Pharmatek Solutions

Driving Compliance, Empowering Innovation

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Pharmatek Solutions

Driving Compliance, Empowering Innovation

ISO/IEC 27001:2013 Certification
(Information Security Management System)

ISO/IEC 9001:2015 Certification
(Quality Management System)

Leadership team with **60+ Years of Domain Experience**

Global Presence
HQ: San Ramon, CA, USA
Siler City, NC, USA
Hyderabad, India
Dublin, Ireland

Engaged with **25+ Emerging Biotech, Big Pharma, & Cloud** providers globally

Over **80** qualified professionals in the organization, 40% auditors

900+ Audits completed,
70+ GxP System Implementations

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Pharmatek Solutions

Computer System Validation (CSV) Audits

Pharmatek can perform the full range of CSV and IIT process audits including IIT security, computer system validation, and FDA 21 CFR Part 11/EU Annex 11 compliance checks to ensure all aspects of regulated computer system risk have been explored, understood, and remediated where necessary.

Computer System Validation Auditing

- System-specific Computer System Validation Audits
- Data Centers
- Backup and Data Recovery
- Business Continuity and Disaster Recovery
- IT Security

Computerized System Development Life Cycle (SDLC) Process Audits

System & Application Development Processes, Including Planning, IQ/OP/PQ, Implementation, and Change Control

FDA 21 CFR Part 11/EU Annex 11 Compliance Gap Analysis

Issue Management and Remediation

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Cloud Compliance Audit Blind Spots

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Backups

Snapshots in lieu of full file/server-based backups:

Snapshots are stored on the same physical devices by default. If Snapshots are leveraged as a backup, they should be shipped off the primary media to a secondary location.

Why is this important:

If the snapshot isn't copied elsewhere, if the primary storage for the server and snapshots fail, everything will be lost and this technique creates a very lengthy restore process of files or folders.

Verification backups are checked for completeness:

Backup software is inherently flawed and doesn't always complete successfully. Restoration verification removes this risk. Are restores periodically tested?

Why this is important:

Backup errors can persist over days or weeks and failures can make it impossible to recover data from backups.

On multi-tenant systems

Will a restore request for another customer force your company to go back in time and lose data:

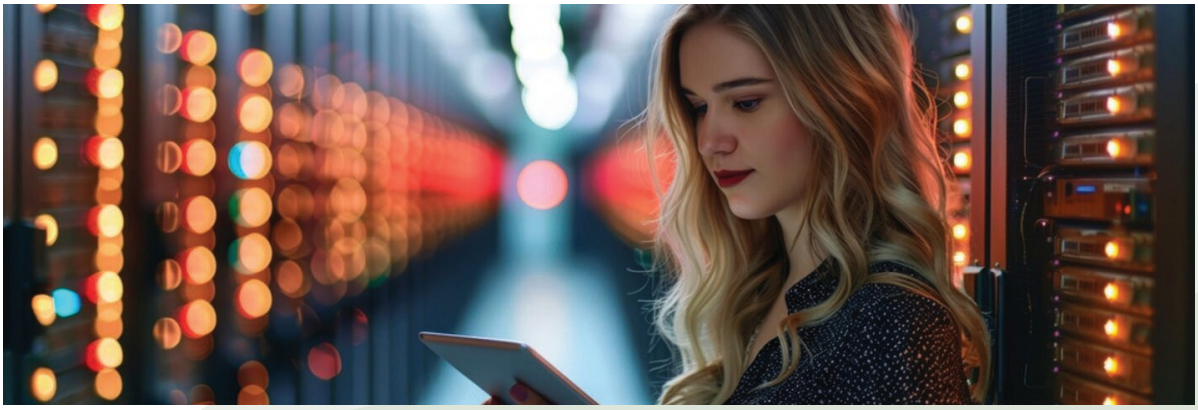
Some SaaS/PaaS designs leverage one system or database for multiple customers. If data from multiple customers is intermingled within the file system or within a database, one company data recovery can impact other customers.

Why this is important:

A restore of data from one of the tenant can create either a rollback in time, or a freeze of the system activities until the restore process is complete.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Technical Staff



Expertise

Software Developers doing IT Engineering tasks:

Software developers are not IT Engineers. It is similar to having an electrician perform plumbing in your home.

