Alternatives to Performing On-site Software Vendor Audits (Using Other Technologies) 
Points to Consider

Chris Meister¹, Vince D’Angelo², Mohammad Imran³, René Kasan⁴, Richard Siconolfi⁵, Joseph Whittemore⁶

1. Monsanto Company, St. Louis, MO, USA
2. Instem, Stone, Staffordshire, UK
3. Smithers Avanza Bioanalytical Services, LLC, Gaithersburg, MD, USA
4. NNIT Switzerland AG, Zurich, Switzerland
5. Procter & Gamble Co., Mason, OH, USA
6. Pfizer Inc., Groton, CT, USA

Introduction
The value of an on-site software vendor audit cannot be underestimated. The audit should assess controls and compliance requirements within the software vendor’s system development lifecycle. However, when an on-site software vendor audit isn’t feasible, alternative audit approaches may be considered. Under certain circumstances, a documented and justifiable risk-based approach may be considered for conducting the audit “off-site.”

Risk Assessment
A software vendor audit process should begin with a risk assessment of the computerized system to be purchased, especially in the context of the regulated business area used. For example, consider the impact of the software usage on patient or consumer safety and the product’s quality and data integrity when evaluating the level of software vendor risk. A low-risk software vendor will have little or no impact on product quality, patient or consumer safety and data integrity.

Based on the risk assessment process, the company may decide that only high-risk computerized systems will be audited on-site; while, moderate and low-risk systems will be audited using alternative methods. The risk assessment results should be documented as part of the computer system validation project indicating what audit approach was employed for the software vendor audit or why the software vendor was not audited.
Audit Approach
Establishing a routine audit schedule with a software vendor will depend on the established history between the company and the software vendor. When is it justifiable to switch from the traditional on-site audit to an alternative approach? The scenarios below describe examples of different audit approaches and their rationale in the context of risk-considerations.

1. **On-site**: Traditional, face-to-face, most thorough, best method to interview, review policies, procedures and actual practices at software vendor’s site.
   - **Rationale**: Conduct on-site audits for high-risk computerized systems. Switch to an alternative audit approach once the computerized system is stable and the previous audit has not revealed any substantial findings.
   - **Examples** of high-risk software vendors include data reporting, data archiving, system back-up, enterprise mission-critical software, and/or custom software. Other examples include clinical and health systems, and systems used in critical steps in the manufacturing or product supply process.

2. **Desktop or Virtual**: Software vendor provides requested documentation, which is reviewed remotely and may be combined with telephone and video conference reviews and interviews. Consider newer technologies such as telepresence, the use of virtual reality technology, etc.
   - **Rationale**: Conduct remote audits for moderate risk computerized systems. Switch to a questionnaire audit approach after determining that the software vendor has exhibited a strong compliance reputation in the marketplace and the previous audit has not revealed any substantial findings. Consider that the software vendor may select best examples of documentation rather than unbiased examples that may be requested during an on-site audit.
   - **Example** of medium-risk software vendors includes routine laboratory instrumentation firmware.

3. **Questionnaire**: Software vendor completes a questionnaire.
   - **Rationale**: Conduct questionnaire audits for low-risk computerized systems. A questionnaire audit is also sufficient for follow-up audits when a stable relationship with the software vendor has been established, even if considered a higher than low-risk profile. Consider that the questionnaire will be a self-assessment of the software vendor.
   - **Examples** of low-risk software vendors may include network infrastructure, simple training record administration system or document management systems only used to list documents, not to author, review or revise.

Note: Each company must have its own risk-based approach to document and determine risk levels of its computerized systems.

Frequency
Conducting periodically scheduled biennial audits is recommended to determine that software vendors are still in business, whether a software vendor has reorganized, relocated or been acquired by another company, whereby changes are made in their organizational structure that may impact their quality, operations or support. Otherwise, rather than periodically, a company may conduct an audit only if a previous audit had not been performed in the previous two years before purchasing another new system from the same software vendor.

Audit Preparation
Before conducting an on-site or remote audit, it is highly recommended to prepare a detailed audit agenda and manage expectations with the software vendor. This is beneficial to resolve any misunderstandings or differences in terminology. It may be necessary to include a glossary of terms to help clarify and define deliverables being requested. The scope, objective, and requirements for the audit should be clearly documented, defined and agreed upon prior to the audit. Review the schedule of events outlined in the agenda with the software vendor to assure there is enough time allotted to meet the scope of the inspection.

The audit agenda must identify SOPs, documents and deliverables to be inspected. Research what the company may already know about the software vendor and any documentation that may have been reviewed in previous inspection(s) to determine the scope. Ensure the auditor has access to the SOP on SOPs, and the
SOP for the software vendor’s system development lifecycle. When the software vendor has multiple sites, ensure that the audit is to be conducted at the site where key processes are performed; otherwise, ensure the site to be audited has access to the records for the processes to be inspected.

On-Site Audit
An on-site audit allows the auditor to discuss software vendor policies and procedures directly with staff members, review examples of documentation and pursue questions based on responses from those interviewed. A confidentiality agreement or non-disclosure agreement (NDA) may not be required if documents remain on-site.

