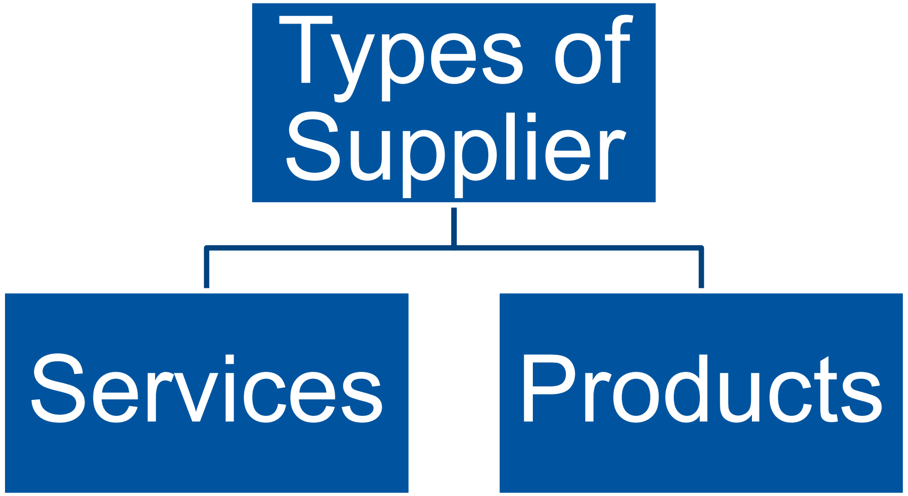
VENDOR QUALIFICATION AND QUALITY AGREEMENTS FOR CLOUD XAAS SUPPLIERS

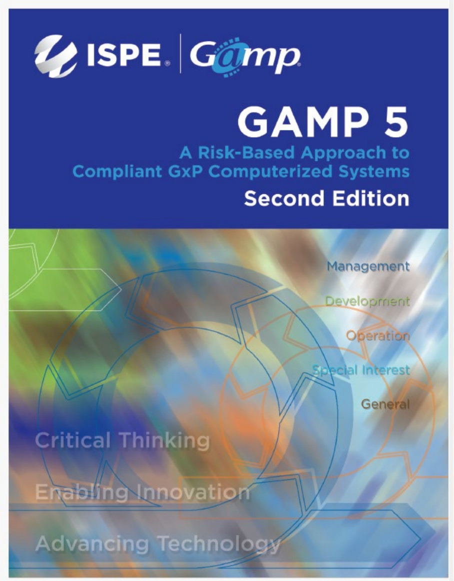
PRESENTERS:
GEETU ABBI & STEPHEN FERRELL

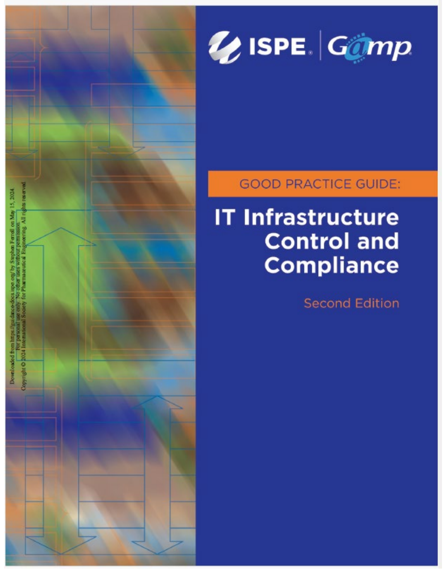
Introduction

GAMP 5© 2nd Ed., GAMP© Infra Appendix 7 on Outsourcing, and GAMP© Infra Appendix 11 on Cloud provide detailed guidance on the key steps and considerations for evaluating an XaaS provider in a regulated environment



- Chapter 7, Supplier Activities describe requirements and expectations of the regulated Company from the supplier
- Section 7.2, lists good practices that should be employed by suppliers to be compliant with regards to SDLC, QMS & security aspect.





Audit Type…

The regulated company remains **accountable** for the regulatory compliance of their operations regardless of whether they choose to outsource/offshore some or entire operational processes to external service provider(s).

