BOC Cloud Services

Service Offering, Data Protection, IT-Security and Compliance

Last Updated: 2025-09-05

BOC Group
Design your Enterprise

Contents

1. Management Summary

BOC Cloud Services provides a secure and reliable platform for businesses to operate BOC products without a local installation and without the need of allocation IT-resources on the customer's end. We offer a range of service options to meet the unique needs of each of our customers, and our team is dedicated to providing the highest level of service and support. We benefit from our experience from many years of developing world-class products and solutions, hosting and operating services as well as integrating BOC Cloud Services with customer infrastructures.

In this document, we provide an overview of our cloud service offerings, including service level agreement and reports, maintenance services, and hotline support. In addition we point out how we ensure data protection and IT security measures, and compliance with various regulations and industry-specific requirements.

We take the security and protection of our customers' data very seriously, and have implemented a number of measures to ensure the confidentiality, integrity, and availability of their data. These measures include database encryption options, encryption at transfer, business continuity management, and penetration tests.

We are committed to compliance with all relevant regulations and industry standards, and have obtained a number of certifications and audits to demonstrate our commitment (ISO 27001, ISO 27018). We also have processes in place for managing risks, managing suppliers, and protecting intellectual property rights.

Thank you for considering BOC Cloud Services. We look forward to the opportunity of working together and supporting your business needs.

2. Service Offering

BOC Cloud Services is the preferred Hosting Service Provider for BOC Products (ADONIS, ADOIT, ADOGRC) as well as related Modules, Add-Ons and Web Services. Customers can either choose to have their existing BOC licenses operated by BOC Cloud Services (hosting only) or obtain BOC Products as Software as a Service (SaaS). Either way, BOC Cloud Services will ensure the efficient and seamless operation of your services in our cloud environment.

To give our customers the best possible experience with our products, in addition to our promise of service availability (2.2 Service Level Agreement and Reports), the SaaS offering includes corrective and preventive maintenance (2.3. Maintenance) and hotline support for service requests and incident reporting (2.4. Hotline).

For more information about extensions that can enhance your chosen service, please visit BOC Group's Marketplace.

2.1. Service Description

Customers who opt-in for SaaS or Hosting with BOC Cloud Services get access to the full service package for their respective BOC product of choice. This includes:

- Provisioning of the BOC product instance in one of BOC's cloud locations
- Operation of the products with a 24x7 service availability
- Integration of the product instance with customer- managed Identity Providers
- Automated backup of customer data in two separate locations
- Rollout of software updates in mutually agreed maintenance windows
- Monitoring of the availability of the service including system performance
- Capacity monitoring and management of the underlying infrastructure
- Regular security updates for all involved systems executed outside typical working hours
- Maintenance of Business Continuity and Disaster Recovery Plans including regular tests
- Access to BOC Support Desk for Incident and Problem Management as well as request fulfilment

BOC Cloud Services are provided in two different locations to support regulatory requirements with respect to data location. The available options are:

Option 1: Germany

- Primary IaaS-Provider
  - Amazon Web Services EMEA Sàrl, 38 Avenue John F. Kennedy, L-1855 Luxembourg, Data Center in Germany (eu-central-1)
- Disaster Recovery IaaS Provider:
  - Amazon Web Services EMEA Sàrl, 38 Avenue John F. Kennedy, L-1855 Luxembourg, Data Center in France (eu-west-3)

Option 2: Switzerland

- Primary IaaS-Provider
  - Cloudsigma AG, Badenerstrasse 549, 8048 Zurich, Switzerland, Data Center in Switzerland
- Disaster Recovery IaaS Provider:
  - Amazon Web Services EMEA Sàrl, 38 Avenue John F. Kennedy, L-1855 Luxembourg, Data Center in France (eu-west-3)

2.2. Service Level Agreement and Reports

BOC is aware of its responsibility regarding the availability of its services and has therefore taken extensive technical and organisational measures to make its systems as robust as possible and give our customers an uninterrupted user experience. However, if unexpected incidents occur despite all preventive measures taken, they will be immediately resolved with automatic system restores or, if necessary, manual actions will be taken by our experienced Support Desk Team.

As part of the contractual agreement, BOC provides a Service Level Agreement (SLA) with competitive response and recovery times.

For example, BOC guarantees a 99% availability of its services with scheduled maintenance windows outside of normal business hours, response times of less than one hour in case of incident reports, and short recovery times in case an incident lead to an interruption of the service.

