromeleon CDS in the cloud, investigating the use of cloud-native databases such as AWS Aurora[™] and services such as AWS CloudFormation[™], where infrastructure and software templates can be created for rapid and consistent deployment. Thermo Fisher are exploring how Chromeleon CDS can be provided using the Software as a Service (SaaS) model, a subscription service where potentially both the infrastructure and software required for CDS operation would be rented and managed for you.

Future development could potentially see the use of other cloud capabilities that could speed up workflows and data processing; imagine integrating CDS with Artificial Intelligence (AI) and Machine Learning (ML) to produce rapid, consistent, and accurate peak integration.

This white paper focuses on laaS public cloud deployment for Chromeleon CDS, the benefits and challenges of laaS. Providing food for thought if you are unsure about deploying your CDS in the cloud.

Chromeleon CDS has been installed with AWS and other CSP, for example, Azure and Google Cloud Services, and is currently in operation with several science-based organizations working, for example, in Biopharma, Pharma, and the Gas and Oil sectors.

How is Chromeleon CDS deployed in the cloud today?

To understand the challenges and benefits of the cloud it is necessary to understand how Chromeleon CDS is currently deployed in the cloud. The current deployment model is laaS but with on-premise elements. System infrastructure, software, and data reside in the cloud with on-premise instrument controllers linking instruments to the cloud and providing Network Failure Protection (NFP). The use of laaS is particularly suited as Chromeleon software has been optimized for operation in virtualized environments. You may already have Chromeleon CDS installed on virtual servers within your on-premise infrastructure.





Infrastructure as a service is, as the name suggests, where CSP supply and manage cloud infrastructure and Chromeleon CDS is installed, validated, and operated on virtual computing instances. When compared to on-premise deployment, an laaS provider manages virtualization, servers, storage, and in-cloud networking. Customers manage the operating system, application, runtime, required middleware, and onsite hardware, as well as managing access and security inside the cloud.

Remember, under GxP and data integrity guidance, organizations are always responsible for identity management for any application and the data generated.

Overview of Chromeleon CDS deployment in the public cloud

An laaS Chromeleon software deployment is essentially identical to an on-premise system. The required server applications are installed on virtual server instances in the CSP infrastructure.



Figure 2. Overview of Chromeleon CDS in the cloud

On-premise elements

There is still a need for on-premise hardware. Thermo Scientific[™] 247 Instrument Controllers or instrument control PCs (IPC) are the data interfaces between your instruments and servers and must still be situated near the instruments in your laboratories. These provide the buffered transfer of data from the instrument to the servers delivering NFP.

If data was streamed directly from the instrument to cloud or on-premise servers, any network interruption could result in data loss which would be unacceptable to any business.

NFP

Chromeleon software's NFP utilizes its unique XVault[™] technology allowing data to be generated during a network failure and ensuring the continuous operation of your laboratory. If the connection is down, your data is still recorded in the local Data Vault on the controller, then uploaded to the server when the connection is restored.

All information required to operate Chromeleon CDS for example, licenses and user access management data, is securely cached on local instrument controllers and client PCs. In the event of a network outage, laboratory operation can continue uninterrupted for up to 7 days.

Connection to the cloud

Chromeleon CDS data needs to get from your site into the cloud. Content router and firewall settings must be configured to allow data traffic to leave your site. At the other end, a private gateway must be configured to allow your data to enter the cloud. You can connect your application and site to the cloud either using a Virtual Private Network (VPN) or a CSP-specific direct connection. VPN is an encrypted connection which allows secure data transfers over the internet, while a direct connection is a private connection from your premises to the cloud. The connection to the cloud is a key consideration and can have a major impact on the performance of the system. This will be examined further as one of the challenges associated with CDS cloud deployment.

Virtual Private Cloud (VPC)

The public cloud is a shared computing environment. All hardware and resources are shared by multiple customers (cloud tenants) and Virtual Private Clouds (VPC) are the architecture provided to keep everyone separate. They can be used to keep tenants, applications, and data separate providing private cloud functionality within the public cloud.