Why is this important:

Software development, Tech/DevOps and IT Engineering are different skillsets. IT Engineering requires experience as does writing good code. In either scenario when one role is trying to do the others, the output will be most likely functional, but not resilient or implemented correctly (due to the lack of experience).

Coverage

Are there enough skilled IT Engineers on staff to cover vacations, holidays or a sudden change in staffing levels:

If there isn't enough staff in proper coverage numbers, then the service provider runs the risk of not having proper staff to attend to issues.

Why this is important:

If there is one skilled IT Engineer on staff, what happens during their vacation, sick days or if they leave. Who has the experience and skill to cover. Nobody should be expected to be on-call 24/7.

Security

Tooling

Are the security tools in place the current standard:

Security tooling is moving very quickly as it is quickly becoming a battle of the "have's and the have nots". The "have nots" will become easy targets.

Training

Security training is an organizational obligation and not just for the security team. It is important to understand how the service provider manages security training:

Small security issues can become big security issues and they can originate from anywhere in the service provider staff or technical footprint.

Common Vulnerabilities and Exposures (CVEs)

How is the service provider tracking, managing and remediating Common Vulnerabilities and Exposures (CVE)s:

It is important to understand the processes for monitoring and actions the service providers take when high-risk CVEs are issues. What is the timeliness and process to remediate.

Risk

There should be strong security personnel to evaluate true risks:

Available exploits in a solution doesn't mean there's a real security risk as one needs leverage to exploit a risk.

Conversely, any open network port to the internet should be covered by up-to-date intrusion detection and intrusion prevention solutions and are vigilantly patched. VPN connectivity is preferred.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Technical Debt

Technical Debt means the age and supportability of critical components of the service delivery platform needs to stay current, patched and within support by its manufacturer:

Operating Systems, databases, software, network devices and other components in SaaS or PaaS offerings age over time and eventually come out of supportability.

Why is this important: Aging components need to be maintained regularly or the staff will create a "wall of work" to catch up to current standards. As components age, their interoperability with other components increases risk. Deferred maintenance is an indicator of an immature service offering and prioritization.

Service platforms should be on the latest stable release or the previous release (and patched):

When things get busy it is easy to ignore platform based upgrades customer systems rely upon. When technical debt is present, it is an indicator that there isn't enough staff to keep platforms current.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Backups

Snapshots in lieu of full file/server-based backups:

Snapshots are stored on the same physical devices by default. If Snapshots are leveraged as a backup, they should be shipped off the primary media to a secondary location.

Why is this important:

If the snapshot isn't copied elsewhere, if the primary storage for the server and snapshots fail, everything will be lost and this technique creates a very lengthy restore process of files or folders.

Verification backups are checked for completeness:

Backup software is inherently flawed and doesn't always complete successfully. Restoration verification removes this risk. Are restores periodically tested?

Why this is important:

Backup errors can persist over days or weeks and failures can make it impossible to recover data from backups.

On multi-tenant systems

Will a restore request for another customer force your company to go back in time and lose data:

Some SaaS/PaaS designs leverage one system or database for multiple customers. If data from multiple customers is intermingled within the file system or within a database, one company data recovery can impact other customers.

Why this is important:

A restore of data from one of the tenant can create either a rollback in time, or a freeze of the system activities until the restore process is complete.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Third-Party Service

Service Account and Built-in account Management

How are built-in and service accounts kept secure?

Many devices have built-in administrator accounts which cannot be removed or are the only option for managing that device. Additionally, service accounts are often created so that one system can communicate with another. Quite often, these built-in and service accounts have elevated privilege levels.

What to look for:

Is access to the passwords for these types of accounts restricted in such a way that only those with the highest level of access can retrieve them and are those retrievals logged and attributable to specific users?

Are these passwords changed from time-to-time?

Is use of these kinds of accounts kept to the bare minimum?

How does the use of third-party services affect the operation if they are offline?

With so much moving to cloud-based services, what is the impact to these services being unavailable from time-to-time, and how can a loss of availability be mitigated?

What to look for:

If a cloud-based service such as email, antivirus, server/service hosting, etc. becomes unavailable for some period of time, what is the business impact?

Have proper contracts and service level agreements been established such that any outage is guaranteed to be within the tolerance of the business requirements.

Does the service provider have proper controls and services to guarantee a minimum of disruption in the event of an outage.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Third-Party Service

Security

What level of access does the vendor have to my data? If they have access, what policies do they have in place to ensure that my data is not accessed?