Our promise of an available service is supplemented by the contractual obligation to grant service credits of 25% of the applicable service fee, if BOC repeatedly fails to recover service downtimes within the guaranteed time period.

2.3. Maintenance

As part of the maintenance service, BOC Group provides subsequent releases of its Services on a regular basis. Such releases may contain

- introduction of new functionalities,
- preventive measures against security threats and incidents,
- correction of incidents and
- adaptation of the service to legal requirements.

In order to give customers the best possible balance between version stability and early access to new functions, each customer with a dedicated BOC Cloud instance can decide when and how often new releases are to be introduced in their instance. Nevertheless, security-relevant updates may be introduced immediately without prior notice.

Depending on the software version release type (Major, Minor or Long Term Support (LTS)) corrective support is provided for various time periods. Information regarding the current maintenance period can be found in the online documentation centre of ADONIS and ADOIT.

New releases come with adaptation of documentation and a detailed description of the new functionalities. Just have a look at our latest Public Release Announcements (ADONIS / ADOIT) and get familiar with the new capabilities of our services, or subscribe to our newsletter to enrich your transformation initiatives with insights from expert articles, customer experiences, product updates and more!

2.4. Hotline

A specialised Support Desk Service is available for all BOC Cloud Services. BOC Group's technical Support Desk Service handles incident reports and service requests by e-mail or phone. Our team of skilled and highly trained professionals is available to assist you during business hours, ensuring that any issues you may encounter are quickly and effectively resolved. BOC Group's specialists answer your technical questions about BOC Cloud Services with the highest priority. Within our Service Level Agreement we guarantee response times of less than one hour.

BOC Group has implemented organisational measures to ensure that our Support Desk Team has the expertise and knowledge to handle any situation that may arise and that personnel resources are available even in high demand situations. We regularly invest in training and skills development to ensure both the confidentiality of your data, as well as customer-friendly and helpful services.

BOC Support Desk hours:

Monday-Friday, 08:00-18:00 CET, except Austrian bank holidays

BOC support channels:

Telephone: +43 1 905 10 81-2880

Email: hotline@boc-group.com

3. Confidentiality, Integrity and Availability

As an IT service provider, BOC Group puts highest priority on the protection of customer data with respect to its Confidentiality, Integrity and Availability. The technical and organizational measures implemented by BOC Group to ensure information security and data protection include controls:

- to prevent access by unauthorized persons,
- to prevent data processing systems being accessed by unauthorized persons (including encryption processes),
- to ensure that those authorized to use a data processing system may only access the data corresponding to their access authorization,
- to ensure that personal data cannot be read, copied, altered or removed without authorization,
- to ensure that it is possible, after the activity, to check and ascertain whether personal data has been entered in, altered, or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others may be processed only in accordance with the Customer's instructions (contract control),
- to ensure that personal data is protected against accidental destruction or loss,
- to ensure that data collected for different purposes can be processed separately.

3.1. Database Encryption Options

To support our customers in fulfilling strict compliance regulations, BOC Cloud Services offer different database encryption models to choose from, relying on the proven encryption technology provided by the database vendor and state-of-the art key management. Encryption is implemented by means of AES-256 and covers encryption of data files, transaction logs and backup sets. Customers can chose from the following key management options.

3.1.1. Key managed by BOC

BOC manages the key encryption key (KEK) in Azure Key Vault. Customers can request that BOC enables encryption of the database used by the customers' SaaS accounts at any time. This option is available in all BOC Cloud locations.

3.1.2. Bring Your Own Key (BYOK)

It is possible to use the model Bring your Own Key, provided that the customer can export a key encryption key from one of the supported HSM models, then to be imported into BOC's Key Vault. This option is available in all BOC Cloud locations.

3.1.3. Hold Your Own Key (HYOK)

In situations where the customer prefers to have their own key material used to protect the data encryption key (DEK), the preferred option is to apply the Hold Your Own Key (HYOK) model. In such a scenario, the customer manages a Key Vault in their Azure Tenant and dedicates a key to be used for the SaaS database. This option is available in all BOC Cloud locations.

3.2. Encryption at Transfer

All traffic to and from the BOC Cloud platform is encrypted with state-of-the-art cryptographic methods when crossing public internet. This includes HTTPS with TLS >=1.2 for end user traffic as well as API access, TLS 1.3 and IPSec for administrative access by the operations team and for site-to-site connections.

