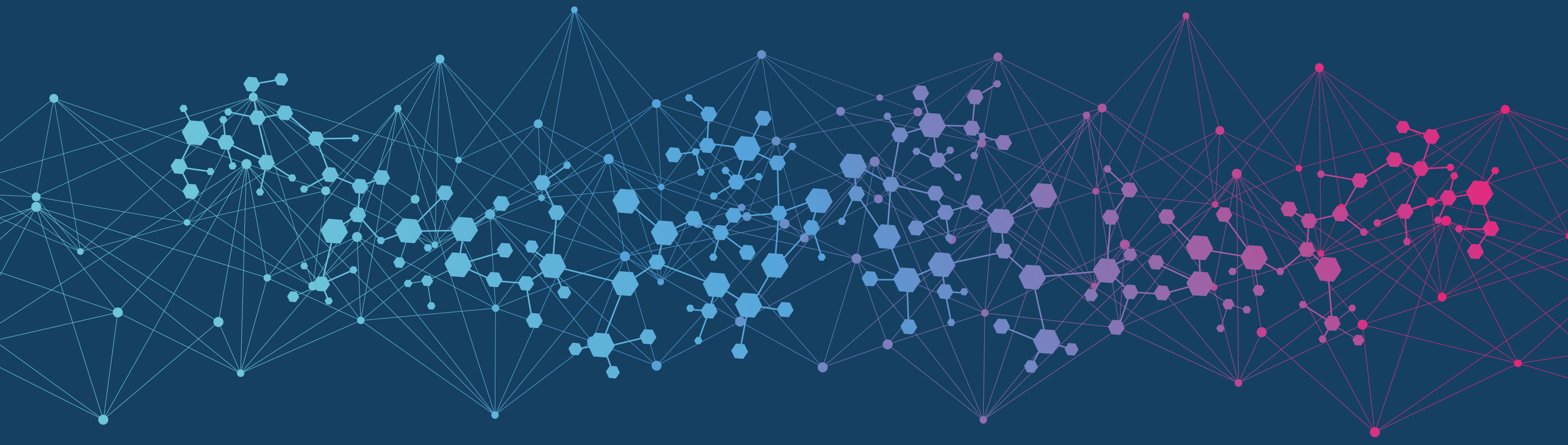
IS THE CLOUD A SAFE PLACE FOR YOUR DATA?

How Life Science organizations can ensure integrity and security in a SaaS environment

Written by
Damien Tiller
Quality Manager, IDBS

CONTENTS



ABSTRACT

Demonstrating data integrity is central to all processes within the Life Sciences industry. As the evolution of technology presents new opportunities and considerations to managing data, organizations can find it challenging to balance what is possible against the guidance provided within regulatory frameworks.

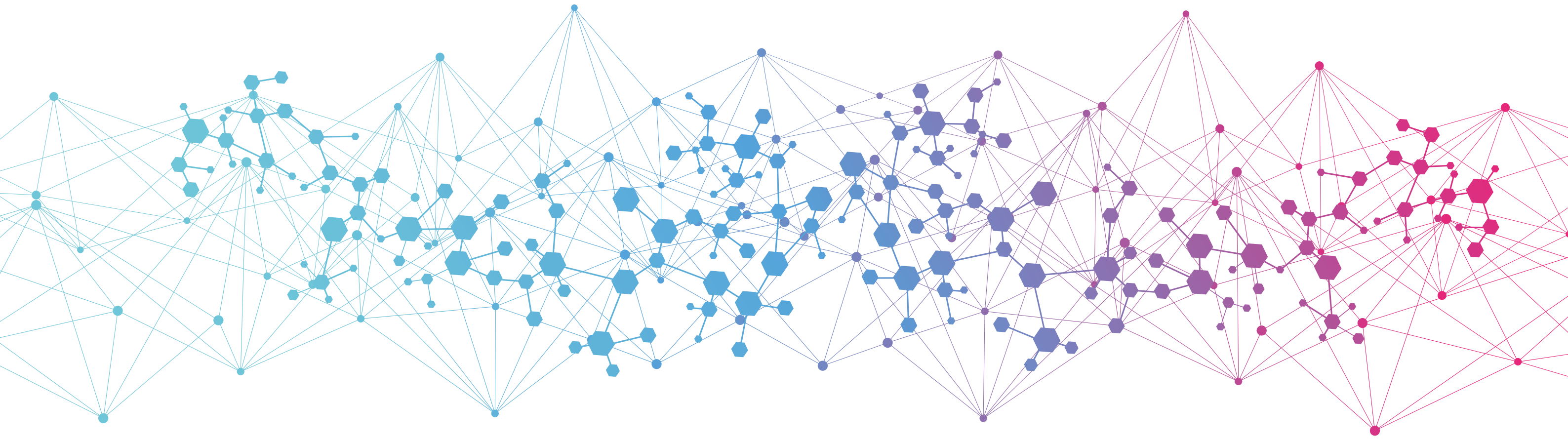
The interpretation of guidelines can be further complicated when you consider that some of this guidance, such as **ENV/MC/CHEM(98)17, The Organisation for Economic Co-operation and Development (OECD) series on principles of good laboratory practice (GLP) and compliance monitoring, was last updated in 1997** – long before Software as a Service (SaaS) and cloud technology was as widely spread and robust as it is today.