Encryption policies

What encryption policies are in place in transit and at rest?

The serviced provider should be able to share the encryption algorithms for both data in transit and at rest.

Source Code Escrow

Software source code for smaller providers should be available:

In the event the service provider goes bankrupt, the customer can obtain a copy of the software to self-support until a new solution can be provided.

Service Contracts/Support

Are service contracts with the manufacturer maintained on all hardware, software, and platforms?

Any device in an environment which can impact the availability or security of operation should have active service and support contracts with the manufacturer.

Why is this important:

Fixes for bugs and security flaws are typically available on to those with active service contracts.

In the event of an outage or disruption in service, it may be necessary to contact the manufacturer to analyze and remediate the outage.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Disaster Recovery

What is the RTO/RPO and do I get to decide if/when my systems is failed over? If the system is failed over, what data would you lose?

You may lose data if your RPO is 24 hours and you fail over 23 hours later. If you get to decide if you fail over or not based on the type of outage, then you may choose not to fail over as to not lose data.

Is testing done periodically to ensure systems come up in remote environment? Does this ensure that the RTO and RPO can be met for my system.

Testing should be conducted to make sure that the system comes up in the remote location. However, if you chose a recovery point outside of the RPO, then it may mean that you can't get the data back in that timeframe. Also, if infrastructure needs to be restored first, then it may impact the time of recovery.

Do backups and monitoring continue to work in the DR environment?

If the system if failed to a remote location, you'll want to confirm that you have these tools enabled before you start doing work on the system.

Business Continuity

The service provider should be able to prove their business continuity of staff and technical solution.

Geographic diversification of technical staff and geographic resilience of the platform should be available.

What's the failback process?

If the system is going to be failed back, could you lose additional data?

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Operating System

Patching of customer systems and service provider management systems:

Need to make sure operating systems are at a near term patch-level and not left unpatched for long periods of time.

Patching

How are maintenance periods managed? What is the communication? Do I get to decline patching for my system/applications?

Understanding when your system may not be available and options you have for ensuring it's available when you need may be critical to your business.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Database

Database backup properly configured

Database backups should meet customer requirements and be configurable and monitored for success.

Patching

Databases should be patched routinely for security and known bug fixes (not inclusive of major releases, service packs or similar)

Database monitoring is setup:

The service provider should be monitoring connectivity, database processes, database partition capacity.

For multi-tenant solutions, each customer database schema should be separated.

In the event one customer needs to do a database restore, this activity shouldn't impact other customers database instances.

Capacity

Are resources (CPU / RAM / Disk / Bandwidth / Power / etc.) within the environment managed properly?

Within an IT operation, there are always "consumable" resources. For instance, every time a new server is built, it may consume hardware resources such as RAM and CPU, software resources such as licensing, space for backups, DR reservations, etc.

What to look for:

Are there processes in place to allocate, monitor, and manage those resources?

Do these processes consider day-to-day operational changes?

Do these processes account for failures within the domain, such as a power circuit, storage system, or ISP outage?

Risk

Ownership of data

Is there any component of the solution where the service provider, or third parties can lay claim to any of the processed data (e.g., AI programs learning from your data). If it is present, can you disable it (e.g., DocuSign)

Service provider having an understanding and remediation of people, process and technical risks.

Everything breaks, people leave and processes breakdown. How does the service provider protect critical areas of their service delivery.

Emailed Alerts:

How are platform alerts collected and aggregated? If email is used, how is it verified that email notifications or alerts are being sent/received.

Verification emails are being sent/received from their sources to appropriate parties is critical. Without these alerts, failures without received warnings can follow. Using aggregators such as Splunk, are useful to sift through the noise, but if tools like Splink never get the alerts, the tool doesn't warn of a risk.

Operations Risk Management:

How is risk being managed in the operation of the environment?

IT Infrastructure requires constant maintenance to avoid technical debt, patch security flaws, and improve performance and functionality. These maintenance activities are typically in the form of software updates and configuration changes, which carry inherent risk due to changing the behavior of the devices and systems that they run on.

