



# Auditing XaaS Providers for GxP Applications

Stephen R Ferrell  
Managing Director, Americas  
CompliancePath Ltd.  
GAMP Boston Forum  
Jan 2020

1

## CompliancePath Overview Services & Solutions

### CompliancePath Experiences

- ✓ 5 + years Industry experienced CSV specialists
- ✓ "SCOTsourcing" – Remote deployment from Scottish test centre of excellence
- ✓ CompliancePath principles have trained the FDA on cloud, computer validation and data integrity.
- ✓ Global client base
- ✓ Cross vertical customers: Pharmaceutical, Biotech, NHS, CRO, Medical Device.

### Service Models

- ✓ Validation/Compliance/Quality as a Service
- ✓ Cost efficient and transparent
- ✓ Plug-and-play compliance with fixed costs

### CSV Approach

- ✓ Risk Based Approach
- ✓ Full suite of executed validation documentation
- ✓ GAMP Influenced
- ✓ Pragmatic Compliance



Connecting

Pharmaceutical

Knowledge

ispe.org | 2

2

# GxP XaaS Delivery

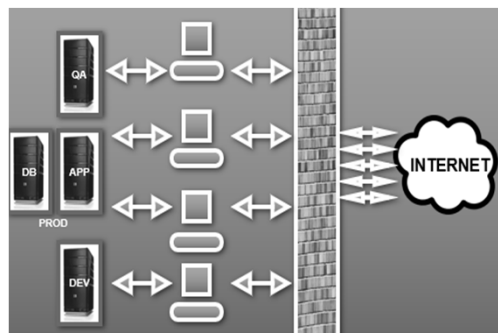
## Delivery Models & Risk

3

3

### Traditional GxP Application Delivery

..the way it was

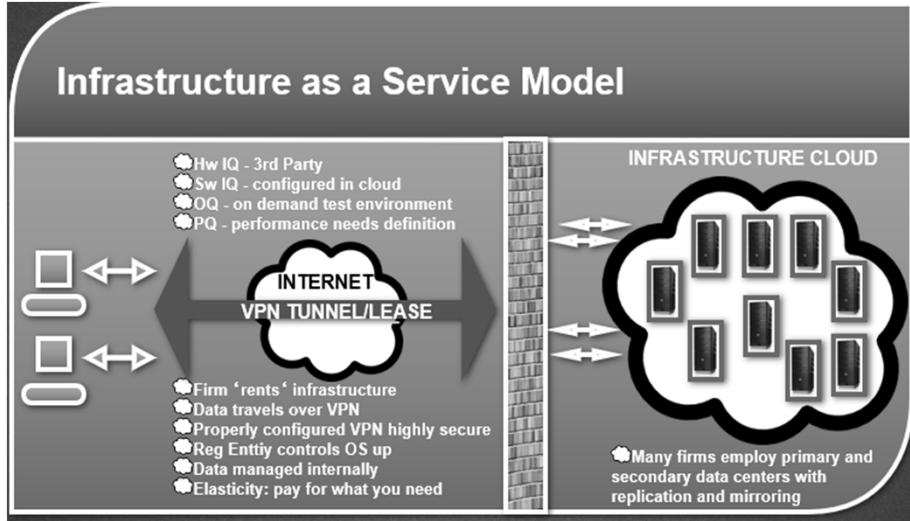


- Physical Servers
- Hardware on site
- QA & Prod Servers IQ'd
- QA used for OQ
- PROD used for PQ
- Client PC's have Client side application software
- Contained behind corporate Firewall
- Infrastructure considered 'low risk'