3.3. Business Continuity Management

BOC's Cloud Services is the operations model for many customers relying on the optimal reliability, performance, and security for their BOC product accounts. To ensure these service quality attributes even in adverse situations, BOC has developed a Business Continuity Plan specifically for the offered Cloud Services based on an impact analysis covering all relevant services and assets.

BOC Products store data in relational databases and in the file system on the web server. To protect the data in cases of unintended deletion or modification as well as in disaster scenarios where the productive datasets are lost or corrupted, a robust backup and restore procedure has been implemented within the BOC Cloud Services platform.

BOC also maintains a secondary service location for disaster recovery purposes at a state-of-the-art geographical distance from the primary location, operates the baseline services in these locations and executes recovery tests on a regular schedule.

3.4. Penetration Tests

For BOC Group, as a SaaS provider, it is important to conduct regular penetration tests to ensure the security of our systems and applications. By conducting these tests on a periodic basis, we can identify and address vulnerabilities before they can be exploited by an attacker. This not only helps to protect our own systems, but it also helps to protect customers and their data.

Penetration tests simulate hacker attacks under controlled conditions and fulfil two primary functions. Firstly, they help us ensure that we are meeting our security obligations. Secondly, they help us identify any weaknesses in our systems that need to be addressed. We are happy to provide reports of our penetration tests upon request.

4. Compliance

4.1. Data Protection

At BOC Group we are committed to protecting the privacy of our customers and have implemented robust measures to ensure the security and confidentiality of their personal information. We understand that user's personal information must be protected, and we take steps to ensure that data is only processed in a fair and responsible manner.

We are ISO 27001 and ISO 27018 certified, which are internationally recognized standards for information security management and protection of personal data in the cloud. In addition, as an European provider, we strictly adhere to GDPR requirements and are fully compliant with the EU's data protection regulations.

As a SaaS provider we act in the role of a processor and are committed to protecting the privacy of our users. In this capacity, we process personal data only on behalf of our customers and only use this data for the specific purposes outlined in the data processing agreement. These agreements ensure that the processing of personal data is carried out in accordance with the relevant data protection laws, including GDPR. In particular, we

- process personal data only on documented instructions from the customer,
- ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality,
- have implemented appropriate technical and organisational measures (see section 3 Confidentiality, Integrity and Availability of this document)
- only engage another processor with prior authorisation
- assist our customers with the fulfilment of their obligation to respond to data subjects requests.

Data protection and GDPR compliance is our top priority. That's why we only use European data centres for storing and processing customer data. BOC Cloud Services customers can choose between our two primary IaaS providers, either Amazon Web Services EMEA Sàrl (AWS) using its data centre located in Germany or Cloudsigma AG, using its data centre in Switzerland. Similarly, we use the AWS datacentre in France for disaster recovery purposes.

These IaaS services are specifically designed to meet the stringent requirements of European businesses, including the General Data Protection Regulation (GDPR). By using European data centres, we can ensure that your data is stored and processed within Europe, helping you meet any specific data protection requirements you may have and ensuring compliance with relevant regulations.

With regards to the most recognised data protection related decision by the European Court of Justice (ECJ), the so called Schrems II decision, we want to reassure that we, together with our IaaS providers, have taken additional measures to mitigate these risks stipulated by the ECJ within its decision. Our measures include the option for customers to use a Hold Your Own Key (HYOK) model, in which customers retain control of their encryption keys. Together with our IaaS providers, we also assure challenging law enforcement requests and if subsequently required by the authorities, only disclose the minimum amount of data necessary.

4.2. Certificates

4.2.1. ISO 27001

At BOC Group, we prioritize the security and confidentiality of our customers' data. BOC Cloud Services are ISO 27001 certified, demonstrating our commitment to meeting the highest industry standards for information security management.

ISO 27001 one of the most recognized global standards for information security management. It outlines a set of best practices and requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). An ISMS is a framework that helps organizations manage and protect their sensitive data, including financial information, intellectual property, and personal data.

To become ISO 27001 certified, an organization must meet a number of requirements, including:

- Developing and documenting a set of policies and procedures for information security management
- Maintaining an inventory of relevant assets
- Conducting risk assessments to identify potential threats to the organization's information assets
- Implementing controls to mitigate identified risks
- Regularly reviewing and monitoring the effectiveness of the ISMS
- Deriving improvement initiatives from internal and external performance evaluation audits

By meeting these requirements and demonstrating compliance with the ISO 27001 standard, BOC Cloud Services assure their customers and stakeholders that we have implemented strong measures to protect sensitive data and prevent data breaches.