What to look for:

Using methods such as installing only GA/LTS software releases, maintaining a full test environment in which patches can be evaluated before being installed in production, and having comprehensive back-out plans can help mitigate these risks.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Risk

Risk in Complexity

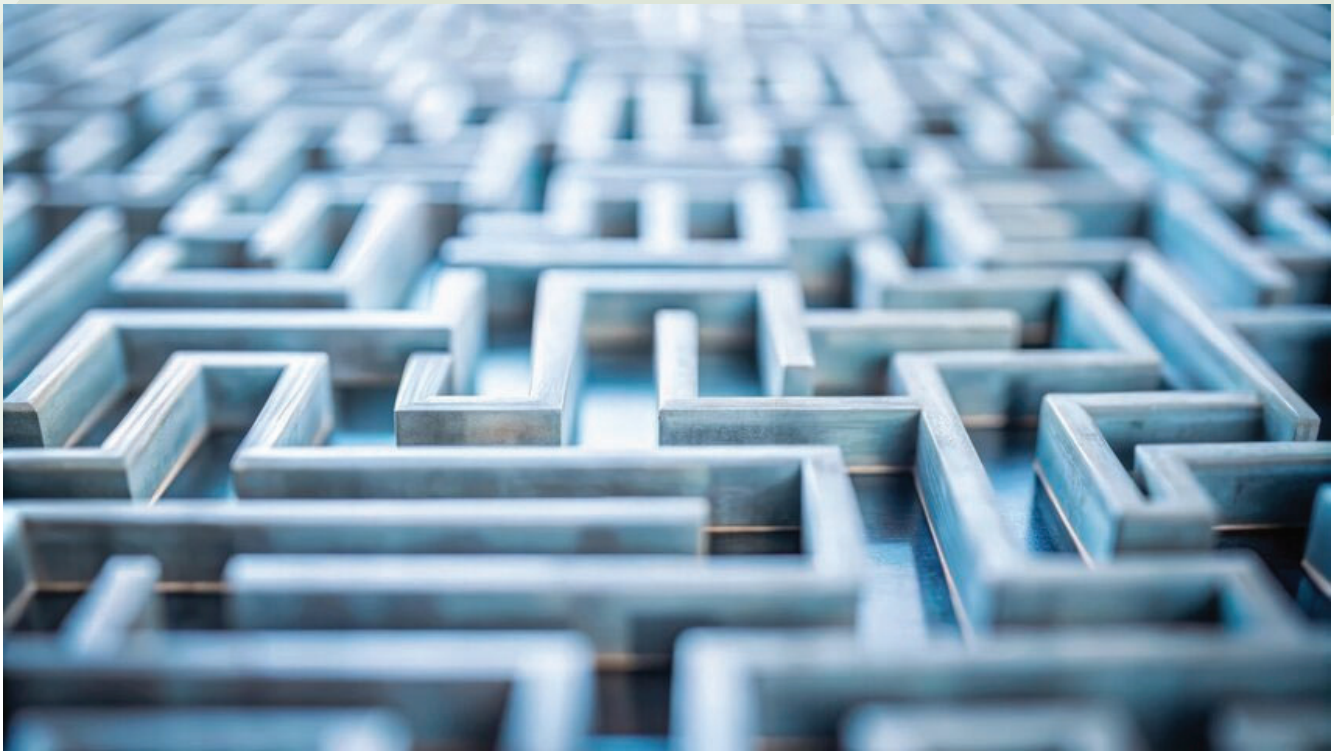
Have efforts been made to reduce complexity and build a consistent environment?

Often, IT environments will be deployed ad-hoc, by different people at different times, or with poor planning. These environments can have "sprawl" or "cruft" and even multiple systems with identical usage can be configured differently at different times.

What to look for:

Are any configuration management tools or procedures in place?

Are there processes to ensure consistent deployment and on-going management?



Pharmatek Solutions
Driving Compliance, Empowering Innovation

Audit

What am I provided if I am audited by an agency?