Chromeleon CDS Servers

The Chromeleon Domain Controller and servers are installed in the virtual environment on provisioned computer instances — the hardware infrastructure within the cloud.

Chromeleon CDS requires a Microsoft[™] SQL Server or Oracle[™] database. This can be installed and managed by you on a computer instance. CSP provide managed databases where an SQL database can be setup, maintained, and managed for you. Thermo Fisher and AWS are currently testing the use of Relational Database Services (RDS) with a view towards the use of cloudnative database services.

CSP database services

- Amazon Relational Database Service (RDS)
- Azure SQL Managed Instance
- Google Cloud SQL

Additional services

CSP offer other services to help optimize your cloud performance, cost, and security, for example;

- Security and network monitoring
- Cloud audit trails changes and access logs
- Cost estimation tools and utilization monitoring

Chromeleon terminal client servers

Chromeleon CDS can be installed on terminal client servers providing virtual workstation PCs in the cloud. CSP offer various remote desktop services that can be used to access these workstations, for example, Remote Desktop Services (RDS) or WorkSpaces.

Users can access the application by connecting remotely via the internet. You define the computing power of these virtual workstations, so you don't need high powered PCs onsite to process data. As these cloud-based workstations are installed in the same infrastructure as the server components, (Data Vaults, raw data, database servers, etc.) data processing performance is at least as good as on-premise systems, if not better, due to the infrastructure hardware used. These workstations are referred to as a thin client.

As discussed earlier, Chromeleon CDS must use 247 Instrument Controllers or IPC's to provide instrument control and network failure protection. It can also be installed on remote workstations, where data can be processed but the workstation doesn't control any instruments. The speed of internet connection will impact performance when using thick clients or IPCs to process data. You are using the locally installed software to process data which therefore needs to be moved to and from the cloud.

Thin clients have the advantage of being co-located with the database servers etc, so the processing is happening inside of the cloud on virtual workstations, minimizing data upload and download.

VPN or direct connect

A major difference between an on-premise and cloud deployment is that on-premise servers are connected to instruments and controllers via a Local Area Network (LAN). It is relatively easy to achieve low latency and high bandwidth over an onsite LAN, but in a cloud deployment instruments and controllers are connected to servers in the cloud via a Wide Area Network (WAN) normally the internet.

The latency (connection speed) and bandwidth (connection capacity) can both be affected by other business applications using the same connection. The distance between you and your cloud data center is also a factor.



Figure 3. Latency and bandwidth

As previously mentioned, using the closest regional data center is best practice and a multi-site implementation can use a central Chromeleon Domain Controller with local data centers for each site to ensure performance. Your site can be connected via a VPN or direct connection, you can choose which method of connection best meets your requirements based on usage, cost, and performance. Achieving on-premise-like performance is a challenge and must be considered as part of any deployment project. Thermo Fisher will work with you to understand your requirements and usage, helping guide you to the correct solution.

Time for change, time for cloud?

The project to replace, upgrade or migrate your CDS is a massive one and as part of that project you can consider whether to host Chromeleon CDS in the cloud. No organization can make the move to cloud just for the sake of it. Understanding the benefits and challenges of deploying and operating Chromeleon CDS in the cloud can help you make an informed decision and prepare a business case for the right solution for your organization.

If you already have experience of operating software systems in the cloud or are ready to make the step into the cloud, Chromeleon CDS is ready. Not sure? Then it's time to consider the balance between challenges and benefits of CDS cloud computing.

Cloud benefits and challenges

There are numerous benefits of cloud computing and many organizations are already taking advantage with cloud deployment of applications such as Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP).

Organizations migrating any system to the cloud face challenges relating to security, costs, governance, resources, connectivity, and compliance.

A survey of 750 organizations found that their top cloud challenges were security, spend, governance and expertise

- 81% security
- 79% managing cloud spend
- 75% each for governance, lack of resources/expertise and compliance
- Respondents estimate 30 percent of cloud spend is wasted
 Source: FLEXERA[™] 2021 State of the Cloud Report²

To begin, it is worth taking a moment to think about the core difference between cloud and on-premise infrastructure using the analogy 'Pets vs Cattle' which is attributed to Microsoft Engineer Bill Baker who made the analogy during a presentation about scaling Structured Query Language (SQL) servers.

