ISPE®

Using SaaS in a Regulated Environment – A Life Cycle Approach to Risk Management

July 2016

A Concept Paper by the ISPE GAMP Community of Practice

Acknowledgements

This Concept Paper was written and reviewed by members of the GAMP® Cloud Special Interest Group (SIG) of the ISPE GAMP® Community of Practice (COP). It represents industry best practices based on the experiences and input from the individuals listed below and does not reflect the views of any one individual or company.

SIG Chair

Kathy Gniecko	F. Hoffmann-La Roche	Switzerland

SIG Sponsor

Michael Rutherford	Eli Lilly and Company	USA

Document Authors

Ekaterina Sidorova	Novartis Pharmaceuticals	Switzerland
Phil Harrison	Formpipe Life Science	United Kingdom

Particular thanks go to the following for their support of this Concept Paper:

Chris Clark	TenTenTen Consulting Ltd.	United Kingdom
Arthur (Randy) Perez	Novartis Pharmaceuticals	USA
Sion Wyn	Conformity Ltd.	United Kingdom
Christopher White	Alexion	USA

Table of Contents

Limitation of Liability
In no event shall ISPE or any of its affiliates, or the officers, directors, employees, members, or agents of each of them, or the authors, be liable for any damages of any kind, including without limitation any special, incidental, indirect, or consequential damages, whether or not advised of the possibility of such damages, and on any theory of liability whatsoever, arising out of or in connection with the use of this information.

In two articles published in *Pharmaceutical Engineering* [1] and [2], the GAMP® Cloud SIG provided an overview of some of the primary challenges and concerns regarding whether cloud solutions can be adopted, as well as the specific challenges related to the Infrastructure as a Service (IaaS) delivery model.

The GAMP® Cloud SIG has now created three companion Concept Papers covering the topic of Software as a Service (SaaS) and Platform as a Service (PaaS):

- “SaaS in a Regulated Environment – The Impact of Multi-tenancy and Subcontracting” is focused on the SaaS cloud model description, various business models used by the SaaS providers and security and privacy concerns related to those models.

- “Using SaaS in a Regulated Environment – A Life Cycle Approach to Risk Management” (this Concept Paper), looks into the life cycle of the relationship between regulated company and SaaS provider and delves deeper into the issues a delivery team can face in their exploration of moving a business supporting system to a SaaS provider.

- “Evolution of the Cloud: A Risk-Based Perspective on Leveraging PaaS within a Regulated Life Sciences Company” is intended to help to explain how PaaS compares to other cloud solutions (specifically IaaS), as well as discussing risks and associated pragmatic controls that regulated companies should consider when leveraging PaaS within their organization.

1 Introduction

In the evolving regulated IT environment there are many things to consider when thinking of turning to the cloud for a solution. This Concept Paper describes issues and risks to consider when establishing a reliable, secure, and economically sound relationship with the SaaS provider. These risks have been divided per relationship stage with some practical process controls offered to mitigate those. While it is not universally true, SaaS providers delivering specialized support to regulatory business processes (e.g., Clinical Trails, Release Testing, AE reporting) tend to have a good understanding of the needs of regulated companies.

Using a SaaS provider can be an excellent option for regulated companies, but doing appropriate research and identifying the company’s specific support needs are critical to making the right choice of SaaS provider. Those needs/requirements should be assessed across the entire span of the relationship with the SaaS provider, rather than just meeting the immediate need of the end user.

Internal IT relationships within pharmaceutical organizations have been long established and consist of reviewing current performance and planning long term IT roadmaps to support the business. Whenever business requirements change, it is expected that an internal IT department will adjust their service offering accordingly. This internal relationship is determined by organizational structure, and guided or controlled by internal Operational Level Agreements (OLAs)/Service Level Agreements (SLAs).

In contrast, SaaS providers are likely to be serving multiple customers; therefore they may not be able to adjust their service “on demand”, e.g., introducing a new software feature for a single customer would not make much sense if others do not need it. The relationship with the SaaS provider is driven by the duration and content of the contract. Changing an internal agreement is always easier than changing an external contract and this limitation should be taken into consideration.

There are also advantages that the use of SaaS providers has over maintaining large internal IT departments. SaaS providers allow regulated companies the opportunity to select a service offering that best suits them both as users and for their budget. In addition, the use of SaaS providers also provides the ability to exit the relationship if the service is no longer needed or not adequately provided.