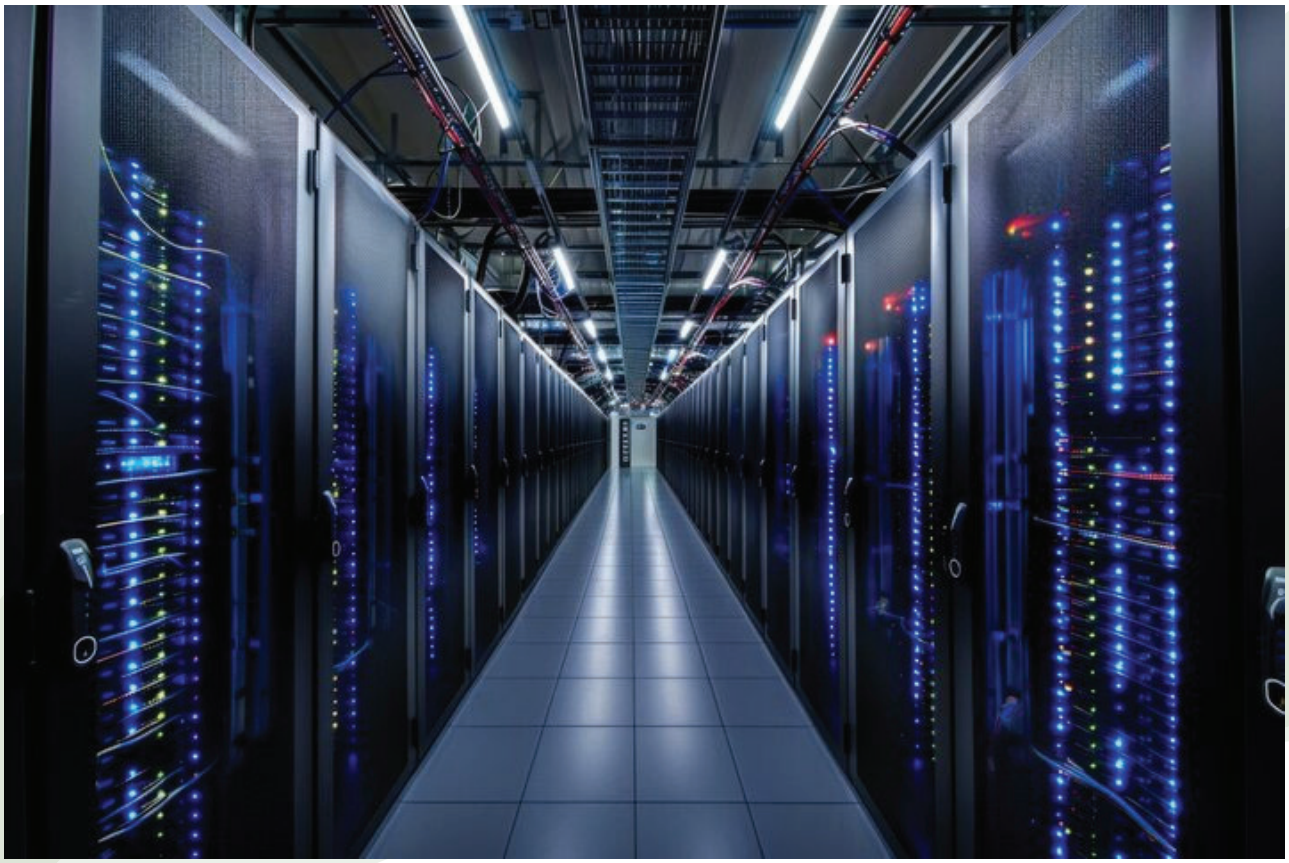
The service provider should understand the regulatory audit responsibilities and times lines for responses.

How does the service provider track new regulations and guidances' and what's the process for integrating applicable new regulations.

Having a documented process with objective evidence is critical to see that they are taking their regulatory compliance responsibilities seriously.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Decommissioning



Do you have a decommissioning procedure and how do I get my data back?

Having a procedure ensures that you understand what will happen to your data if you need to leave the environment and ensures that you can get your data back or store it per regulatory requirements.

At the end of an agreement, in what form will data be provided and can they share an example.

Exports should be in human readable form and/or not need the service provider to continue to access and use the data for regulatory purposes.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Public Cloud

How do you ensure that my data remains in a certain location?

Locations are set up in public clouds which may allow your data to be stored in other countries. It is important to understand how the provider managed data movement and how the locations are managed.

How is my data segregated from other clients in the public cloud?

Are there separate subscriptions? Tenants? Other methods?

How are security policies maintained and documented for my environment? Do we have the ability to maintain separate policies for each customer environment?

Global policies may only be applied and you may have no control over these policies. If that's the case, how does the vendor ensure that these are up to date and changes don't impact your environment.

Service Level Agreement:

Does the cloud provider offer SLAs for uptime, performance guarantees, and support responsiveness?

Understanding SLAs with Cloud providers is essential for ensuring uptime, performance guarantees, and support responsiveness. Companies must understand what SLAs mean and plan accordingly for redundancy as well as fail over strategies.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Public Cloud

Third Party Integration

Does the cloud provider integrate with currently utilized third-party tooling?