The ability to interpret regulations and ultimately demonstrate to customers and regulators that data is safe, integral and available is more important than ever. But when working with SaaS providers, the adherence to regulations may require more than simply visiting an on-premise location where data is stored.

In many instances, visiting a physical location is no longer practical, and in some cases is even impossible. Many large Infrastructure as a Service (IaaS) organizations, such as Amazon Web Services (AWS), have made the decision not to provide the exact street address for their datacenters to reduce security risks.

Historically, when paper records were kept in a filing cabinet or even a server on-site, auditors would have expected to see an exact location for the data but, as with the AWS example above, this is now an increasingly outdated way of working.

Within both the cloud and information security, it is important to be able to meet the needs of regulators while getting products to market. This whitepaper explores the potential concerns that regulated customers may have when moving from an on-site deployment model to a hosted SaaS model. It will look at how the integrity of data can be assured and how due diligence can be demonstrated when the ability to physically inspect the hosting facility is no longer possible or practical.



THE RISE OF CLOUD SOLUTIONS IN LIFE SCIENCES

If you take a step back from the different software solutions available to the Life Sciences industry, and do not focus on any single product or solution, it becomes possible to consider the variance in requests for information made by the market during the vendor selection phase. All stakeholders of the drug development lifecycle, from research to manufacturing, are looking to make use of new technologies but have little clarity around how to demonstrate that the cloud is a safe place for their data.

Organizations in the Life Sciences industry are looking to use technology to reduce the resource required to manage the large volumes of data that are generated. Many companies are turning their attention to the cloud and cloud-based services. An early article by Montrium gave guidance in 2015 **(Montrium 2015)** that addressed this market change, stating that the cloud will continue to gain traction in professional environments with more and more critical business applications moving towards this new approach.

Almost five years on and organizations continue to scale up their use of electronic systems. However, there remains a lack of clarity on how best to handle data when it comes to SaaS providers. This can be traced to understandable concerns rooted in the ability to demonstrate data integrity criteria to the regulators and to customers downstream in the manufacturing supply chain.

This concern is not unfounded when we look at some of the large data breaches that have occurred from the use of cloud and SaaS providers. **(Security Solutions 2019)** Incidents such as First American Financial Corp, the largest real estate title insurance company in the U.S., that were reported in July of 2019 to have exposed transaction records of 885 million individuals.

Despite these high-profile breaches, there is still an appetite for moving data out of filing cabinets and into the cloud – particularly because cloud-based solutions, often using best-in-breed specialist providers, typically mean data is more secure than in a traditional on-premise solution. And that is before you consider the inherent cost savings, collaboration benefits and ability to integrate with new technologies.

Across the Life Sciences industry, companies must demonstrate that they have appropriately assessed SaaS vendors and have mitigated any risk of hosting GxP-regulated applications in the cloud. The basic principles of vendor assessment still apply to SaaS vendors. But with regulatory guidance evolving from being aimed at paper records or in-house information technology (IT), interpreting them for cloud-hosted solutions poses new challenges.

Emphasis must, therefore, be put on understanding the risks and having appropriate mitigation plans in place.

So how can organizations be sure that data is safe, secure, available and has integrity when hosted in the cloud?