The internationally recognized auditors attested us with the following "Overall Impression": "*The ISMS has already reached a very high level of maturity. For all tasks required by the standard as well as all other relevant procedures, all processes are described in a central process house and illustrated with the in-house tool ADONIS. This enables a very structured approach to be recognized in general. Supporting customers is a recognizably high priority, and therefore all requirements that customers request to support their data protection responsibilities are covered by the corresponding processes.*"

Upon request, we are happy to share our full Statement of Applicability (SoA) and the latest certificate, which demonstrate our commitment to maintaining the highest standards of security and compliance.

4.2.2. ISO 27018

In addition to being ISO 27001 certified, we also adhere to the ISO/IEC 27018 standard, which specifically addresses the protection of personal data in the cloud. This standard outlines best practices for the handling and processing of personal data in a cloud computing environment, including the protection of data privacy, security, and compliance. By following this standard, BOC ensures that our customers' personal data is treated with the highest level of care and respect, and that it is handled in a way that is compliant with relevant data protection regulations.

Please request the full Statement of Applicability (SoA) and our latest certificate to receive more information about our commitment to data protection in the cloud.

4.3. Security Audit

To ensure that we are meeting the highest security standards, we conduct regular internal audits as well as external audits. Our internal audits are designed to identify any potential non-conformities or weaknesses in our systems and processes and to implement measures to address them. We also undergo external audits to obtain certifications such as ISO 27001 and ISO 27018, which demonstrate our commitment to meeting industry-recognized standards.

In addition to these regular audits, we are also open to conducting other audits upon request and at the request of our customers. This allows us to fully address any specific concerns or requirements that our customers may have and to demonstrate our commitment to meeting their needs.

4.4. Notifications

As there can never be a 100% guarantee that security incidents can be prevented, a well-defined process is needed for the case of such security incident or data breach that involves customer data. We have a mature incident response process in place to ensure that the incident is promptly and effectively dealt with. This process involves:

- Identifying and assessing the nature and scope of the incident
- Containing the incident to prevent further impact
- Investigating the cause of the incident
- Implementing measures to prevent similar incidents from occurring in the future

- Notifying affected parties as required by law or our customers' contracts
- Providing regular updates on the status of the incident and any actions taken

We have a dedicated team in place to handle incident response and we work closely with our customers to ensure that any impact on their operations is minimized. Our goal is to quickly and effectively resolve any incidents and to prevent them from happening again in the future.

4.5. Risk Management

Risk Management involves cyclical processes for identifying, analysing, evaluating, and treating information security risks to meet the risk acceptance criteria. The main purposes of Risk Management are systematic control of risk levels and supporting decision making with regards to investment on security counter measures, as well as integration of new technologies. The BOC Risk Management framework is based on the ISO/ICE 27005 standard and best practices for risk assessment from NIST (National Institute of Standards and Technology); both ex-ante indicators (i.e. proactive approach) and ex-post indicators (i.e. reactive approach) are considered for controlling the risks, i.e. implementation of preventive or corrective measures.

Internal and external context of the organization, including cloud services customers' requirements and expectations with regards to security and data protection, are considered in the Risk Management program. This means that all information and ICT assets (either owned by BOC or supplied by third parties) such as infrastructure elements, systems, services, facilities as well as processes and procedures that are relevant for development, operation, and support of BOC SaaS products are subject to regular risk identification, evaluation, and treatment.

In the identification phase, possible threats and relevant vulnerabilities of assets are defined and risk scenarios are formulated. Furthermore, identified risks are analysed to determine if existing controls and measures are adequate to resist the threats; otherwise, risks are evaluated to estimate their probable impacts and likelihood of occurrence. Additionally, risk treatment strategies (i.e. mitigate, accept, transfer, avoid) are assigned to evaluated risks and treatment measures are prioritized. Treated risks must be re-assessed according to a schedule to verify the effectiveness of implemented measures and the acceptability of residual risks. Evaluated risks are reported to top management where further initiatives are discussed and planned.

BOC's Risk Management program and processes are monitored and evaluated for their effectiveness by the means of annual reviews as well as measuring and analysing Key Performance Indicators ; adaptation is done where deemed necessary.