Only with an on-site audit will the auditor be able to physically observe the location in order to better assess safety and security. It allows a potential visit to the data center if it is on-site. If the data center is hosted and pivotal to the on-site audit, consider adding its assessment to the audit agenda.

Desktop or Virtual Audit
Additional preparation should be considered for planning and executing a desktop or virtual audit to assure that appropriate personnel and documentation will be made available. Although the interaction is not directly face-to-face, an auditor can still use available technologies to connect and develop relationships with those being audited. The following points should be discussed when preparing and planning a desktop or virtual audit:

- **Time zone**: Depending on the location, the auditor may have a small window of time when personnel will be available.
- **Technology**: At some locations, the bandwidth and quality of network connection or video conference may be an issue. Some locations have less reliable network connections. Check if there are any expected outages around which to schedule. As the inspection is conducted, be aware that there may be technical difficulties, whereby timelines may need to be adjusted and extended.
- **Language barriers**: Determine if translation will be necessary. A video conference may be helpful to understand and follow what a person is saying when it is not his/her native language. However, audio interruptions and delays may impact the ability to interpret discussion.
- **Type of evidence capturing**: Determine how evidence will be demonstrated in electronic systems when a non-paper based review is needed. Electronic access is sometimes easier on-site while being seated next to trained personnel who are guiding the auditor through the system.

More information and data are being captured electronically these days; therefore, a large portion of the audit agenda may be completed remotely. However, a remote audit may not give the auditor the ability to tour the facility or the software vendor’s server rooms to directly discern physical security.

Ensure that the software vendor will provide the right type of information and documented evidence needed to complete the audit within the scheduled timeframe. Determine how the software vendor will provide requested documents; sending documents through email may not be secure, in which case, an alternative method should be explored. The software vendor may or may not have systems established to confidentially share documents remotely. The software vendor may require a confidentiality agreement or non-disclosure agreement (NDA) before documents are shared.

If the software vendor allows, an auditor may arrange to continue online remote access to document beyond the allotted days of the audit. Maintaining access to the documentation for a couple of weeks after the audit will allow the auditor to complete the audit report with more accurate information.

Consider that the software vendor may not be able to send information that would otherwise be accessible during an on-site audit. European data protection laws and regulations related to the transfer of data outside the EU might limit what can be sent electronically. Check that the software vendor has a security policy in place and is complying with it. The onus may actually be on the auditor having his/her own process and security policies in place to allow the exchange and transfer of information.
Questionnaire
If sending a questionnaire in lieu of an on-site or remote audit, the questionnaire may be more detailed in order to acquire information tailored for specific software system requirements. A cloud service provider questionnaire will be different than a Commercial-Off-the-Shelf computerized system or even a customized computer system questionnaire.

Prior to sending a questionnaire, the business owner should inform the software vendor of the company’s intent to validate the vendor’s software system and that the company’s computer system validation process requires a vendor assessment. This is beneficial so that the software vendor can make arrangements with the appropriate personnel to prepare and return responses within a specified timeframe.

When sending a generic questionnaire to a software vendor it can be very confusing if there are questions that are not applicable for the specific service or software being provided. The software vendor will not necessarily know that a question is not applicable and may attempt to answer it, with the resulting response being confusing for both parties (e.g., is the system capable of electronic signatures). To avoid confusion the auditor must provide a point of contact that the software vendor may contact at any time.

In addition to assessing the responses in the questionnaire, the auditor can review the software vendor’s website for information that may describe the software vendor’s history, products, and services. The auditor can also evaluate how the specific product offers necessary features in support of accomplishing regulatory compliance and the technical requirements of 21 CFR Part 11, Annex 11, and other applicable electronic record and signature requirements.

Leveraging
Requesting copies of audits, certifications or inspections conducted by other groups or agencies may be leveraged to arrange the scope of an audit or reviewed while conducting an audit; however, this must not replace the company’s due diligence in conducting it’s own audit. Here are a couple of examples of what a software vendor may provide to claim compliance, to avoid an audit:

1. Interest group audits: Official or unofficial audits conducted by a user interest group and shared amongst the members.
2. Certification/accreditation-based audits: International Organization for Standardization (ISO), Service Organization Controls (SOC) and other certifications will provide some assurances that the software vendor may have a quality management system (i.e. ISO 9001), compliance with security requirements (i.e. SOC 1, 2, 3) and/or good software engineering practices that are routinely inspected.

Conclusion
Various parameters drive the rationale and appropriateness for a selected audit approach. Which way to go is a question of choice when considering the risks and must be documented. With the digitalization of information and focus on an organization’s core business competencies, there is a need to establish the criteria and guide the right resources to the most feasible approach. The aforementioned audit approaches, when used with a documented and justifiable risk-based filter, can help today’s QA Professional develop sensible auditing techniques.

References
References are provided below with additional information for auditing software vendors and to assist with preparing questionnaires for a remote host or cloud service provider.

PI 011-3, Good Practices for Computerised Systems in Regulated “GxP” Environments (http://www.picscheme.org)

Cloud Security Alliance Consensus Assessments (https://cloudsecurityalliance.org/group/consensus-assessments)