On-premise servers are likened to pets. They are unique, manually built, often given names, and receive special treatment. When your server is 'sick' it's all hands-on deck because if it fails, everything stops. The server is nursed back to health often at great expense, time, and effort.

Cloud servers are cattle analogues. CSP have data center 'farms' where servers are built and managed by others using automated tools. There are racks and racks of identical servers so if a problem occurs, they are swapped and repaired offline minimizing down time and impact to your business.

Clouds are the industrialization of server room infrastructure, providing highly available, consistent, reliable, secure, and flexible computing resources on demand. You no longer manage the hardware, which is both a benefit and a challenge. Understanding your responsibilities as a cloud customer is key to the successful deployment and continued operations of a cloud-based application.

Costs management

It is very difficult to draw an accurate cost comparison between on-premise and cloud deployments. How much power does your server room consume and how much of that is for CDS infrastructure? What about maintenance and IT labor costs? laaS usually includes power and proactive maintenance as part of your cloud rental. Regional variations in the cost of electricity are one of the reasons the prices of cloud services vary around the world even when using the same supplier.

CSP provide some useful Total Cost of Ownership (TCO) calculators to help with cost analysis when comparing cloud and on-premise running costs. Large CSP have hundreds of thousands of customers meaning they can achieve higher economies of scale which translates into lower pay-as-you-go prices but, as we have seen, many cloud users estimate they are wasting money. How is this possible?

Well, flexibility and scalability of resources are a huge benefit, but if your cloud is not managed correctly you can end up paying for resources you are not using. Adding software licenses, for example, for SQL, increases the cost of an instance and can reduce the potential savings. CSP offer a variety of payment models and yes, you can pay on demand, but there are cost savings to be made if you reserve resources and pay partially or totally upfront.

The following charts (Figure 4) illustrate the pricing plans available for two of the compute types required for Chromeleon CDS when deployed with AWS. You can make significant cost savings by committing to using a specific amount of compute over a fixed term (1 or 3 years), paying partially or totally upfront also reduces costs.

CSP give more pricing information on their websites and offer free-to-use cost estimation tools including the AWS Pricing Calculator, Azure Pricing Calculator, and Google Cloud Pricing Calculator. CSP also provide usage monitoring tools such as AWS Trusted Advisor, Azure Advisor and Google Cloud console which can alert you to any potential cost savings.

Understanding CSP price models and the proactive monitoring and management of usage costs is key to achieving maximum cost benefits.



^{*}Where C5.xLarge and C5.2xlarge are Elastic Compute Cloud (EC2) instances



Figure 4. Source: AWS Pricing Calculator September 2021, Hourly cost for dedicated AWS EC2 instances instanced with Microsoft Windows OS. Selected Region: Ireland

Hardware capacity

If your on-premise hardware is still operating efficiently, or you have just replaced your server infrastructure, you are unlikely to consider a move to the cloud, as you are locked in until your next hardware refresh. However, server hardware requires periodic replacement as performance and reliability decline over time, or hardware may go out of support or be incompatible with the latest technology or operating systems. In this case Cloud could be a consideration when you next come to replace your server hardware.

With industry refresh cycles currently averaging between 3-5 years, when the time comes to refresh on-premise infrastructure you need to estimate the capacity required up to your next refresh.

Where do you see your business in 5 years? How do you accurately predict workloads over extended periods? Using average data volume results in under capacity at peak, while using peak volume results in over capacity at lower workflows. Will your hardware support Chromeleon CDS updates so you can use the latest instrumentation and analytical techniques?