4

## IaaS GxP Application Delivery

Underneath the application



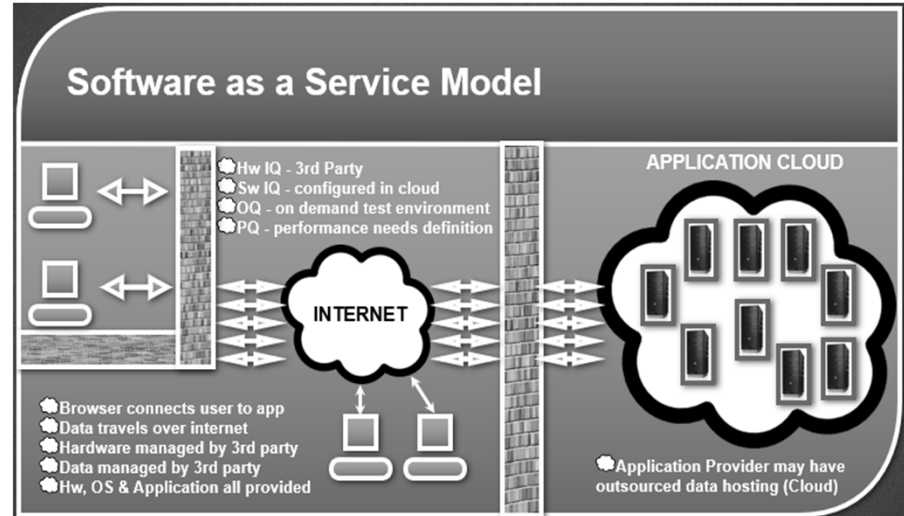
Connecting Pharmaceutical Knowledge

ispe.org | 5

5

## SaaS GxP Application Delivery

Application Delivery



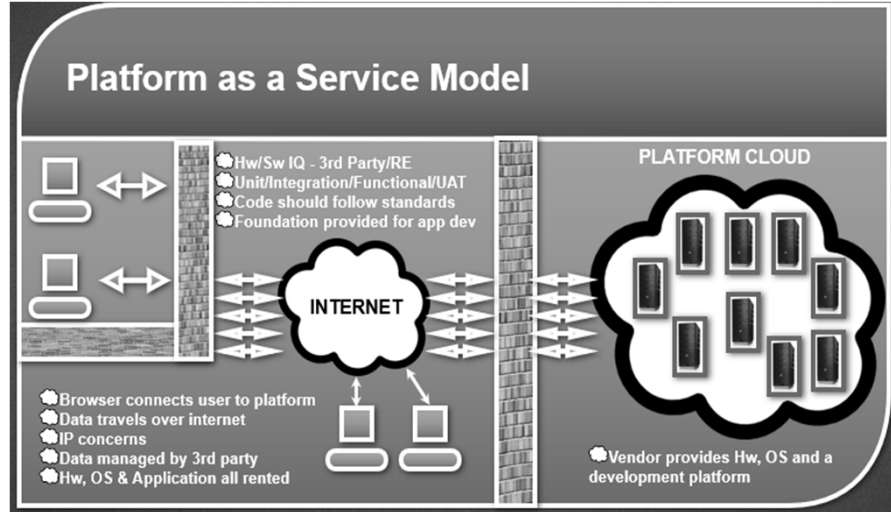
Connecting Pharmaceutical Knowledge

ispe.org | 6

6

## PaaS GxP Application Delivery

### Platform Delivery



7

## GxP SaaS Controls

What to look for...

- Service Level Agreement (I/P/S)
- Validation & Qualification (I/P/S)
- Data Privacy (I/P/S)
- Data Segregation (I/P/S)
- Change Management (I/P/S)
- Configuration Management (I/P/S)
- Security Management (I/P/S)
- Server Management (I/P/S)
- Client Management (I/P/S)
- Network Management (I/P/S)
- Problem Management (I/P/S)
- Help Desk (I/P/S)
- Backup, Restore, and Archiving (I/P/S)
- Disaster Recovery (I/P/S)
- Performance Monitoring (I/P/S)
- Supplier Management (I/P/S)
- Periodic Review (I/P/S)
- Retirement of Platforms (I/P/S)
- SDLC Standards (S/P)
- Software companies may not fully grasp cloud delivered applications
- Managed services are not within the traditional threshold of software companies
- In many cases they may have outsourced their Infrastructure and may not be asking the right questions



8

## GxP Cloud Model

Building Blocks...