INTERPRETING **OUTDATED REGULATIONS**

When considering how to show this most critical aspect of the Life Sciences supply chain – that the data is safe and has integrity – guidance should be sought from the regulations. However, some regulatory guidance, such as GLP principle §9.2.7 (the OECD document which has not been revised since 1997), is not worded in a way that is easily interpretable considering more recent technological and security best practice approaches.

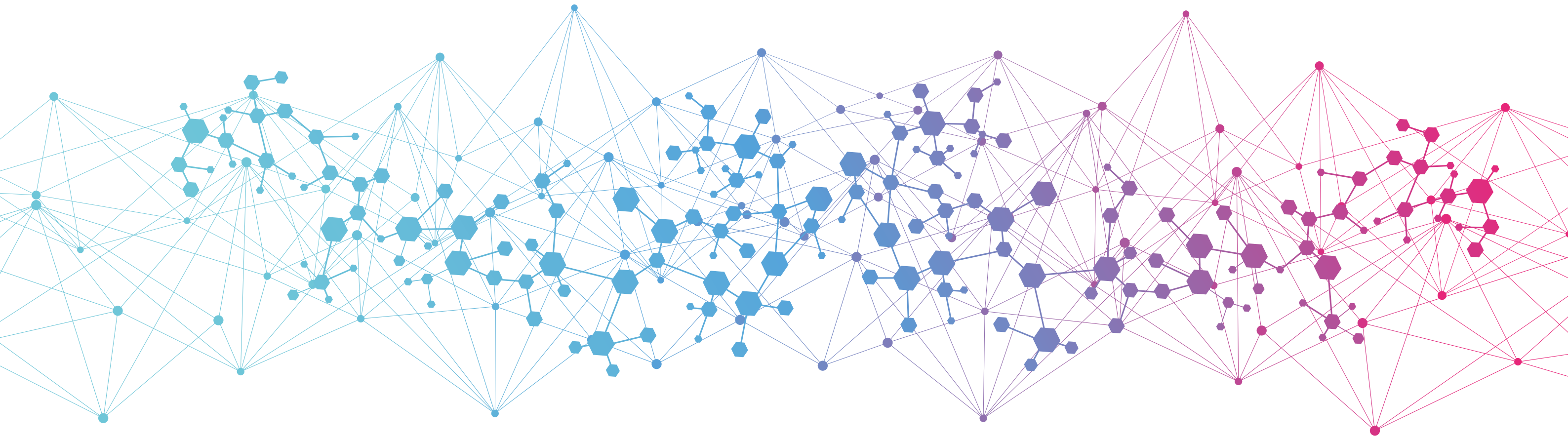
The regulation states: (OECD) "The location(s) where the study plan, samples of test and reference items, specimens, raw data and the final report are to be stored." This refers to information that must be contained in the final report and the wording makes use of the latest technology, such as the cloud, challenging. This requirement is often interpreted as referring to the street location being the physical address of the server or data center. However, for obvious reasons, the street address for high security cloud data centers is often not disclosed.

When considering if you can reference the geographic location in place of a building or room, there is a lack of clarity apparent in both OECD and US GLP regulations that require that the location of the final GLP study report and the GLP archive is documented.

R.D. McDowall explains there is no definition in either regulation or associated OECD and AGIT guidance documents of the word location. This then causes individuals and organizations to take actions to interpret this meaning themselves. A flexible approach to determining any location could mean:

- **Street address**
- **Facility site name**
- **Geographical area**
- **URL for remote access to a computerized system**

The Food and Drug Administration (FDA) draft GCP guidance goes further than any other regulatory authority in allowing SaaS applications to be used for clinical investigations provided certain conditions are met.



INTERPRETING **OUTDATED REGULATIONS** *CONTINUED*

This is in direct contrast to a communication included in a conference held the week commencing 27 January 2020 in which a French GLP inspector mentioned during a presentation that he considered the cloud incompatible with GLP requirements.