4.6. Supplier Management

BOC relies on suppliers to provide their services in accordance with regulatory requirements, as well as industry best practices and standards. Each supplier is selected according to strict guidelines to reduce information security risks. Suppliers who meet the security requirements and pass the security assessment are selected. These security requirements comply with industry relevant standards, regional and global regulations and obligations, as well as BOC's SaaS customers' security and data protection expectations.

Supplier management processes consist of Suppliers Identification and Evaluation where suitable suppliers are selected after their capabilities with regards to security, compliance and business expectations are evaluated; Contract Management where security and compliance requirements such as Non-Disclosure-Agreement, Data Processing Agreement, Technical and Organizational Measures, and other expectations such as SLA, audit right, incident handling collaboration, contact details, non-compliance consequences, etc. are negotiated and agreed upon. Supplier Service Delivery Management where suppliers' performance, compliance with agreed security measures, and changes to the provided services are monitored and managed. Furthermore, in the course of Risk Management processes, relevant risk scenarios emerging from suppliers and provided services are evaluated and monitored.

BOC's SaaS offering relies on the public cloud Infrastructure as a Service (IaaS) provided by Amazon Web Services (AWS) and Cloudsigma AG that are located in EU and Switzerland and ensure data sovereignty within these regions. Both providers use state of the art data centres that comply with relevant security and compliance

requirements and are certified for ISO 27001, ISO 27018, ISO 27017, ISO 9001 standards, as well as GDPR. In addition, AWS even offers a stronger security compliance program by being compliant with industry and country/region specific standards such as GxP, PCI DSS, FedRAMP, HIPAA, C5, etc. and providing SOC 1, SOC 2, and SOC 3 reports.

4.7. Intellectual Property Rights

BOC Group is aware of its responsibility with the handling of your confidential data entrusted in our tools and therefore strictly refrains from using such data for its own purposes. All data stored in our Services are the sole intellectual property of the Customer. Nevertheless, we protect this data like our own. BOC Group has state of the art measures in place to protect this data from unauthorized access by third parties and will ensure its constant availability through continuous data backups.

Customers are free to export their data stored in the service at any time. Even after termination of the service, we keep your data for another 90 days and make it available to you in standardized formats for your further use (XML).

On the other hand, the provided Products and Services are the intellectual property of BOC Group and are licensed to you on a user-based scheme. Our user-based licensing model allows you to enjoy the benefits of transparent access limitations and full cost control. With this model, you only pay for the users you order, so there are no hidden costs or surprises when exceeding transactions. In addition, user-based licensing offers flexibility, as usage rights can be easily transferred to other people in your company at any time. Plus, you won't have to worry about geographical or hardware limitations. Overall, user-based licensing ensures that you have full control over your costs and access to our Products and Services.

When you use our Services, you can trust that we are committed to ensuring that no third-party intellectual property rights are infringed. We take great care to ensure that our Services are fully compliant and that our customers are protected. With BOC Group, you can confidently and securely use our Services, knowing that you are protected against any potential intellectual property violations.

4.8. Ethical and Environmental Considerations

At BOC Group, we take our commitment to ethical, environmentally responsible, and corruption-free practices very seriously. Our team is fully aware of their responsibilities in this regard, and we have implemented a range of measures to ensure that we meet the highest standards in all of these areas. We are dedicated to providing our customers with the best possible service, and we believe that this requires us to adhere to the highest ethical and legal standards at all times.

BOC Group commits its employees to apply its high ethical and environmental standards in their day-to-day behavior with others. Among others, this includes human rights, equality, health and safety, anti-corruption and anti-bribery principles. BOC Group promotes respectful cooperation, collaboration and environmental protection within the company. Furthermore, when selecting its suppliers and subcontractors, BOC Group strives to commit them to the same level of ethical and environmental standards. BOC ensures that any potential contractors and suppliers at all levels are carefully evaluated before they are selected.

4.9. Industry-specific Compliance Requirements

BOC Group commits to upholding the highest standards of compliance and is fully aware of its responsibility to adhere to industry-specific regulations. We understand that industries such as banking, pharma, and insurance have strict compliance requirements, and we are committed to meeting these requirements. BOC's commitment is shown by serving many customers from these industries with strict compliance regulations.

We want to assure you that we are committed to meeting these standards and have implemented necessary measures to ensure compliance, including conducting regular reviews of our outsourcing arrangements and maintaining robust governance and risk management frameworks. This includes regular audits and reviews of our processes and systems to ensure that we are meeting all necessary regulations.