Audit types

- Postal audit using a questionnaire (can also be performed via email)
- On-site audit (or virtual online audit if appropriate)

Considerations

- Before outsourcing, conduct audit to gauge provider's ability to meet regulatory and security requirements.
- Conduct periodic audits, addressing any compliance issues.
- When leveraging certifications, ensure they meet GxP requirements.
- Ensure adequate logical and physical controls at data centers

GAMP 5© 2nd Ed.,Supplier Activities & Appendix M2

Review of Supplier’s QMS

Evaluate supplier's documented QMS procedures and standards (GAMP 5© 2nd Ed., Section 7.3)

- Ensure activities are performed by trained, competent staff *(GAMP 5© 2nd Ed., Section 7.3)*
- Evaluate evidence of conformance and continuous improvement *(GAMP 5© 2nd Ed., Section 7.3)*
- QMS should align with standards like ISO 9001 but many XaaS will have an SDLC centric QMS, be open minded, look past semantics. *(GAMP 5© 2nd Ed., Section 7.3)…*

Assess Information Security Management System(ISMS)

- Supplier’s ISMS should be aligned with ISO 27001/SOC 2/ HITRUST *(GAMP© Infra Appendix 11 Cloud)*
- Covers security policies, risk management, access control, incident management, business continuity *(GAMP© Infra Appendix 11 Cloud)*
- Current ISO 27001:2022 version has additional controls for cloud security, threat intelligence, data privacy
- HITRUST CSF certification demonstrates security and privacy controls *(GAMP© Infra Appendix 11 Cloud)*

Evaluate SDLC

- Review software development lifecycle methodology
- Practices should include defined requirements, design reviews, testing, release controls
- Use of automated tools and Agile/DevOps methodologies *(GAMP 5© 2nd Ed., Section 7.3)*
- NIST SP 800-64 provides guidance for secure software development
- Ensure CI/CD schedule is understood, and provisions are made to support it

(GAMP 5© 2nd Ed., Section 7.3, 7.4-7.11)

Review Third-Party Attestations & Certifications

SOC 2 Type II

- Confirm in-place security, availability, processing integrity, confidentiality & privacy controls
- Ensure SOC 2 report covers relevant systems/processes in scope

Certifications

- ISO 27001, HITRUST, ISO 9001, ISO 27017, certifications provide assurance of ISMS
- Review results of penetration testing, vulnerability scans

(GAMP© Infra Appendix 11 Cloud)

Quality Agreement - Understand YOUR Quality & Security requirements

- Clearly specify quality, security, and compliance, requirements in Quality Agreements/ Master Services Agreement
- Align requirements with regulations like 21 CFR Part 11, Annex 11, HIPAA as applicable
- Include in contracts and service level agreements

(GAMP 5© 2nd Ed., Section 7.4, GAMP© Infra Appendix 7 Outsourcing)

Understand XaaS Quality Agreement or SLA's

Define roles and responsibilities of supplier and customer

Specify requirements and records to be maintained for demonstrating fulfillment of specified service i.e., Changes, Incidents, Deviations & CAPAs, backups, disaster recovery and business continuity and Training