VALIDATE

Connecting
Pharmaceutical
Knowledge

ispe.org | 9

9

## Cloud Risks for e-Records

Part 11 on the move

- ✓ Privileged user access - who has access to the data
- ✓ Open/Closed system line becomes blurred
- ✓ Changes such as OS patches can impact validated status if not properly managed
- ✓ SLA needs to extend accountability of Part 11 adherence to all stakeholders
- ✓ Data segregation – how is it proven / enforced
- ✓ Encryption is effective but isn't a cure-all.
- ✓ Restore & Recovery – required to test and prove it
- ✓ Data Quality vs Data Integrity

Connecting
Pharmaceutical
Knowledge

ispe.org | 10

10

## GxP Cloud Model

Building Blocks...

- ✓ Cloud offers no substantive benefit to Compliance
- ✓ Raises Risk profile of Network Infrastructure
- ✓ Puts importance IT SOP's on an equal footing with Mfg.QA.QC SOP's
- ✓ Potentially places vast amounts of FDA regulated data in the hands of untrained personnel
- ✓ Can help drive down COGS for Regulated Entities but will cost translated into efforts to strengthen SISPQ?
- ✓ 'Big Data' offers immense possibilities for R&D and clinical studies

**ISPE**      Connecting      Pharmaceutical      Knowledge      [ispe.org](http://ispe.org) | 11

11

## GxP XaaS Delivery

Delivery Models & Risk

12

12

## Auditing GxP SaaS Application Providers

Leveraging 3<sup>rd</sup> party certifications



- ✓ We can leverage 3<sup>rd</sup> party certifications to build a case for GxP compliance
- ✓ Not all certifications are created equally
- ✓ SOC 1 & SOC 2 controls are not the high water mark but rather the first step to assurance
- ✓ ISO 27001 is a far better indicator as to a company's commitment to data management
- ✓ NIST 800:53 provides the most holistic control set that covers not only the cloud controls but also the SDLC



Connecting

Pharmaceutical

Knowledge

ispe.org | 13

13

## Auditing GxP SaaS Application Providers

Using FedRAMP/NIST 800:53



- ✓ We can use publicly available FedRAMP and NIST guides to build our own GxP Application audit
- ✓ Vendors should be audited based on the risk of the application they are delivering
- ✓ Maturity of GxP understanding varies widely, some Cloud providers are GxP centric like Validated Cloud others rely on third party certs to build their case like Amazon and Azure.
- ✓ We need to change traditional audit approaches to fully appreciate xaaS delivery for GxP applications



Connecting

Pharmaceutical

Knowledge

ispe.org | 14

14

## FedRAMP

### Program Highlights

- The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a “do once, use many times” framework that saves cost, time and staff required to conduct redundant agency security assessments.
- Allows the Federal government to provide a comprehensive Cloud based framework without endorsing a single 3rd party or NGO framework.



Connecting

Pharmaceutical

Knowledge

ispe.org | 15

15

## FedRAMP

### Control Categories

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity

Based on  
NIST SP  
800-53



Connecting

Pharmaceutical

Knowledge

ispe.org | 16

16



## FedRAMP

### Active Controls

- **Approximately 180 Active controls across 17 categories**
- **7 original controls withdrawn by NIST**
- **Controls can be process enforced, application enforced or a combination**

**Today we will look at 27 select controls against the following GxP Application Audit criteria:**

- **Data integrity and security**
- **Service Level Agreement**
- **Compliance to P11, GxP' s**
- **Validation for intended use**



Connecting

Pharmaceutical

Knowledge

ispe.org | 17

17

## Auditing GxP SaaS Application Providers

### AC-5 Least Privilege

#### Data Integrity

Least Privilege contributes to data integrity by advocating that only users executing any particular function in an application or infrastructure component are trained and of an appropriate organizational level.

#### Service Level Agreement

Cloud Administrator has limited/no access to applications.  
SLA defines security boundaries for provider and any engaged 3rd parties.

#### Compliance to P11 & GxP' s

Closest trace(s): 11.10(d), 211.68(b), 820.75(b)(2), ICH E6/E9

Associated system(s)/product(s): Any application/system with regulatory data.