If you get your estimates drastically wrong, capacity may be too low giving poor system performance resulting in unhappy end users and lab managers. Aiming high and setting capacity to ensure performance at predicted peak workloads will increase the TCO and cost of any project to replace hardware resulting in an unhappy Chief Financial Officer (CFO) and you may never receive the benefits of these additional costs. Cloud computing is flexible and scalable. This is a massive benefit, get your predictions wrong and you can easily add more resource, so the cloud will grow with your organization. Storage and computing capacity can be added through online dashboards in minutes. You can also scale back during quieter periods.

When using the on-demand cost model there is no need for accurate capacity estimations, but in order to maximise cost savings there is a requirement to reserve resources, committing to 1 or 3 years and paying some or all of the rental costs upfront. To optimize costs, it is necessary to estimate usage, but cloud flexibility means you can adjust your requirements at any time.

Infrastructure, management and maintenance

If you have decided to install on-premise where will the servers for your enterprise CDS reside? If the answer is a purpose built, air-conditioned server room with multiple layers of physical, environmental, technical security with a team to support it, then the cloud may not be appropriate for your business right now.

laaS is suited to all types of organizations but can be particularly useful for sites where there may be minimal IT support to manage and maintain enterprise grade infrastructure. If your server is going to be in a dusty, hot, undersized, repurposed broom cupboard with no access control and a leaky roof, then laaS may be the answer to some of your infrastructure problems.



Figure 5. Variability of work load and system usage can easily result in the infrastructure being under or over capacity.

Search the internet for 'server room nightmares' and you will see some astonishing pictures that would keep IT team members awake at night.

Has your server room been hit by a Cat.5 hurricane or do you have a data leak? How hot does it get when the air conditioning fails?



Figure 6. Server room chaos

A huge benefit of the cloud is that you don't have to manage or maintain the server room infrastructure for your CDS. You are not just renting computing power, the associated life support systems, such as backup power supplies, air conditioning, fire detection, and suppression, and storage are part of the deal. The cloud removes some of the heavy lifting of IT infrastructure management, but remember there is still infrastructure to be managed on your site, for example, IPC's, VPN, LAN, and internet gateways and you are still responsible for managing costs and security.

This may also be a challenge to an organization's operation in compliant environments. You no longer control the infrastructure and the personnel that operate and maintain it. Understanding the impact and control of change is a challenge to both the CSP and the cloud customer.

Capital vs operational expenditure

Installing or replacing servers costs money. Money that must be spent up-front as a lump sum or capital expense (CapEx). Renting cloud services removes the need for a hefty upfront investment converting CapEx into ongoing operational expenses (OpEx). As we have seen CSP offer various pricing and payment plans, which can reduce costs even further. Removing capital expense from an implementation project significantly reduces TCO.

OpEx has several advantages over Capex. For example, both are treated differently for taxation purposes. OpEx costs are fully tax deductible in the tax year they are made. With CapEx tax deductions are made over the lifetime of an asset as it depreciates.

OpEx cash flows are more predictable and smoother over time as there are no lumpy outlays. Simplifying and speeding up the budgeting process, more good news for your CFO.

Purchasing IT hardware as CapEx has the advantage of greater control. You own the hardware and have total control of these assets. The use of cloud may represent a challenge to some organisations as they are giving up control of the infrastructure to key systems.

Cloud security

All major CSP operate a shared responsibilities model for security where the CSP is responsible for the security of the cloud and customers are responsible for the security inside the cloud. CSP have high standards of both physical and technical security and provide reliable, available hardware. As a customer you must ensure the security of any cloud-based applications, the data generated, encryption of data in transit, as well as identity management for both the cloud and application.



Capital Expenses vs Operating Expenses

Figure 7. CapEx vs OpEx

Tools are provided so that customers can manage user identity and cloud access. Which provide similar functionality to Chromeleon CDS administration. Roles and access groups can be set up to define permissions and levels of access for different types of users. Of course, you are responsible for these configurations and their maintenance.

CSP don't allow visitors to their data centers, it's part of their physical security so you can't go and audit them, but third parties do regularly carryout audits to ensure they are compliant to global industry standards, such as ISO 27001 information security standard and ISO 27017 information security controls for cloud services. Audit reports are available for review as part of your contract with a CSP.