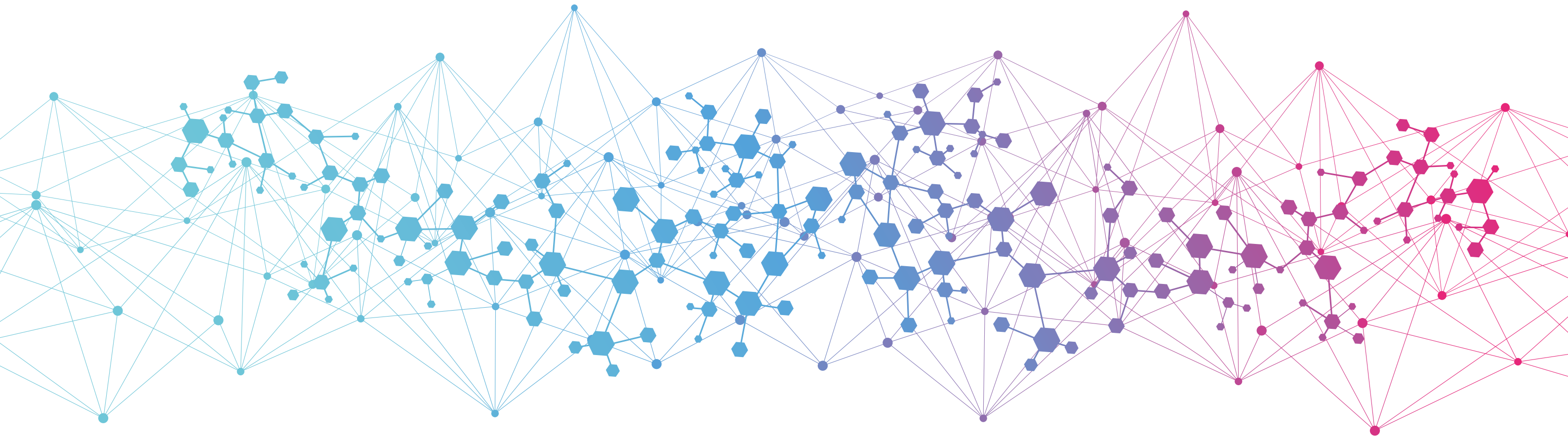
The expectation of the final report detailing the exact location of the data was also confirmed when IDBS met with the regulators earlier this year. However, many organizations within the Life Sciences industry have already begun moving their data to the cloud. The case study Veiga and Calnan (2018) demonstrates some of the benefits of this, such as enhanced cost-effectiveness, ease of implementation, flexibility, and scalability.

Veiga and Calnan go on to explain how the pharma company in their study outsourced its research and development (R&D) to a clinical research organization (CRO). In turn, the CRO outsourced the data collection duties to a hospital where the trial subject/patient data was collected. They detail how a CRO also contracted a third-party IT company (SaaS provider) which was responsible for the data management processes associated with the clinical trial. Both examples can demonstrate the integrity of their data in highly regulated situations whilst satisfying the requirements of the regulations and still ensuring that the best practice attributes of cloud security were maintained.

When considering the safety and integrity of the data, detailing the exact postal address of the data is not necessarily the roadblock it could be perceived to be. Indeed, as technology has progressed and organizations strive for new ways to keep their data secure, many organizations, such as Amazon Web Services [AWS], choose not to disclose the exact location of the data as this could put their site at risk from attempts to disrupt or destroy the data. This approach has now become best practice.

When data is stored across multiple locations and these locations are kept highly confidential, data is often more secure and less likely to be subject to integrity issues.

The challenge is ensuring that an organization in the Life Sciences industry is able to demonstrate that suitable due diligence of the infrastructure has been carried out without being able to visit the location, or even knowing the exact location the data is stored.



WORKING THROUGH THE **CERTIFICATION MINEFIELD**

A potential solution to the challenge of demonstrating that checks for due diligence have been adequately carried out is to rely on the compliance documentation of the supplier. Whilst certifications such as ISO 9001 standard (requirements for a Quality Management System) and ISO 27001 standard (requirements for an Information Security Management System) do provide assurance, there is a limit to the transparency of information: the successfully audited organization may not be able to provide full details of the audit, leaving the pharmaceutical organization feeling unsure it can demonstrate the risk has been sufficiently mitigated.

Many SaaS organizations now base their offerings on standardized Infrastructure-as-a-Service [IaaS] provided by AWS and others. AWS (2016) claim that they can meet the requirements of GxP and have many whitepapers and other such documents that detail how the system can be configured to meet the requirements of GxP. However, these documents do not provide much in the way of auditable documentation that can be used to demonstrate to the regulators or customers further down the supply chain the integrity and safety of the data and that the requirements of the regulations have been met.