The regulated company should consider the beginning, middle, and end relationship before engaging the SaaS provider, in order to take full advantage of the engagement of the SaaS provider and to mitigate any accompanying shortcomings. This Concept Paper discusses risks during three phases of this relationship and has labeled these phases as the:

1. Concept Phase

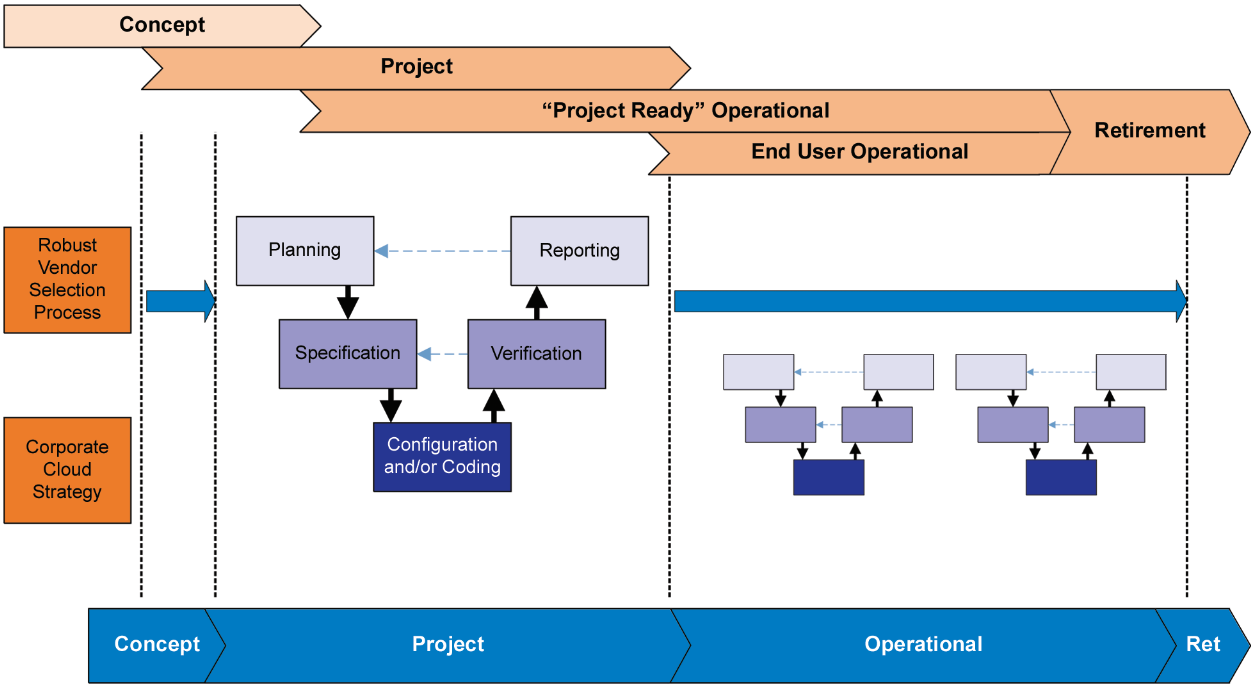
2. Operational Phase

3. Retirement Phase

2 Relationship to the GAMP® 5 Model

The GAMP® 5 phases apply to SaaS cloud applications, but need to be shifted when compared to in-house delivered and maintained systems. The shift is a result of when an application is considered "productive" versus "in production". The in-house developed application is classically referred to as "in production" when the application is deployed to the end user in support of the business process, as described by the GAMP® 5 model and reflected in blue in Figure 2.1. These applications, by virtue of being "in house" will leverage the corporate security and privacy framework through the Project and Operational phases.

Figure 2.1: GAMP® 5 Model and SaaS delivery



In addition, the GAMP® 5 Concept phase typically needs to be expanded for SaaS scenarios to ensure that a vendor selection process and a corporate strategy are established. Ideally, the cloud strategy and vendor selection processes should already exist and be leveraged by individual projects. However, if not established at a corporate level, a team will (as part of a project) need to ensure that the vendor and solution is suitable for the intended scope and application of the project. This is also the point where the Project and Operational phases of the GAMP® 5 model will likely start and overlap (see Figure 2.1).

