A Beginner's Guide to IT System Inspection Readiness: Checklist to Prepare For IT Systems–Related Issues In Inspections

GENERAL ACTIVITIES		
It is important that all personnel have appropriate qualifications, level of access, and defined responsibilities to carry out their assigned duties (Annex 11, §2 [6]).		
Questions related to the organization at the department level	**Response**	
Is the departmental handbook/description or similar document up to date?	☐ Yes	☐ No
Are responsibilities included in job descriptions?	☐ Yes	☐ No
Is training/competency of staff and consultants documented (e.g., CVs) and up to date?	☐ Yes	☐ No
Is ownership of systems/infrastructure/tools documented? Is the information available for this for the past three years?	☐ Yes	☐ No
Is the staff list, including external/contract staff, up to date?	☐ Yes	☐ No
Has QMS content been updated according to the review schedule?	☐ Yes	☐ No
Questions about computerized systems in general	**Response**	
Are high-level presentations available?	☐ Yes	☐ No
Is it clear who will present the material?	☐ Yes	☐ No
Is the functional and purpose overview (data-flow level) in place?	☐ Yes	☐ No
Does the presentation include a validation overview?	☐ Yes	☐ No
Can (expert) users adequately perform the document walkthrough?	☐ Yes	☐ No
Questions for technician/support staff (detailed requests)	**Response**	
Are stakeholders (e.g., technicians, archive, document center, vendors) informed and ready to be available during the inspection?	☐ Yes	☐ No
Questions about general controls related to the operation and maintenance of the system	**Response**	
Is there a list of nonconformities and major incidents related to the system for the last two years?	☐ Yes	☐ No
Are challenging/complex nonconformity or major incident cases identified and explanations prepared?	☐ Yes	☐ No
IT SYSTEM ACTIVITIES		
Questions about the IT system in general	**Response**	
Are we prepared to share a high-level presentation of the system (3–6 slides), including the system life cycle (from conception to current), that covers the following?		
• Main GxP functions and users	☐ Yes	☐ No
• Validation strategy	☐ Yes	☐ No
• Dataflow	☐ Yes	☐ No
• Software structure	☐ Yes	☐ No
• Hardware structure	☐ Yes	☐ No
• Inputs/outputs of data	☐ Yes	☐ No
Questions based on overview of observations *Review any observations/findings where the actions are still in progress and prepare justifications for these not being closed.*	**Response**	
Do the validation documentation and reports cover the relevant steps of the life cycle? (Annex 11, §4.1 [6])	☐ Yes	☐ No
Is risk management applied throughout the life cycle of the computerized system, taking into account patient safety, data integrity, and product quality?	☐ Yes	☐ No
As part of a risk management system, are decisions on the extent of validation and data integrity controls based on a justified and documented risk assessment of the computerized system? (Annex 11, §1 [6])	☐ Yes	☐ No

Questions about the life-cycle approach for the system	Response	
Are the system requirements available?	☐ Yes	☐ No
Is there an up-to-date risk assessment in place for the system?	☐ Yes	☐ No
Are design specifications in place?	☐ Yes	☐ No
Does the system satisfy standards and policies (e.g., security requirements)?	☐ Yes	☐ No
Has a design review been conducted?	☐ Yes	☐ No
Is the source code in a controlled repository?	☐ Yes	☐ No
Was the code review performed?	☐ Yes	☐ No
Were module and integration tests performed?	☐ Yes	☐ No
Is evidence available to verify that the system can consistently deliver accurate and reliable results?	☐ Yes	☐ No
Is test evidence available?	☐ Yes	☐ No
Does testing cover the following, based on conducted risk assessment?		
• Backup and disaster recovery	☐ Yes	☐ No
• Prevention against loss of critical data and controlled restart after a power failure	☐ Yes	☐ No
• System access and security features	☐ Yes	☐ No
• Audit trails and logging of critical manual interactions	☐ Yes	☐ No
• Manual data entry features, input validation	☐ Yes	☐ No
• Electronic signature features	☐ Yes	☐ No
• Alarms and error messages	☐ Yes	☐ No
• Critical transactions	☐ Yes	☐ No
• Transformation of values into x-y graphs (x-y test)	☐ Yes	☐ No
• Interfaces and data transfers	☐ Yes	☐ No
• Exception handling	☐ Yes	☐ No
• Data archival and retrieval	☐ Yes	☐ No
• The ability to deal with high-volume loads	☐ Yes	☐ No
• System performance	☐ Yes	☐ No
Is the system released by QA with all approvals according to the QMS?	☐ Yes	☐ No
Questions about operation of the system	**Response**	
Does the system owner regularly evaluate the compliance status (e.g., annually)? Is the review approved by the QA person?	☐ Yes	☐ No
Is a report of periodic evaluation of users created? Is it approved by the QA person?	☐ Yes	☐ No
Is a periodic review of the audit trail performed?	☐ Yes	☐ No
Is a periodic review of user access rights performed?	☐ Yes	☐ No
Are procedures in place for granting/revoking user access to the IT system described in the SOP?	☐ Yes	☐ No
Is the access structure documented (user/user-group profiles) and approved by a quality-responsible person?	☐ Yes	☐ No
Has the system manager performed and documented surveillance of actual system access attempts?	☐ Yes	☐ No
Is full control of the system passwords established (grant, audit trail for use), and are procedures in place?	☐ Yes	☐ No
Questions about the SOP(s) related to system operation and maintenance	**Response**	
Is there a list of current operational manuals, guides, or similar documents?	☐ Yes	☐ No
Are there identified operator prerequisites, training, education, privileges? Are they documented?	☐ Yes	☐ No
Is there a log of users, major changes, problems, and any observations of the continuing safe use of the system?	☐ Yes	☐ No
Is there an SOP for system operation and maintenance?	☐ Yes	☐ No
Is there an SOP for handling changes in the system?	☐ Yes	☐ No
Is there an SOP for configuration management of the system?	☐ Yes	☐ No
Is there an SOP for system backup and recovery?	☐ Yes	☐ No
Is there a contingency, disaster, and recovery plan?	☐ Yes	☐ No