CSP invest vast resources to continually improve security and defend the cloud against cyber criminals, providing firewalls, encryption key management, and services to mitigate against Distributed Denial of Service attacks (DDoS).

Is the cloud secure? The CSP stake their business on it, but the challenge for any organization adopting IaaS is that while they are no longer responsible for infrastructure management, they are still responsible for ensuring and monitoring security inside the cloud. They must understand their responsibilities with regards to security, implementing and maintaining best practices.

SOPHOS[™], an IT and Cybersecurity organization, highlighted several cloud security failings.³ Of the organizations surveyed:



Figure 8. Source: Sophos, The state of Cloud Security 2020

Organizations moving to the cloud must understand their security responsibilities and work with CSP to ensure the adoption of best practice. Organizations must develop expertise or leverage existing cloud skills or knowledge when migrating an application into the cloud.

FLEXERA[™] found 77% of the organizations they surveyed have developed central cloud teams or cloud center of excellence (CoE)².

Backup, restore and disaster recovery

If your onsite CDS server failed how long would it take you to get back up and running? Your disaster recovery plan should define how you will restore operations and your Recovery Time Objective (RTO) states how long you expect it will take. The Recovery Point Objective (RPO) is a measure of your tolerance to data loss. How many days/hours/minutes of data can you afford to lose? How much time can pass between data backups?

Using the cloud simplifies backup and restore procedures, allowing you to test your disaster recovery plans, minimize disruption, and accelerate the recovery process in several ways:

- Provision automatic failover, where operations are transferred to alternative servers without interrupting your processes
- CSP offer backup and restore solutions for your application and data. These are centrally managed services which can be used to automate backup procedures
- Economies of scale. Reduced data storage costs mean you can backup more often and keep more restore points, thus significantly reducing your RPO
- Create a template of your cloud infrastructure and application so it can be recreated quickly and consistently either during disaster recovery or as part of disaster recovery testing. It could also be used during company expansion
- Use cloud templates to deploy CDS test environments where backup data can be restored and compared to live data, allowing you to validate your data backup processes with documented evidence. These test environments can be deleted when complete, reducing costs.

Using the cloud can reduce your RTO from days to hours and minimize potential data loss by allowing low RPO. Once again, the CSP shared responsibilities model is clear on responsibilities with regards to disaster recovery plans and that they are responsible for cloud services only.

As a cloud customer, you are responsible for the disaster recovery plan for the application. CSP provide services that can facilitate your plans, but they are not configured by default and must be specified as part of your project concept, installation, testing, and validation processes.

Rapid global deployment and regional data

CSP have data centers around the world providing global connectivity and rapid deployment. Infrastructure can be managed and provisioned using Infrastructure as Code (IaC).

IaC is the process of managing and provisioning cloud infrastructure using a machine-readable description file. IaC can be used to create a cloud template during development and testing of your infrastructure. Once complete and qualified, a template of the infrastructure you provisioned for Chromeleon CDS can be used to provision a new, identical deployment within hours. These templates accelerate infrastructure deployment for new sites in any location. Cloud template services are provided by CSP, but you are responsible for the creation and management of these templates.

IaC and cloud templates solve the problem of 'environment drift' and a template of your infrastructure can be created and used to generate the same environment every time the template is applied. Templates are version controlled so can be rolled back during development and managed under change control.

Using the closest data center is good practice, giving the fastest connections between you and the cloud, but also allowing you to comply with any customer agreements or legal data regulations on where your data can be stored. The modular architecture of Chromeleon CDS means that you can operate with one Chromeleon Domain Controller, centralizing administration, but locate Data Vaults within regional data centers allowing you to comply with local data regulations. The use of Organizational Units, access control, and role privileges enable you to carve up your CDS operations allowing separate sites or labs to operate under local procedures.

To gain advantage of these features requires administration of both the cloud and the application. The challenge to any organization is to develop the skills and governance procedures required.