In order to ensure that a vendor's SaaS offering will meet a business process, Proof of Concepts (POCs) or pilots are typically undertaken prior to a final vendor decision. The moment that the SaaS system is attached to a corporate network, or data is placed with the SaaS provider, the system can be thought of as operationally "project ready". Elements such as change management, security monitoring, access management, and communication of incidents at the vendor site should be established, in the same way as for an "in house" project. Once a system is "project ready", the regulated company will have to rely on the SaaS provider's security and privacy frameworks.

SaaS systems can be thought of having two transitions to an Operational phase:

- The first transition is when the system is accessible by the regulated company for purposes of POCs or configuration.
- The second transition is when the system is made available to the end user to support the business project.

2.1 Concept Phase

The activities and considerations of the Concept phase should occur prior to engaging with a SaaS provider and should be performed by a regulated company in order to enable adequate planning of delivery activities. Phases labeled as Operational and Retirement phases of the relationship describe potential risks and issues that should be considered during what would map to the traditional GAMP® 5 life cycle phases.

A company should develop a could strategy that includes the classification of business processes that also accommodates the data and potential risks to product quality and patient safety, as well as data integrity. Consideration should be given to the overall architecture of the information landscape of the regulated company's long-term integration needs. Audit and contractual needs should be established to assure control over providers and any sub-contractors, in order to facilitate necessary company and vendor interactions in subsequent phases.

It should be noted that some suppliers offering public cloud and multi-tenancy solutions may be less likely to be interested in being audited by regulated industry customers. In some senses this means the regulated company may face a "take it or leave it" attitude. If the supplier's current standard controls are not what are needed for regulated applications and data, a company may have to look elsewhere, or institute additional controls of its own. Additional controls by a regulated company may be of only limited effectiveness when considering SaaS solutions.

There should be a clear understanding of the processing and hosting landscape of the future solution to ensure that security and privacy risks are addressed.

2.2 Operational Phase

The Operational Phase commences as soon as the regulated company starts working with the SaaS solution, whether this is for release of software to the company, end-user training, or reviewing the software to potentially adjust business processes. This could involve using either test or production data, and the type of data should be detailed during the Concept phase. All the standard IT operational processes (incident, problem, change management, etc.), as well as security/data privacy processes, should be engaged as soon as the regulated company starts to put data into the software. Business continuity and disaster recovery should be possible and access rights should be actively managed. This is also the time that measurement of Key Peformance Indicators (KPIs) should begin, including:

- availability
- response and resolution time to reported incidents

The SaaS provider may perform these processes alone, or in conjunction with a third party or the regulated company, depending on the service and the offerings of the SaaS provider.

2.3 Retirement Phase

The first time to think about the end of life for a SaaS solution relationship should not be at the moment the company makes the decision to move to another SaaS provider (or bring the solution in-house), but during the Concept phase. Many issues, including those of data extraction, should be addressed during construction of the vendor agreement, not at the termination of the agreement. The data architecture should have been understood sufficiently well to know if the data can be returned to the regulated company's landscape easily or whether migration activities will need to address conversation of the data. The regulated company is responsible for the data for much longer than any likely relationship with a SaaS provider.

3 Overview of Potential Risks

Tables 3.1 through 3.3 provide a detailed overview of potential risks delivery teams may encounter when entering into a relationship with SaaS providers. The tables should be viewed as a starting point for a focused examination of specific risks with specific providers rather than an exhaustive resource. The tables also offer the readers suggestions on how likely risks may be mitigated if identified and planned for at the beginning of the relationship. Similar considerations may need to be addressed with the SaaS provider's sub-contractors, depending on the business model.