#### Validation Approach

Defined user levels in Config Spec  
Access grant/modify/revoke defined  
Positive & Negative Testing  
An attempt to show 'least user' cannot exceed brief.



Connecting

Pharmaceutical

Knowledge

ispe.org | 18

18

## Auditing GxP SaaS Application Providers

### AT-1 Security Awareness

#### Data Integrity

Security awareness has broad implications for Data Integrity. While time money and resources might be spent on logical security within applications, physical security and the awareness of the infrastructure team of the type and risk of the data they are responsible for are equally important.

#### Service Level Agreement

Ensure that Cloud Provider has an active security management plan in place and is aware of the nature of the data (drug, device, patient) that they are hosting/storing.

#### Compliance to P11 & GxP's

Closest trace(s): 11.10(b), 211.68(b), 820.75(b)(2), ICH E6/9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, Medical Devices

#### Validation Approach

Data Center Qualification should include an inventory of site SOP's.  
Training Records for Staff.  
Regulated Entity to should audit to ensure active enforcement of Data Center's security policy.



Connecting

Pharmaceutical

Knowledge

ispe.org | 19

19

## Auditing GxP SaaS Application Providers

### AU-2 Auditable Events

#### Data Integrity

Ensures data integrity is verifiable via non editable audit trails & logs.  
Important to define audit events vs. auditable records.

#### Service Level Agreement

Cloud provider should detail auditable events:  
1. What is auditable by regulated entity/regulatory agency  
2. What is actively audited/monitored by provider

#### Compliance to P11 & GxP's

Closest trace(s): 11.10(e), 211.100(b), ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, Medical Devices

#### Validation Approach

Test audit trail functionality an implementation across both regulated applications and when applicable infrastructure components.



Connecting

Pharmaceutical


Knowledge

ispe.org | 20

20

**Auditing GxP SaaS Application Providers**  
 AU-3 Audit Record Content


<p><b>Data Integrity</b>          Direct correlation with P11. Consider that as designed, legacy cloud (network) components may not share all P11 audit trail expectations.</p>	<p><b>Service Level Agreement</b>          Consider a Part 11 specific statement in the SLA that outlines the audit capability of the application(s)/product(s) in scope.</p>
<p><b>Compliance to P11 &amp; GxP' s</b>          Closest trace(s): 11.10(e), 211.100(b), ICH E6/E9           Associated system(s)/product(s): ERP, QMS, EDC/RDC, Medical Devices</p>	<p><b>Validation Approach</b>          Expect to see standard audit trail testing, the 'records' related to the system in scope should have been clearly defined in the system configuration documentation</p>

 Connecting Pharmaceutical Knowledge ispe.org | 21

21

**Auditing GxP SaaS Application Providers**  
 AU-10 Non-Repudiation


<p><b>Data Integrity</b>          Arguably the highest risk control with regards to data integrity. The concept of non-repudiation, when enforced, ensures that data creation, edit, deletion is directly attributable to the individual(s) actioning the data</p>	<p><b>Service Level Agreement</b>          Ensure NDA goes beyond typical non-disclosure to address access to company data. However, most effective enforcement will be within the system</p>
<p><b>Compliance to P11 &amp; GxP' s</b>          Closest trace(s): 11.10(e), 211.68(b), ICH E6/E9           Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices</p>	<p><b>Validation Approach</b>          Extensive security testing to ensure that predicate rule records are fully accountable to the users who have interacted with them</p>

 Connecting Pharmaceutical Knowledge ispe.org | 22

22

**Auditing GxP SaaS Application Providers**  
CA-2 Security Assessments


<p><b>Data Integrity</b> In the Cloud context security assessments are a critical component of both the risk and configuration management process. It is vital to understand all of the constituent's interaction with the system in scope, both at the personnel and component level.</p>	<p><b>Service Level Agreement</b> SLA should required some level of regular security assessment at specific intervals in addition to standard intrusion detection/prevention and monitoring functionality.</p>
<p><b>Compliance to P11 &amp; GxP' s</b> Closest trace(s): 11.10(g), 211.68(b), ICH E6/E9  Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices</p>	<p><b>Validation Approach</b> Ensure documented remediation of identified security vulnerabilities from the executed assessments.</p>