Centralized administration-application and cloud

The Chromeleon CDS Administration Console is the central access point for all administrative tasks. User management, policies, Data Vault, and licenses are all controlled from the Admin Console which can also be used to create maintenance windows for instruments, instrument controllers and terminals. This, coupled with the functionality to schedule and automatically 'push' patches and upgrades from the administration console, saves time and reduces system down time.

How many instruments and PCs are part of your Chromeleon software installation? Think of the time taken to visit each PC in turn and apply an upgrade or patch.

In addition to the application the cloud requires administration, with many organizations creating a centralized cloud administration team. If you are a multi-site organization the cloud delivers this functionality across your whole business. Administration and maintenance can be handled from 'HQ' minimizing the burden on any other sites where there may be a lower IT presence.

Smaller organizations face the challenge of developing cloud expertise or outsourcing the administration of cloud applications at additional cost.

Remote access and easy collaboration

So far, all the benefits of Cloud CDS have been for the IT department. After all, Chromeleon CDS is the same software regardless of where it is installed, but the end users experience can be affected by the latency and bandwidth of your internet connection.

Users can currently access Chromeleon CDS remotely without the cloud by using VPN and remote desktop applications, but cloud can simplify remote access and minimize the hardware required. Authorized users can connect to virtual workstations via the internet and access Chromeleon software, instruments and data anytime, anywhere, enabling them to check on the progress of their sequences and even process data remotely. With the use of electronic signatures, data can be reviewed from home accelerating lab workflows.

If you have multiple labs across one site, or spanning multiple sites, all using Chromeleon CDS in the same cloud infrastructure, you can collaborate easily with colleagues throughout your organization. For example, instrument methods, processing methods, and report templates can be moved quickly from the development labs to the quality control lab where they can be utilized in eWorkflow[™] procedures. This simplifies method transfer and gives complete traceability in data audit trails.

Instrument or method troubleshooting and training can be provided by your experts wherever they are located. Your labs can work together as a team. Remote access and easy collaboration enable more efficient and united lab operations when using Chromeleon CDS in the cloud and throughout your organization.

Understanding your business requirements and getting the right connection

As we have already discussed, latency and bandwidth are key to system performance. As such, it is essential that as part of any project to implement or migrate Chromeleon CDS to cloud, you understand your organizations usage or intended usage so you can provide the performance you require and optimize your costs. The challenge is to measure your current data volumes and flow, predicted growth, and discover what potential impact other systems have on your connections.

In laaS you are responsible for 'sizing' the connection to the cloud. Thermo Fisher can supply latency guidelines for the connections between Chromeleon CDS components, but bandwidth requirement is determined by your data output.

The flexibility of cloud infrastructure means that computing power and storage can be scaled up and down quickly, but additional internet connections or direct connect services take longer to provision. User requirements for connection speed and capacity must be established in the concept phase of the CDS implementation project. Thermo Fisher can help you understand and define your infrastructure requirements for Chromeleon CDS operations.

GxP compliance and validation of laaS CDS

The processes involved in validating any system are a challenge to organizations and require planning and resources. Validating and operating a GxP compliant cloud CDS is comparable to on-premise operations. Working with your software vendor and by leveraging the information they provide, a user requirement specification can be created for both the application and the infrastructure needs. Your IT department must work with the CSP to provision the required virtual infrastructure. This can be qualified against your user requirements specification to ensure the correct infrastructure has been provisioned. Components of the system are qualified and the whole system or process is validated using the same validation processes that would be used for an on-premise system, but there are additional considerations to be made when validating a cloud-based system.

Failover, backup procedures, and storage locations must be defined as part of any implementation project and tested during the qualification and validation. An agreement or contract must exist between you and the CSP. In GxP regulated industries, CSP must be treated as a service provider in line with your company's quality and IT management systems. You must carry out due diligence when selecting a service provider and the regulatory guidance is clear, a formal agreement must exist between you and a CSP.

Life science companies are operating GxP applications in public clouds today. CSP have published white papers on achieving GxP compliance in the cloud. These papers all refer to the previously discussed joint responsibilities model for security and clearly define the roles and responsibilities each party has in ensuring compliance. White papers on this topic can be found on CSP websites.