Table 3.1: Project/Concept Phase

Risks and Issues	Potential Impact	Mitigating and/or Corrective Actions
Issues Internal to the Regulated Company		
Lack of understanding of the importance of the business process and the data it contains.	Without a clear understanding of the sensitivity and relationships of the data going to a SaaS provider at the start of the contract, technical problems may surface later in the Operational phase.	Thorough architecture planning, including technical elements, data flows, master data management, future expansion, and interfaced solutions.
Lack of comprehensive strategy on what can go out to the cloud.	Can lead to selection of the wrong solution or failure to understand the risks. Potential inadvertent exposure of proprietary information and personally identifiable protected data. Highly sensitive data is out of regulated company's direct control and sensitive critical GxP processes are affected, inconsistent master data and data flows, may be difficult/costly to integrate with other solutions.	An internal company classification standard should be developed that incorporates relative data and the inherent controls that need to be met by SaaS providers for different levels of data sensitivity.
No process for selection of SaaS providers.	Potential to select a poor/unqualified SaaS provider unable to provide a service that meets security, quality and compliance requirements of the regulated company.	Requirements for the selection of a SaaS provider should be developed.
Issues Related to the Provider		
Lack of ability to integrate with other internal solutions – supporting systems (e.g., Identity Management) and transactional business systems.	SaaS solution may not be fully integrated into the internal IT landscape. The remaining integrations will need to be performed manually; such additional costs should be planned for.	During architecture planning, elements such as data flows, master data management, interfaces, and future expansion should be assessed.
No process for engaging a SaaS provider.	Potential to engage a poor/unqualified SaaS provider unable to provide a secure or quality service. Signing contracts that are detrimental to the regulated company.	Requirements for reproducible assessment of potential SaaS providers should be developed.
Regulated company carries full responsibility for actions of the SaaS provider, as well as any subcontractors used by the SaaS provider.	SaaS provider's quality system may not meet regulated company's standards. For example, the provider has neither an incident tracking system nor any informal practice of recording issues with the production system.	The regulated company should understand the criticality of the information that will be placed with a provider. Counter measures to assure continued availability and integrity of such information cannot be established with a SaaS provider that cannot demonstrate established basic IT controls such as Change Management, Incident Management, etc.

Table 3.1: Project/Concept Phase (continued)

Risks and Issues	Potential Impact	Mitigating and/or Corrective Actions
Issues Related to the Provider (continued)		
Regulated company carries full responsibility for actions of the SaaS provider, as well as any subcontractors used by the SaaS provider. (continued)	Provider's quality system may meet regulated company's standards in form, but not in substance. For example, the SaaS provider may have established a Change Management process, but the process is used only for recording major changes to the SaaS product.	Partnering with the SaaS provider can establish elements of Quality System to be augmented, as warranted by the data and business process. If the SaaS provider agrees to enhance their Quality System, contractual conditions should be established that allow for increased monitoring during the time a SaaS provider is augmenting their Quality System.
	SaaS provider's Quality System may meet a regulated company's standards in substance but not in form. For example, a company may log all installation processes on a Wiki rather than issue a comprehensive install manual.	Company standards and formality of those standards against the criticality of the information to be placed with the SaaS provider should be assessed as part of vendor selection. Where possible, compliance with standards to aid in decision process should be assessed.
Without direct contractual relationship the ability of the regulated company to audit a SaaS provider's sub-contractors and demand remediation activities is limited.	A privacy/security breach of the regulated company's data or a GxP-relevant incident may occur within a SaaS provider's sub-contractors premises.	The SaaS provider's supplier management framework should be verified as part of vendor selection, to ensure that sub-contractors (if any) are appropriately controlled. Request the results of any internal audits performed either by the company or independent audit organization (e.g., Service Organization Controls (SOCs)).
	SaaS provider's subcontractors may use a quality system that does not meet the regulated company's requirements.	The SaaS provider's supplier management framework should be verified as part of vendor selection, to ensure that sub-contractors (if any) are appropriately controlled.
The SaaS provider may use multiple datacenters; hence the physical location of regulated company data storage may not be clearly identified.	Regulated or personal data may be stored or processed outside national or continental boundaries. This could give rise to potential non-compliance with local regulations or cross-border transfer requirements.	All relevant locations used for storage, processing, backup, disaster recovery, etc., should be known at the start, defined in contracts, and cannot be changed by the SaaS provider without consent of the regulated company. Supplier Audits should address either all relevant sites, or cover the (centralized) processes that are applicable at all the specified locations, as a minimum.
	Data may be moved between locations as part of the SaaS provider's load-balancing activities, without the regulated company's knowledge or consent. The SaaS provider may introduce new locations, which are outside the scope of previous vendor audits.	The SaaS provider's controls should adequately cover multiple sites with the required level of assurance and security.