Something more is needed. One solution is to use a system that details thoroughly the way a SaaS provider is set up, the controls they have in place and lists out any non-conformities. IDBS found the solution here to be the SOC 2® - SOC for Service Organizations: Trust Services Criteria and reports. The independent and third-party audit carried out against the Trust Service Criteria inspects almost 200 aspects focusing on information security, data integrity, availability, and archive.

More information is available in the article recently published by N. Hemmer (2019) in which she also explains how SOC 2 is comprehensive enough that the scope of the examination alone will likely be enough for service organizations' clients to get the assurance they need with respects to the security of their information/data.

This assurance comes from the style in which the SOC 2 type 2 report is carried out. For a SaaS organization to show they are compliant with SOC 2 type 2 they must not only show they have the relevant controls in place but that the controls have been operated effectively over a six to 12-month period. This prolonged and multipoint audit is something that would not normally be possible if a customer came for an on-site audit of one to two days once every few years when assessing a supplier.

Unlike the ISO certifications that have very limited information, the SOC 2 type 2 report contains details in a structured and easily auditable format, the independent auditor's report, and an assertion from the leadership of the SaaS organization themselves. Also included is a "Service Description" that lays out exactly how the SaaS provider is structured, how the data moves through the system and how it is controlled. More importantly, the report also includes any observations or exceptions. IDBS has successfully completed a SOC 2 Type 2 audit and a report is available detailing the controls and the compliance to this standard over a 6-month period of business.

CONCLUSION

If the perceived problem is an inability to be able to demonstrate the controls of data in the cloud, and the reliability of a SaaS supplier to a regulator or customers further down the supply chain, then utilizing the detailed examination of the SOC 2® - SOC for Service Organizations: Trust Services Criteria audit report would give a high degree of visibility of these organizations, where security reasons do not permit on-site audits or where on-site audits may not be possible. SOC 2 type 2 would give a comparable level of assurance.

Such is the thoroughness of SOC 2, it can often provide a better assessment of an external provider than a potential 1- or 2-day audit on-site.

With SOC 2, leading organizations operating in the Life Sciences sector can demonstrate an established framework for internal controls that facilitates accountability and a commitment to security. It also allows them to demonstrate operating effectiveness, increased efficiencies and reduced costs, which translates into a platform that is safe, secure, and adds value, while helping to build increased trust and transparency with Life Sciences customers.

REFERENCES

AICPA.org (2017) SOC 2® - SOC for Service Organizations: Trust Services Criteria. Retrieved from: **https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html**

Amazon Web Services (2016) Considerations for Using AWS Products in GxP Systems. Retrieved from: **https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_GxP_Systems.pdf**

Henriquez, M. (2019) The Top 12 Data Breaches of 2019 Security Solutions for enabling and assuring business. Retrieved from: **https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019**

Nicole Hemmer (2019) Trust Services Criteria (formerly Principles) for SOC 2 in 2019. Retrieved from: **https://linfordco.com/blog/trust-services-critieria-principles-soc-2/**

OECD (1997) "OECD series on principles of good laboratory practice and compliance monitoring". Retrieved from: **http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=env/mc/chem(98)17&doclanguage=en**

Veiga, E. Calnan, N. (Dec 2018) "Assuring Data Integrity and Data Privacy Compliance when using Software-as-a-Service (SaaS) in the Life Science Sector". The Journal of Validation Technology Vol. 24, Issue 6, Dec 2018. Retrieved from: **http://www.ivtnetwork.com/journal-validation-technology/journal-of-validation-technology-4211**

AUTHOR
Damien Tiller, Quality Manager, IDBS

ADDITIONAL CONTRIBUTORS
Anthony Barnardo, Director of Governance, Compliance and Risk, IDBS
Liz Tyler, Senior Director, Quality and Operations, IDBS
Roman Vincent, Director of Marketing, IDBS
Chris Powers, Content Manager, IDBS
Iris Barbier, Scientific Content Writer, IDBS

IDBS

info@idbs.com
www.idbs.com

UK (HQ)
Tel: +44 1483 595 000
2 Occam Court,
Surrey Research Park
Guildford, Surrey, GU2 7QB

USA (BOSTON)
Tel: +1 781 272 3355
285 Summer St.
Fifth Floor
Boston, MA 02210

USA (ALAMEDA)
Tel: +1 510 814 4900
1301 Marina Village Pkwy
Suite 320
Alameda, CA 94501