 Connecting Pharmaceutical Knowledge ispe.org | 23

23

**Auditing GxP SaaS Application Providers**  
CM-2 Baseline Configuration


<p><b>Data Integrity</b> Standard Configuration Specification should expand to capture the static configuration of the cloud components comprising the system. Dynamic components should be analyzed through the prism of risk in order to benefit from the elasticity that the cloud provides.</p>	<p><b>Service Level Agreement</b> SLA should codify the change and configuration management process in order to ensure that the 'validated' state is maintained through the system life cycle.</p>
<p><b>Compliance to P11 &amp; GxP' s</b> Closest trace(s): 11.10(k), 211.68(b), 820.70(i), ICH E6/E9  Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices</p>	<p><b>Validation Approach</b> Configuration verification typically occurs at the end of the Installation Qualification phases and prior to the execution of Operational Qualification/functional testing.</p>

 Connecting Pharmaceutical Knowledge ispe.org | 24

24

**Auditing GxP SaaS Application Providers**  
 CM-7 Least Functionality


<p><b>Data Integrity</b>                  Often network appliances and software will have additional ports, protocols, and services that are not necessarily required for the system in scope. To minimize possible security impacts or data integrity issues the concept of least functionality should be applied.</p>	<p><b>Service Level Agreement</b>                  Ensure statements as to the enforcement of least functionality are included in the SLA. Would likely require audit enforcement from regulated entity.</p>
<p><b>Compliance to P11 &amp; GxP' s</b>                  Closest trace(s): 11.10(d) , 11.10(k), 211.68(b), 820.70(i), ICH E6/E9</p> <p>Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices</p>	<p><b>Validation Approach</b>                  Verify that disused port' s services and protocols are turned off or are otherwise inaccessible.</p>

 Connecting Pharmaceutical Knowledge ispe.org | 25

25

**Auditing GxP SaaS Application Providers**  
 CM-9 Config. Mgt. Plan

<p><b>Data Integrity</b>                  In order to ensure a continued compliant state of a cloud based product one would expect a configuration management plan or policy to be in place. a good framework for this the concept of 'standard' changes (ITIL) should be encouraged to ensure low risk actions are not overburdensome, but are preapproved.</p>	<p><b>Service Level Agreement</b>                  Ensure a commitment exist to manage configuration and change in an order fashion. Determine communication/approval path between cloud provider and the regulated entity.</p>
<p><b>Compliance to P11 &amp; GxP' s</b>                  Closest trace(s): 11.10(k), 211.68(b), 820.70(i), ICH E6/E9</p> <p>Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices</p>	<p><b>Validation Approach</b>                  Require examples of recently executed change/configuration controls. Ensure mechanism exists for periodic re-evaluation of validated state,</p>

 Connecting Pharmaceutical Knowledge ispe.org | 26

26

## Auditing GxP SaaS Application Providers

### CM-10 Information Systems Recovery

#### Data Integrity

Data Integrity beyond the real-time 'write' is critical both from a business and regulatory data integrity perspective.

#### Service Level Agreement

Critical component of SLA, a very clear recovery and reconstruction component should be clearly defined

#### Compliance to P11 & GxP's

Closest trace(s): 211.68(b), 820.70(i), ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

#### Validation Approach

Require Cloud provider to perform regular disaster testing in conjunction with regulated entity.



Connecting

Pharmaceutical

Knowledge

ispe.org | 27

27

## Auditing GxP SaaS Application Providers

### IA-2 Identification and Authorization (Internal)

#### Data Integrity

The system should provide a unique ID and authentication method for organization users. Challenges for single sign on.

#### Service Level Agreement

Connectivity and authentication should be defied. VPN, Lease Line, straight web connection (https)

#### Compliance to P11 & GxP's

Closest trace(s): 11.10(d), 211.68(b), 820.70(i), ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

#### Validation Approach

Standard security testing against establish configuration and company policy. Consider policy flexibility, not all SaaS applications will necessarily support the same authentication mechanisms.