Table 3.2: Operational Phase

Risks and Issues	Potential Impact	Mitigating and/or Correcting Actions
Lack of timely reporting of issue/incident for application and infrastructure.	Support resources are not only being shared across just one organization but across many. This may not just involve problems with the application that sits on the cloud, but any part of the supporting infrastructure on which the application sits. If the application comes from a third party outside the SaaS provider, then the SaaS provider acts as a go-between, which can lead to more delays.	The response/resolution time KPIs should be established in the contract/Service Level agreement (SLA) between the regulated company and the SaaS provider, as well as between any IaaS cloud sub-provider and the software provider. Regular operational reviews should be performed.
		SaaS provider audits should be performed in order to verify end-to-end processing of incident/issues/bugs and release management.
Regulated company has no control over SaaS provider release schedule (Timing).	A SaaS provider publishes and adheres to software releases regardless of whether the regulated company has been able to assess the impact on the company's configuration or internal testing cycles.	At the regulated company, the establishment of a "governance board" consisting of IT and the business departments/representatives that will review the vendors release calendar can provide time windows to assess and plan for upcoming changes.
		A rating of changes should be established with the SaaS provider to assist the regulated company to understand the relative risk of a change and to plan for in-house regression testing when warranted.
		The regulated company can minimize the amount of regression testing needed if the regulated company can minimize any customizations made to the SaaS solution. Generally, functionality customized by the regulated company has no guarantees that it will remain functional through the life cycle of the SaaS provider's product.
		The establishment and alignment of release calendars at the regulated company can be synchronized to the SaaS provider's schedule for planned releases.
	The degree of regression testing done by the SaaS provider at time of release will likely not be known to the regulated company.	SaaS providers can develop a standard suite of regression tests that should be performed as a part of the SaaS provider's release process. Regulated companies should also plan on establishing a flow of tests that will assure that the highest risk functions or processes remain stable from throughout an entire release schedule.
Regulated company may have to accept software functionality changes that will impact business processes.	SaaS provider publishes and adheres to software releases regardless of whether the regulated company has been able to perform an assessment of any organizational impact on the business	Measures as listed above will still hold. SaaS providers should establish user groups that will guide enhancements of the base application in a way that can support the widest collection of regulated companies.

Table 3.2: Operational Phase (continued)

Risks and Issues	Potential Impact	Mitigating and/or Correcting Actions
SaaS provider's security framework may not meet the regulated company's standards.	A security breach of the regulated company's data that is under the control of the SaaS provider may occur and impact data integrity, confidentiality, and/or availability. It may have a direct (e.g., fines) or indirect (e.g., loss of reputation) impact on the regulated company.	As a part of the vendor selection, security and privacy controls applied by the SaaS provider to the regulated company's data should be verified. Contracts should include clauses covering: • Regular security measures to be performed by the SaaS provider and its sub-contractors (e.g., vulnerability scanning) • Agreement for the regulated company to perform its own security/vulnerability tests on SaaS environment
		The summary of security monitoring activities performed by the SaaS provider should be available, where possible.
		Regular audits of the SaaS provider should be performed and/or independent audit reports (e.g., SOC) should be requested to ensure continuous verification.
Security/privacy breaches are not communicated to the regulated company.	SaaS providers may fail to notify the regulated company in case of impact on integrity, availability, or confidentiality of the regulated company's data within the SaaS provider or its sub-contractors' premises. Fines for losses/violations relating to personal data fines and other regulatory penalties may apply in addition to business losses.	The breach notification process of the provider, including interfaces with sub-contractors (if any) should be verified as a part of the vendor selection. Timelines for notification and internal contact should be included in the contract.
Security policies are not communicated to the SaaS provider's associates.	SaaS provider associates' behavior may lead to the breach of regulated company data (e.g., though uncontrolled administration rights on the workstations that are used to manage the production environment, lack of general security awareness, lack of understanding of the personal data classification and its implications).	Measures taken should be verified as a part of the vendor selection. Examples of such measures include: • Minimizing the impact of the SaaS provider's associates on the regulated company's data (e.g., local administration rights control, terminal access to production environment) • Increasing the associates knowledge and awareness of the topics of security and privacy (e.g., training programs) • Ensuring consistency of Human Resources (HR) processes (e.g., background checks, leavers' checklists)
Security of the data outside of the SaaS solution but under control of the SaaS provider and/or its sub-contractors.	While the SaaS solution itself may have a robust security framework, it may not apply to the data transferred to other solutions (e.g., physical devices used for backup) within control of the SaaS provider and/or its sub-contractors.	All flows of the regulated company's data, including those of supporting processes, such as backup tapes transportation or logs' analysis, should be verified as a part of the vendor selection. Where possible contractual clauses should be considered, e.g., encryption of the backup tapes.