The integration of third-party systems into cloud platforms is difficult due to the differences in their APIs, authentication methods, and data formats. Integration complexities must be dealt with to ensure compatibility and reliability.

Legacy System Integration

Will the cloud vendors API integrate into my legacy applications?

The integration of cloud-native applications with legacy systems may be challenging due to architectural and technology stack differences. Companies must account for data migration, API compatibility, and the possibility to re-engineer some systems to achieve seamless integration.

Audit

Does the cloud vendor offer auditing tools for your environment and how are they configured?

Most public cloud providers offer audit trail features to help customers monitor and manage their cloud environments effectively. These features provide a detailed record of activities and changes within the cloud infrastructure, which is crucial for security, compliance, and troubleshooting. However, some of these features may not be activated automatically.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Public Cloud

Cloud Costs

Does the cloud vender offer tools to monitor cost of resources provisioned?

Inefficient management of resources can lead to a blow-out in cloud costs. Companies should always monitor usage of resources, select less costly instance types, and implement auto scaling and resource tags policies. Cloud billing is complicated with prices based on CPU hours, storage space used, data transferred etc. To avoid unexpected costs, companies should understand billing metrics, set budgets, and use cost management tools.

Connectivity

Is the network connectivity to the cloud provider redundant?

Reliable connectivity is essential for public cloud services. Companies should plan for network redundancies, implement caching strategies, deploy Content Delivery Networks (CDNs) while also considering caching methods to mitigate connectivity issues.

Access Management

Are access audits performed on a regular basis?

It is difficult managing access permissions, roles, or policies across different cloud services. To avoid unauthorized access, utilize centralized identity & access management (IAM), enforce the principle of least privilege, and conduct regular audits on access controls.

Data Security

Is storage data encryption available on cloud-based storage?

Cloud storage requires secure data handling procedures. Companies must encrypt sensitive information and configure communication protocols to that storage. Such as TLS protocol and cloud native security offerings including Key Management Service (KMS) and Encryption at Rest.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Public Cloud

Versioning

Are there processes in place to evaluate changes to public cloud APIs?

As cloud services and APIs change with time, it is necessary to update versions and functional changes. This requires managing version dependencies, API compatibility, and planning for upgrades to avoid application disruptions.

Business Continuity and Disaster Recovery

Are there business continuity and disaster recovery plans in place for when public cloud infrastructure or connectivity is unavailable?

Although cloud providers offer disaster recovery options for networks there is still a need for robust business continuity plans. Engineers should run regular disaster recovery drills, introduce failover mechanisms, or keep backups at several geographic locations.

Backup and Recovery

Are backups in place to recover systems in the event of data corruption?

While cloud providers provide backup and disaster recovery services, companies must configure these solutions adequately and test them. This includes setting backup schedules that align with application recovery point objectives (RPO) and recovery time objectives (RTO) requirements and perform disaster recovery drills to verify those RPOs and RTOs.

Pharmatek Solutions
Driving Compliance, Empowering Innovation

Public Cloud

Compliance

Does the cloud provider have compliance documentation and certificates available to Customers.

Public cloud providers typically have compliance documentation to help their customers meet regulatory and security requirements. These documents outline how the cloud provider's infrastructure and services align with various standards and regulations. Providers should have reports from third-party auditors about their adherence to standards like ISO 27001, SOC 1, SOC 2, SOC 3, PCI-DSS, and others. They also should offer guides and whitepapers that explain how their services can help customers achieve compliance with specific regulations, such as GDPR, HIPAA, or CCPA.

Monitoring

Are monitoring tools configured to identify issues with cloud-based infrastructure and applications?

Monitoring of the Cloud resources and applications is critical in identifying performance constraints, optimizing resource usage, and maintaining service levels. Companies must establish performance baselines, configure monitoring tools, and tune applications and infrastructure proactively. Companies must utilize comprehensive monitoring and logging solutions because the cloud can be hard to debug due to being distributed in nature.

Skillset

Have current FTEs been trained to manage public cloud environments?

Organizations have difficulties recruiting or upskilling those who understand how to develop using native-cloud technologies, cyber-security intricacies, or operational management issues such as patching physical infrastructure together. This also involves learning specific tools and APIs used to interact with various public clouds. It might require education on new competences or certificates to effectively employ these services in practice.