27-Point FDA Part 11 / EU Annex 11 Self-Questionnaire

Use Cerulean's free self-assessment to help you begin to identify gaps in your Part 11 and/or Annex 11 compliance program.

Cerulean provides a formal, two-day diagnostic service for executives, business owners and due diligence teams. Clients receive a formal analysis and set of prioritized recommendations including (where information exists) estimated costs and timelines. Clients can then use Cerulean's report to close these gaps themselves or draw upon the report to issue a request for proposal (RFP) to bring in outside help. For more information on Cerulean's lean Part 11 and Annex 11 compliance services, please contact us through the Cerulean website (www.Ceruleanllc.com).

Instructions

Answer each question below to the best of your knowledge. If you are not sure, chances are you should mark "No." Do not mark "Yes" unless you have some level of documented proof (*e.g.*, training schedules, policies in hand, etc.). This is the time to be critically honest.

Please print as many hard-copies as you desire and share with your colleagues to answer.

There are 27 questions. At the end of the self-assessment is a rating scale.

#	Question	Response
1.	Do you hold annual reviews with your IT/ICT, quality, regulatory affairs and records management teams to discuss applicable regulations, rules and guidance documents as they apply to your records?	Yes No
2.	Do you have a records matrix that (at minimum) identifies key regulated record-types (such as batch files) and required retention periods?	Yes No
3.	Are the information management policies (such as retention time) consistent for both physical and digital records?	Yes No
4.	Do you provide a records integrity primer to all personnel?	Yes No
5.	Do you hold yearly training or refresher reviews on record integrity basics?	Yes No
6.	Is there a formal IT compliance policy related directly to your Quality Policy in place?	Yes No
7.	Do you have a cross-functional risk assessment program in place to identify "reasonable" risks related to your record integrity?	Yes No
8.	Do you have a cross-functional risk assessment program in place to identify "appropriate" controls on your information integrity?	Yes No
9.	Are records management policies regularly audited?	Yes No
10.	Are IT policies and system documentation regularly audited?	Yes No
11.	Have you documented the overall data flow (from creation to storage) on the network for critical G*x*P-related processes?	Yes No
12.	Do you regularly inventory and track all computerized systems?	Yes No
13.	Do you regularly inventory and track all regulated records (such as batch files, formulations, and so forth)?	Yes No
14.	Do you maintain a current listing of systems and their G*x*P-related functionality?	Yes No

#	Question	Response
15.	Do your inventories of systems and records clearly indicate which are "GxP-critical"?	Yes No
16.	Do you have controls in place to prevent any one individual – such as a computer department (IT/ICT) employee or contractor – from being able to delete or alter information without being detected?	Yes No
17.	Have any automated testing tools (such as IT might use) been reviewed by QA for appropriateness (*i.e.*, not just because an individual tester likes this or that technology)?	Yes No
18.	Have computer system and software suppliers (including any outsourced IT groups) been qualified appropriately based on risk?	Yes No
19.	Is there a documented computer system validation plan with review points for business management, IT, Quality and Regulatory Affairs?	Yes No
20.	Is there a physical-based access system (keys, badges, etc.) to get into your company offices?	Yes No
21.	Is there a computer-based access system (userID and password, biometrics, etc.) to get into your company's computers and network?	Yes No
22.	Have business continuity arrangements been documented and tested for G*x*P-critical systems?	Yes No
23.	Are there security policies and training for personnel who telecommute or travel frequently?	Yes No
24.	Have outsourced IT provider requirements (such offsite storage of data backups, software project teams, etc.) been documented in formal contracts?	Yes No
25.	Are logbooks and/or audit trails regularly reviewed of records (both hardcopy and electronic) transported to and from offsite storage?	Yes No
26.	*If you have legacy systems.* Have you maintained documented change control with risk assessments to record integrity for each system?	Yes No
27.	*If you use electronic signatures.* Do you ensure the meaning and context of the signature (*e.g.*, is it review / approval / authorization, the date and time, etc.) is always present with the signature?	Yes No

Scoring

Count the total number of questions that you answered "No" and compare to the chart below.

Note: if you outsource some of your company's G*x*P-related work to people or companies more than 4 time zones away, multiply your total "No" count by 1.15. If you are not fluent in the language spoken by your outsourced providers, multiply your total "No" count by 1.45.

# of NO's	Consequences
26 or more	***Fiasco.*** The integrity of records cannot be trusted.
19-25	***Critical risk.*** Your records integrity is easily compromised without your knowledge. Get help now.
7-18	***High risk.*** This is the range of most companies who receive FDA 483s and other compliance enforcement actions. Without significant improvement, you should not expect to pass a government or third-party audit touching upon IT compliance.
3-6	***Low-Moderate risk.*** Good work. Use the questions in this self-assessment to guide your future improvements. Consider bringing in an outside expert to conduct a workshop tailored to your needs to help define and jumpstart reasonable improvements.
2 or less	***Congratulations!*** You are on your way to best-in-class IT compliance and records integrity in the globalized economy. Take a look at our "other areas to consider" below for ideas on where to assess next for possible gaps and opportunities for improvement.

Other areas to consider: computer systems documentation, troubleshoot standards, computer system validation protocols, records management and litigation discovery policies, your vendor/supplier selection and qualification program, control of computers, proper email and internet usage audits, laboratory controls, environmental controls in IT and records management areas, financial controls, internal computer network alerts, regular computer security reviews, and so on.

Cerulean's formal diagnostic service includes a detailed set of questions and checklists that clients can retain and use for further self-improvement in the future.