Connecting

Pharmaceutical

Knowledge

ispe.org | 28

28

## Auditing GxP SaaS Application Providers

IA-3 Device ID & Auth.

### Data Integrity

Device ID and authentication is critical when a device component is introduced. Consider and authentication a device sending diagnostic information into the cloud.

### Service Level Agreement

SLA should consider logging of device authentication and connection sessions and associated logs.

### Compliance to P11 & GxP' s

Closest trace(s): 11.10(d), 211.68(b), 820.70(i), ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

### Validation Approach

Ensure only devices with proper authentication can connect. Understand impact of lost connection, partial data transfer etc.



Connecting

Pharmaceutical

Knowledge

ispe.org | 29

29

## Auditing GxP SaaS Application Providers

IR-4 Incident Handling

### Data Integrity

Key concept to maintain data integrity. The process for handling incidents is critical in the event of a data challenge such as a recall.

### Service Level Agreement

SLA should outline plan for incident handling, detection, analysis, containment eradication and recovery.

### Compliance to P11 & GxP' s

Closest trace(s): 211.100(a)(b), 820.100 ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

### Validation Approach

Incident handling process should be qualified as part of infrastructure/data center qualification.



Connecting

Pharmaceutical

Knowledge

ispe.org | 30

30

## Auditing GxP SaaS Application Providers

### IR-5 Incident Monitoring

#### Data Integrity

Key concept to maintain data integrity. The process for monitoring incidents is critical for ensuring that the compliant state of the system is maintained.

#### Service Level Agreement

SLA should outline plan for incident handling, detection, analysis, containment eradication and recovery.

#### Compliance to P11 & GxP' s

Closest trace(s): 211.100(a)(b), 820.100 ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

#### Validation Approach

Incident monitoring application(s) should be qualified as part of infrastructure/data center qualification.



Connecting

Pharmaceutical

Knowledge

ispe.org | 31

31

## Auditing GxP SaaS Application Providers

### IR-6 Incident Reporting

#### Data Integrity

Active monitoring with passive reporting should both be considered to maintain data integrity

#### Service Level Agreement

SLA needs to define clear communication channel for regulated entity to receive incident reports from the cloud provider

#### Compliance to P11 & GxP' s

Closest trace(s): 211.100(a)(b), 820.100 ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

#### Validation Approach

Verify reporting functionality of incident monitoring applications.



Connecting

Pharmaceutical

Knowledge

ispe.org | 32

32



## Auditing GxP SaaS Application Providers

MA-1 Sys Maint. Policy

### Data Integrity

Proper maintenance of the Cloud components are critical to keep system availability levels high.

### Service Level Agreement

Most Cloud providers will advertise three, four or five 9's. In other word 99.999% availability. The SLA should provide a level of availability commensurate with the systems risk. The number of 9's a data center can be correlated to the aggressiveness of the maintenance schedule.

### Compliance to P11 & GxP's

Closest trace(s): 11.10(k)(1), 211.68(a), 820.70(g)(2), ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

### Validation Approach

Awareness and Training  
Ensure system maintenance policy is reviewed as part of the qualification. For established systems example maintenance logs could be attached to the validation.



Connecting

Pharmaceutical

Knowledge

ispe.org | 33

33

## Auditing GxP SaaS Application Providers

MP-1 Media Protection Policy

### Data Integrity

Cloud provider must have policy in place to protect backup and archive media for regulated entity. Media storage, labeling and access are key regulated entities archived data considerations.

### Service Level Agreement

SLA should fully disclose the location, media type(s) and distribution of regulated entities archived data.

### Compliance to P11 & GxP's

Closest trace(s): 11.10(c), 211.68(b), 820.180, ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

### Validation Approach

Regulated entity should conduct an audit of Cloud providers media protection processes.



Connecting

Pharmaceutical

Knowledge

ispe.org | 34

34

## Auditing GxP SaaS Application Providers

### PE-2 Phys. Access Authorization

#### Data Integrity

Data Integrity could be compromised if storage location is not physically secured. Expect to see a mixture of active and passive controls. Card swipes, camera systems. etc.