In addition, we require our suppliers, including IaaS providers, to also adhere to these compliance standards. We have robust vendor management processes in place to ensure that all our suppliers are meeting these requirements.

4.9.1. Financial Institutions

When it comes to outsourcing to a cloud provider in the financial sector, various regulations apply depending on the location of the financial institution. For European financial institutions, most commonly the EBA guidelines on outsourcing arrangements apply. For German institutions, the MaRisk AT 9 and § 25a KWG might be applicable as well. Austrian finance institutions need to adhere to § 25 BWG. All these guidelines are intended to ensure that outsourcing transactions are carried out in a safe and sound manner, with appropriate risk management measures and defined legal arrangements are in place.

As a cloud service provider serving the financial industry, we take compliance with relevant regulations very seriously. We are committed to ensuring that our services meet the high standards set by the European Banking Authority (EBA) in its guidelines on outsourcing arrangements or other national authorities.

To that end, we have implemented several measures to ensure compliance with these guidelines. These measures include:

- Conducting regular risk assessments of our operations and suppliers
- Establishing clear contractual arrangements with our customers and suppliers
- Implementing outsourcing addendums with our Infrastructure as a Service providers including the introduction of a right of access and audit
- Implementing robust governance arrangements to ensure that we are able to effectively manage our outsourcing relationships
- Having comprehensive business continuity plans in place to ensure that we are able to continue operations in the event of a disruption
- Implementing appropriate measures to protect data and maintain the confidentiality, integrity, and availability of our systems

In addition to these measures, we also have a track record of successfully serving financial industry customers. We have many reference customers in the financial sector and have therefore proven our ability to comply with relevant regulations and standards. We take pride in our commitment to compliance and our ability to provide reliable, secure, and compliant cloud services to our financial industry customers.

4.9.2. Insurance Institutions

As a Cloud Service provider, we support regulated companies in the insurance sector in complying with the rules on outsourcing in the cloud set forth by EIOPA. According to the EIOPA, control of the outsourced Cloud Services shall be in proportion to the nature, scope, and complexity of the risks associated with the services we provide. On request we provide support for the risk assessment, documentation and analysis of the outsourced services required by this regulation.

In addition, the rights and obligations of the customer and the rights and obligations of BOC Group should be clearly allocated and set out in a written agreement. Such agreements allow the actual exercise of access and audit rights of the outsourcing company. The measures described in this document provide our customers with the necessary information to determine that we, as the Cloud Service provider, are compliant with European and national regulations, as well as appropriate ICT security standards.

In order to provide our outsourcing customers with the necessary control over our services, we have entered into appropriate outsourcing agreements, particularly with our IaaS providers. These agreements allow our outsourcing customers to extend their control rights to our services and ensure that we are meeting their needs and expectations.

In addition to extending control rights to our outsourcing customers, we are willing to extend the outsourcing agreements to allow for the establishment of termination rights and exit strategies. This helps to ensure that our customers have the necessary flexibility to adjust our services to their evolving needs and to end the relationship if necessary. We believe that it is important to have clear and fair terms in our agreements, and we are committed to working with our customers to find mutually beneficial solutions.

4.9.3. Pharmaceutical Industry

There are specific industry requirements for outsourcing to the cloud that are relevant pharmaceutical companies, particularly in regards to GxP (Good Practices for the pharmaceutical industry) and FDA 21 CFR Part 11.

GxP is a set of guidelines that provide a system for ensuring that products are consistently produced and controlled to the quality standards appropriate for their intended use. In the context of outsourcing to the cloud, it is important for pharmaceutical companies to ensure that their cloud provider is able to meet GxP requirements and can provide a secure and compliant environment for the storage and processing of regulated data.

FDA 21 CFR Part 11 is a set of regulations issued by the US Food and Drug Administration that establish the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records. If a pharmaceutical company is considering outsourcing to the cloud, it is important to verify that the cloud provider can meet these requirements.

BOC is a reliable partner for the provision of Cloud Services to pharmaceutical customers. We have a proven track record of working with many pharmaceutical customers and helping them achieve compliance with GxP and FDA 21 CFR Part 11 requirements. Our team is highly experienced in working with regulated industries and is committed to providing a secure and compliant environment for the storage and processing of regulated data. We are confident that we can support your company's needs as a trusted provider of Cloud Services in the pharmaceutical industry.