Three things you need to know about 21 CFR part 11

Fifteen years after becoming effective, 21 CFR part 11 seems to generate as much controversy as it did when it was first implemented. At this point in time, we cannot think of another regulation that sparks as many disagreements with respect to its interpretation and generates as many discussions. Why is that?

Since the inception of the regulation as of August 1997, compliance has been, in our view, analogous to the story of Goldilocks and the Three Bears: compliance in some companies has been ***too hot*** (i.e., too restrictive and expensive); compliance in some companies has been ***too cold*** (i.e., minimal if any at all); and, compliance in some companies has been ***just right*** (i.e., cost-beneficial and based on an effective risk assessment). So, while we do not in any way want to equate compliance with the regulation to a bowl of porridge, we hereby offer three main things that you need to know about 21 CFR part 11 to help you make your compliance ***just right***:

1. <u>You need to know how to assess risks when it comes to 1) developing a validation approach regarding a given system and 2) implementing controls (e.g., audit trails, logical/physical security) to help ensure the trustworthiness and reliability of the records.</u> As indicated in the Scope and Application guidance, the FDA's "current thinking" on the subject, the agency will expect you to have a justified and documented risk assessment regarding these items. However, in order for the respective strategies and controls to be cost-beneficial in context of the potential of the system to affect product quality and safety, and record integrity, a combination of knowledge of system functionality, regulatory understanding, financial prudence and a healthy dose of common sense are required. Take one of these elements out of the equation and the resulting risk assessment will be neither practical nor useful.
2. <u>You need to know the minimum documentation that must be available to support compliance with 21 CFR part 11.</u> Irrespective of the development model employed (e.g., waterfall, Agile/Scrum), the software delivery model employed (e.g., software-as-a-product, software-as-a-service) or data hosting model employed (e.g., internal data center, outsourced hosting), as applicable, a documentation suite that truly supports compliance should encompass the following:
    - User/functional requirements, including 21 CFR part 11 requirements, to describe what the system is supposed to do;
    - Technical specifications to define how the system is built and how it works, and which is the critical component in supporting effective system maintenance (e.g., troubleshooting problems, assessing the impact of planned bug fixes and enhancements);
    - Development/validation SOPs, and evidence of compliance (e.g., required documentation, required approvals, developer-level and user acceptance testing), to define the process for developing and deploying a system that operates as intended and meets regulatory requirements;
    - Traceability between test evidence and all requirements;
    - Change control SOP and supporting change request/change control records to ensure that the system continues to operate as expected;

- Training SOP and supporting training records to support staff qualifications regarding system development, maintenance and use;
- IT infrastructure SOPs (e.g., logical/physical security, back-up and recovery, etc.) and supporting records to evidence on-going protection and availability of records.

3. You need to know that, for a given system, the quality of testing and quality of reviews are of paramount importance because they may compensate for ineffective development and/or validation SOPs. In other words, the devil (or in this case the saving angel) is in the details. Therefore, it is important that

    - Testing is complete and reflective of true system risks;
    - Test evidence is supportive of test results/conclusions and/or does not raise "red flags";
    - Reviews are timely and reasonable (e.g., only a realistic number of detailed test scripts should be reviewed in one day);
    - Incident reports are reviewed and approved by appropriate individuals promptly.

    If testing practices, testing evidence and/or testing reviews are questionable, they will constitute a serious gap from a risk-based perspective because 1) one may not be able to rely on the given system's operation, results, etc., and/or 2) data quality and integrity may be viewed as being compromised.

While there are other aspects to 21 CFR part 11 that one should know (e.g., how to determine if 21 CFR part 11 even applies to you and, if not, how to document such a conclusion), the three items discussed above represent those areas where, in our view, compliance tends to be too hot (i.e., potential business risk in that the cost of doing business may be higher than it should be) or too cold (i.e., a potential regulatory risk in that regularity requirements may not be met which, in turn, may result in business risks based on the operational impact of FDA enforcement actions).