#### Service Level Agreement

Access to the datacenter and associated servers and networks comprising the cloud should be outlined in the SLA.

#### Compliance to P11 & GxP's

Closest trace(s): 11.10(d), 211.28(c), ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

#### Validation Approach

Data Center qualification should include testing of physical security controls.



Connecting

Pharmaceutical

Knowledge

ispe.org | 35

35

## Auditing GxP SaaS Application Providers

### PL-2 System Security Plan

#### Data Integrity

Cloud provider may have multiple data centers, locations or cloud based products. System security planning should be holistic relative the providers business.

#### Service Level Agreement

SLA should support the concept of ongoing security assessments.

#### Compliance to P11 & GxP's

Closest trace(s): 11.10(d), ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

#### Validation Approach

Regulated entity should seek assurance via audit that security assessment(s) are cyclical within the cloud providers quality system



Connecting

Pharmaceutical


Knowledge

ispe.org | 36

36

**Auditing GxP SaaS Application Providers**  
 PS-4 Personnel Termination


<p><b>Data Integrity</b>                  The cloud provider must ensure that upon termination access privileges are revoked. They should also consider changing other security protocols depending on the terminated employees access level.</p>	<p><b>Service Level Agreement</b>                  Depending upon the risk of the engagement, the regulated entity may seek assurances, via the SLA, that terminate employee accounts have been disabled and privileges transferred.</p>
<p><b>Compliance to P11 &amp; GxP' s</b>                  Closest trace(s): 11.10(d), 211.25, ICH E6/E9                   Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices</p>	<p><b>Validation Approach</b>                  The regulated entity should verify via audit that adequate termination procedures exist at the cloud provider.</p>

 Connecting Pharmaceutical Knowledge ispe.org | 37

37

**Auditing GxP SaaS Application Providers**  
 RA-3 Risk Assessment

<p><b>Data Integrity</b>                  Traditional application Risk assessment should be expanded to cover the cloud offering being engaged. Size of data center, number of locations, advertised availability are all important factors to consider.</p>	<p><b>Service Level Agreement</b>                  A well executed SLA is typically a remedial output of a Risk Assessment.</p>
<p><b>Compliance to P11 &amp; GxP' s</b>                  Aligned with the 'Risk Based' approach advocated by FDA.</p>	<p><b>Validation Approach</b>                  Validation should include a trace to the Risk Assessment to ensure that all remedial actions have been addressed prior to 'go-live' .</p>

 Connecting Pharmaceutical Knowledge ispe.org | 38

38

## Auditing GxP SaaS Application Providers

### SA-5 IS Documentation

#### Data Integrity

Vulnerability scanners are used to by cloud providers to seek and identify weaknesses in their receptive networks.

#### Service Level Agreement

Most SLA's will outline at a high level the Cloud providers commitment to vulnerability scanning. Unlikely to specify too much detail as that in itself could create a vulnerability.

#### Compliance to P11 & GxP's

No direct trace, however could easily slot into system specific validation requirements.

#### Validation Approach

Vulnerability scanning can be a 24/7 activity, for complex architecture penetration testing is also recommended.



Connecting

Pharmaceutical

Knowledge

ispe.org | 39

39

## Auditing GxP SaaS Application Providers

### RA-5 Vulnerability Scanning

#### Data Integrity

IS documentation forms the basis of command, control and training for the information system thus having an indirect impact on data maintenance and integrity.

#### Service Level Agreement

Cloud provider should be required to maintain accurate system configuration documentation through the length of the engagement.

#### Compliance to P11 & GxP's

Closest trace(s): 11.10(k), 211.68(b), 820.50, ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

#### Validation Approach

A combination of system configuration documentation, user and administrator manuals typically the basis for an infrastructure qualification.