As we have seen, a service level agreement (SLA) or contract is a key requirement for the compliant use of cloud-based CDS applications and an SLA provides a clear statement of responsibility for each party. It makes sense to apply this approach for all organizations whether regulated or not. SLA are used to define what level of services you expect to receive and what happens if the service falls short of the required level. 3. Suppliers and Service Providers

3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous."

EU Annex 11: Computerised systems ⁴

"6.20. IT Suppliers and Service Providers (including Cloud providers)

Where 'cloud' or 'virtual' services are used, attention should be paid to understanding the service provided, ownership, retrieval, retention, and security of data."

"The responsibilities of the contract giver and acceptor should be defined in a technical agreement or contract."

MHRA Data Integrity Guidance 5

Future forecasts

Chromeleon CDS continues to go digital and work is ongoing to expand digital software offerings and cloud deployment options.

Dongle-free licencing has already been introduced and subscription-based licencing will be made available. Currently, Chromeleon software licences are perpetual, customers are charged per client or instrument, upgrades are not included, and a separate support contract is available.

Licence subscription will have an annual charge, and will include an SLA. This is a step towards delivering Chromeleon CDS as SaaS and the intention is to move towards a full software subscription and licencing model.

Work continues increasing Chromeleon software processing and reporting capabilities, utilizing the processing power of cloud infrastructure to enable the rapid processing of large data sets and provide business analytics tools.

A cloud-based Chromeleon CDS demonstration environment will allow customers to experience and explore the latest versions and features of Chromeleon software operating in cloud infrastructure.

Summary

Operating an application like Chromeleon CDS in the cloud can afford your organization many benefits, for example, flexibility, scalability, reduced infrastructure management, cost savings, and centralized operations.

There are many challenges to overcome in order to deploy and operate applications in the cloud. To some, the cloud may seem like a silver bullet, where all responsibility can be delegated to a CSP and everything will be done for you. IaaS does remove some of the burden of infrastructure management from your organization, but there are still many tasks to be carried out throughout the lifecycle of a system. Remember, when operating applications in any type of cloud, IaaS to SaaS, you are still responsible for the data and access management.

Any cloud deployment requires an organization to take control. You must develop new cloud skills, leverage existing experience, or seek external support. Many organizations go on to create cloud centers of excellence or cloud teams, within their IT teams, to manage their cloud operations. You and your organization must take steps to understand your requirements, how these can be met by cloud service providers, and with the use of an SLA clearly define each parties' responsibilities.

Cloud operations can be secure, cost effective and compliant but they must be installed, configured, monitored, and maintained to ensure they remain so.

References

- 1. Gartner press releases: 2021-08-02 "Gartner says four trends are shaping the future of public cloud"
- 2. FLEXERA[™] 2021 STATE OF THE CLOUD REPORT
- 3. SOPHOS[™] State of cloud security report 2020
- EU Good Manufacturing Practice Medicinal Products for Human and Veterinary Use Annex 11: Computerised systems
- 5. MHRA GXP data integrity guidance and definitions, revision 1. March 2

Learn more at thermofisher.com/chromeleon

For Research Use Only. Not for use in diagnostic For Research Use Only. Not for use in diagnostic procedures.

© 2022 Thermo Fisher Scientific Inc. All rights reserved. AWS Aurora, AWS CloudFormation, Amazon Relational Database Services (Amazon RDS), Amazon Elastic Cloud Compute (Amazon EC2) are trademarked and owned by Amazon Internet Services Private Limited. Azure and SQL Server are trademarked and owned by Microsoft Corporation. Google Cloud is trademarked and owned by Google LLC. Oracle is trademarked and owned by Oracle Corporation. Flexera is trademarked and owned by Flexera. Sophos is trademarked and owned by Sophos Limited. All other trademarks are the property of Thermo Fisher Scientific Inc. and its subsidiaries. This information is presented as an example of the capabilities of Thermo Fisher Scientific Inc. products. It is not intended to encourage use of these products in any manner that might infringe the intellectual property rights of others. **WP000459 0222**

thermo scientific