Table 3.2: Operational Phase (continued)

Risks and Issues	Potential Impact	Mitigating and/or Correcting Actions
Standard service levels (KPIs) for availability offered by the SaaS provider may not match regulated company expectations.	There is a risk that high-level commitments on availability may not be sufficient for the business in practice. For example, a single high-level availability of 99% may not be acceptable if it includes planned downtime periods coinciding with peak activities for the regulated company, which cannot be moved.	Contractual discussions and negotiations should go beyond stated KPIs into the correct level of detail needed for practical business operation. Overall Availability (as a percentage) can be a good starting point, but details, e.g., of the management of planned downtime, may be important to include within the contract.
The SaaS provider's standard procedures for Disaster Recovery (DR) may not meet regulated company expectations.	The SaaS provider's standard DR offering may involve different sites or different countries. Recovery Point and Recovery Time Objectives may be aligned to the needs of other clients or other industries.	Audits and contracts should include DR planning within their scope. Where standard DR is not sufficient, specific arrangements should be set up and understood by both parties.
All user rights are administrated by the SaaS provider.	Legitimate requests for access can be slow to be provisioned; delaying new users from being given access to the system or the removal of users from the system that no longer require access.	The regulated company should establish detailed metrics, including implementation time for such requests, and these should be defined in the SLA/contract.
		Where possible and desired, administration of user access should be performed within the regulated company.
SaaS provider's access rights to regulated company's data for purposes of administration of the system.	Regulated company's data or system infrastructure is exposed to personnel outside the regulated company and needs to be limited. In the event of a disaster event, access may need to be expanded.	The ability to expand and contract system access quickly and thoroughly need to be verified during audit of the business continuity/disaster recovery and operational processes of the SaaS provider.
		In the case of processing of personal data – contractual limitations or clear documentation on processing locations/data pass-through (where needed) should be established.

Table 3.3: Retirement Phase

Risks and Issues	Potential Impact	Mitigating and/or Correcting Actions
Lack of service portability between SaaS providers or between regulated company and SaaS provider.	Continuity of the business should be assured while switching the solution to another provider or bringing in-house. This may occur as a result of a SaaS provider going out of business or relationship termination for other reasons.	While this risk is listed in the retirement section, routine reviews of the service should include assessments of the time and cost to "internalize" the solution and/or data. Requirements for exiting the relationship should be included in the initial contract.
The data has to be available for the required retention period.	Space required for long term retention of inactive records may challenge the SaaS provider's infrastructure, leading the SaaS provider to change from an internally hosted to externally hosted company.	Retention requirements and data extract/storage approach should be defined, based on data processed and stored by the SaaS provider. SaaS provider should be routinely audited. Inactive records may be brought back in-house. Capacity planning should be performed at the beginning of the project and the amount of records anticipated.
	Relationship with the SaaS provider may terminate.	Contractual clauses on data retention should be established, or alternatively, on data extract and an internal archiving solution.
	Litigation cases may require long-term preservation and ability to extract records based on specific rules.	Handling of litigation cases should be planned – extract of the data and its storage while on legal hold should be prepared, either by special contract or by storing the data within the regulated company's facilities.
	Data eligible for destruction may not actually be destroyed.	The party responsible for records purging and how verification will be demonstrated should be defined.

4 References

1. ISPE GAMP® Cloud Computing SIG, "Cloud Computing in a GxP Environment: The Promise, the Reality and the Path to Clarity," *Pharmaceutical Engineering*, Jan/Feb 2014, pp. 58-62, www.pharmaceuticalengineering.org.

2. Streit, Robert and Anders Vidstrup (Members of the ISPE GAMP® Cloud Computing SIG), "Challenges for Regulated Life Sciences Companies within the IaaS Cloud," *Pharmaceutical Engineering,* Sept/Oct 2014, pp. 72-82, www.pharmaceuticalengineering.org.

5 Acronyms

DR	Disaster Recovery
GxP	Good X Practice (X can mean: Clinical, Laboratory, Manufacturing, Pharmaceutical, etc.)
HR	Human Resources
IaaS	Infrastructure as a Service
KPI	Key Performance Indicator
OLA	Operational Level Agreement
PaaS	Platform as a Service
POC	Proof of Concept
SaaS	Software as a Service
SIG	Special Interest Group
SLA	Service Level Agreement
SOC	Service Organization Control

ISPE®

600 N. Westshore Blvd., Suite 900, Tampa, Florida 33609 USA
Tel: +1-813-960-2105, Fax: +1-813-264-2816

www.ISPE.org