Specify performance metrics, availability, support response times

Include right to audit clause and consequences of non-compliance

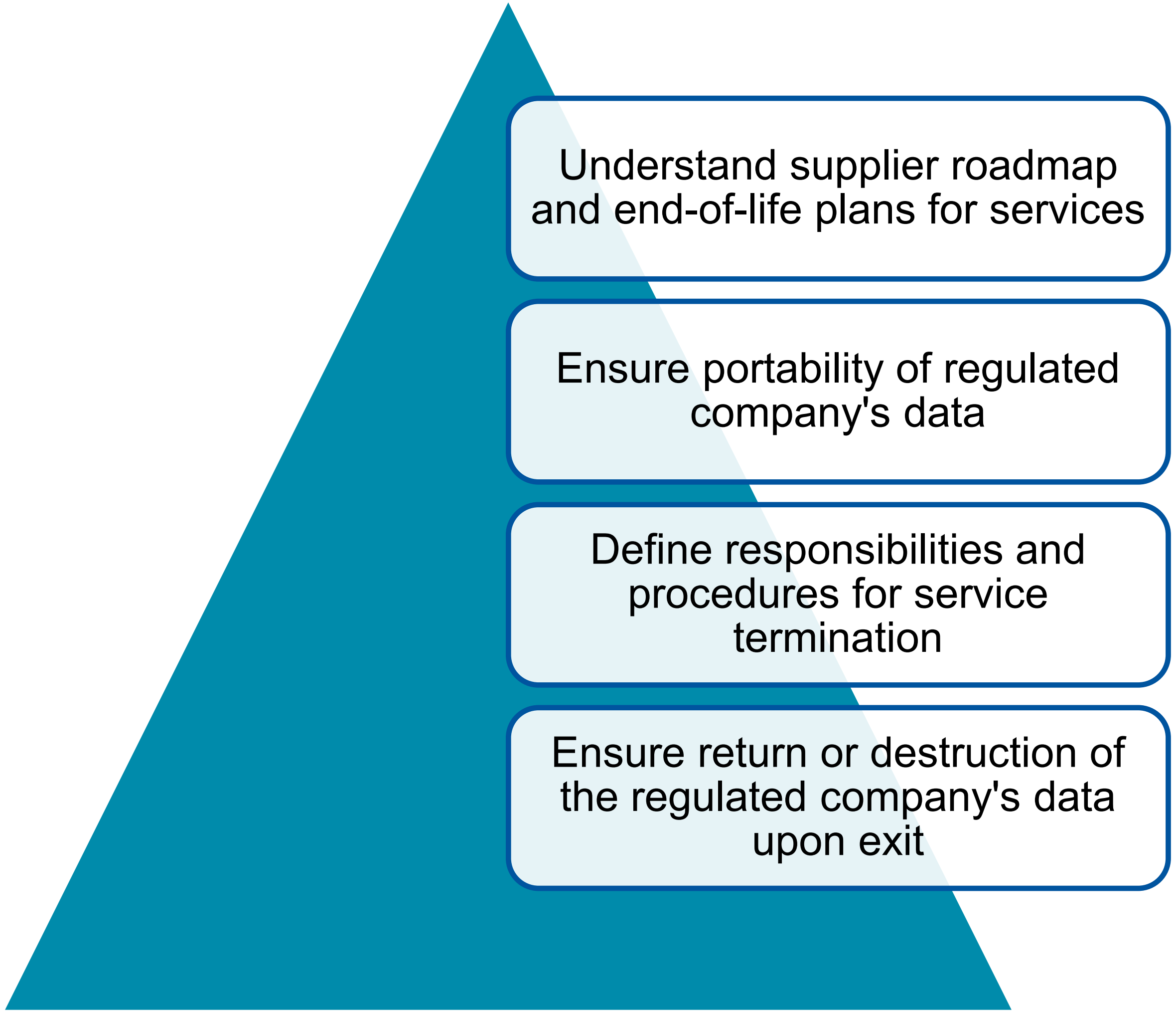
(GAMP© Infra Appendix 7 Outsourcing, GAMP© Infra Appendix 11 Cloud)

Performance & Compliance Monitoring

- ✓ Conduct periodic review of SaaS supplier
- ✓ Monitor fulfillment of SLA performance metrics
- ✓ Evaluate impact of any changes to supplier's organization, services, subcontractors
- ✓ Require notification of security incidents, material changes

(GAMP 5© 2nd Ed., Section 7.13, GAMP© Infra Appendix 7 Outsourcing, GAMP© Infra Appendix 11 Cloud)

Service Continuity & Retirement



Understand supplier roadmap and end-of-life plans for services

Ensure portability of regulated company's data

Define responsibilities and procedures for service termination

Ensure return or destruction of the regulated company's data upon exit

(GAMP 5© 2nd Ed., Section 7.14,
GAMP© Infra Appendix 11 Cloud,
GAMP© Infra Appendix 7 Outsourcing)

ISPE®

Q&A

THANK YOU!