Connecting

Pharmaceutical


Knowledge

ispe.org | 40

40

**Auditing GxP SaaS Application Providers**  
SA-5 IS Documentation


<p><b>Data Integrity</b> IS documentation forms the basis of command, control and training for the information system thus having an indirect impact on data maintenance and integrity.</p>	<p><b>Service Level Agreement</b> Cloud provider should be required to maintain accurate system configuration documentation through the length of the engagement.</p>
<p><b>Compliance to P11 &amp; GxP' s</b> Closest trace(s): 11.10(k), 211.68(b), 820.50, ICH E6/E9  Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices</p>	<p><b>Validation Approach</b> A combination of system configuration documentation, user and administrator manuals typically the basis for an infrastructure qualification.</p>

 Connecting Pharmaceutical Knowledge ispe.org | 41

41

**Auditing GxP SaaS Application Providers**  
SA-10 Developer Cfg. Mgt.

<p><b>Data Integrity</b> Particularly important for PaaS and SaaS deliveries. In the FedRamp context also expands into the developers system development lifecycle and development environment. Typical expectations exists as to the adequacy of the code however they are further expounded by the addition of a managed hardware layer.</p>	<p><b>Service Level Agreement</b> The Cloud provider must guarantee the adherence to good programming practice as well as the maintenance of their SDLC and associated environment.</p>
<p><b>Compliance to P11 &amp; GxP' s</b> Closest trace(s): 11.10(k)(1), 211.68(b), 820.50, ICH E6/E9  Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices</p>	<p><b>Validation Approach</b> Regulated entity should confirm via audit that the provider has an established and effective SDLC program in place.</p>

 Connecting Pharmaceutical Knowledge ispe.org | 42

42

## Auditing GxP SaaS Application Providers

### SC-2 Application Partitioning

#### Data Integrity

Essential concept for virtualized applications performing regulated functions. The partitioning method must be clearly understood, defined and tested to ensure that data encroachment does not occur and that adequate resources exist for virtualized applications.

#### Service Level Agreement

SLA should provide assurance that application partition provides a sufficient border between constituents and that the hardware supporting the virtualized environment is sufficient for task.

#### Compliance to P11 & GxP' s

Closest trace(s): 11.10(k)(1), 211.68(b), 820.50, ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

#### Validation Approach

Relatively easy to verify for applications supporting Pharma. Caution should be taken for medical devices or critical clinical systems (IVRS/IWRS) with cloud component, would recommend private cloud only for this type of application.



Connecting

Pharmaceutical

Knowledge

ispe.org | 43

43

## Auditing GxP SaaS Application Providers

### SI-11 Error Handling

#### Data Integrity

Beyond IDS/IPS also consider response time, availability and uptime. Could be impactful for a system that requires timed processing steps, LIMS as an example.

#### Service Level Agreement

SLA should define the monitoring coverage, frequency, and remediation process employed by the cloud provider.

#### Compliance to P11 & GxP' s

Closest trace(s): 11.10(a)(f)(g)(h), 211.68(b), ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

#### Validation Approach

Monitoring tools should be active not passive. Consider qualifying the monitoring tools as part of the overall data center qualification.



Connecting

Pharmaceutical

Knowledge

ispe.org | 44

44

## Auditing GxP SaaS Application Providers

### SI-4 IS System Monitoring

#### Data Integrity

Error handling should be sufficient to provide both the cloud provider and the regulated entity with the ability to immediately identify and resolve system errors.

#### Service Level Agreement

Should be considered as a component of system monitoring.

#### Compliance to P11 & GxP' s

Closest trace(s): 11.10(a)(f)(g)(h), 211.68(b), 820.70(i), ICH E6/E9

Associated system(s)/product(s): ERP, QMS, EDC/RDC, CTMS, Medical Devices

#### Validation Approach

Error simulation should be conducted within reason and commensurate with the risk of the system. Error simulation should not have a long-term impact on the system.



Connecting

Pharmaceutical

Knowledge

ispe.org | 45

45

## Questions?

Please use the microphone indicated so our recording includes audio of your question

46

46

For further information, please contact

Stephen Ferrell  
at [sferrell@compliancepath.com](mailto:sferrell@compliancepath.com)

Stephen R Ferrell CISA CRISC  
Managing Director, Americas & Asia  
CompliancePath Ltd.