GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS

Editor: PIC/S Secretariat

web site: http://www.picscheme.org

1. Introduction:

A PIC/S working group was established in 2015 to develop guidance for inspectorates on the topic of data management and integrity. The Data Integrity Working Group (DI-WG) includes participants from over 15 PIC/S Participating Authorities, and the remit of the group is to develop harmonised guidance for inspectorates with regard to the expectations for Data Management and Integrity for GMP and GDP regulated entities.

A draft of the PIC/S guidance Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments (PI 041-1) developed by the DI-WG was published by PIC/S on a trial basis in August 2016. The guidance document was designe to facilitate a harmonised approach to data integrity elements of routine GMP inspection. Following the receipt of feedback from PIC/S Participating Authorities in February 2017, a revised document was published on 30 November 2018.

Due to widespread interest from industry following the August 2016 publication of the PIC/S draft guidance, the PIC/S Committee has agreed to engage with stakeholders with an external consultation on the updated draft guidance (version 3). This revised draft will be available for PIC/S Participating Authorities to continue to use on a further trial basis while the external consultation is held in parallel.

2. Scope and duration of the consultation:

The consultation seeks stakeholder feedback on the following questions relating to the proportionality, clarity and implementation of the guidance requirements. Any comments regarding harmonisation difficulties with other regulatory guidance are also welcomed.

Stakeholders are requested to use the structured question format to facilitate collation and assessment of responses. Where 'yes' or 'no' responses are provided, please elaborate as necessary to explain.

The draft guideline (version 3) is downloadable on the PIC/S website and has been formatted with prescribed line and page numbers.

To submit feedback, please provide feedback **exclusively on this dedicated template** which is available on the websites of the below associations and submit by e-mail with subject line "PIC/S Focused Public Consultation – Data Management and Integrity" to one of the following associations which will collect and compile responses. Stakeholders should **only reply once**.

• ECA (European Compliance Academy) Foundation:	
• IFPMA (International Federation of Pharmaceutical Manufacturers & Associations):	
• ISPE (International Society for Pharmaceutical Engineering):	
• PDA (Parenteral Drug Association):	

The consultation period will last 3 months and run from **30 November 2018** to **28 February 2019**

3. Reviewer (name, position, full contact details):

4. Questions for stakeholders:

PI 041-1 section	PI 041-1 paragraph		Question	**ISPE RESPONSE** PLEASE NOTE: This column contains the ISPE response. The response was formulated by global subject matter experts including the ISPE GAMP (Good Automated Manufactuirng Practice) technical community.
All			**Q1.** Are any sections of the guidance document unclear as to the expectations for what should be achieved?	Yes, some clarification in several sections would be helpful. Specific requests for clarification are detailed in the respective sections of this response but some typical examples are: **General obervation** - the terms GMP and / or GDP should be replaced by the more generic term GxP as DI principles and practices should be applied consistantly across all regulated areas. Section 2 - Introduction: The following modifications could improve clarity Line 104: Suggest describing "Good data management practices" in the same way as "Data Integrity" is defined in Line 111 Line 106/107: Description is close or similar to ALCOA+ principles. Suggest the addition of ".. also known as ALCOA+ principles" Section 2.5. It is recommended to move this section to directly after section 2.3 The reference to the MHRA GMP Data Integrity Definitions and Guidance for Industry is out of date. The March 2015 revision has been officially withdrawn and has been replaced by the revision issued March 2018 The term "data quality" appears in section 5.1.1 and a number of other sections. Sometimes the term is used alone and other times it is used alongside "data integrity". The term can have different meanings but is not defined in the document, and it would help to define it. Section 6.4.2 introduces the term "valid, complete and reliable", and section 3.1.2 refers to "data integrity and reliability" - use of the different terms is confusing and it would help to use common terms. In section 11.2.2 the intention of a reference to a Draft Guidance is not clear.
			Q1. continued	Additional terminology should be clearly defined and consolidated in the glossary; terms should be used consistently, in particular, but not limited to: - Section 9.3 "System security" should be completely rewritten and simplified. - Section 9.7 "Storage, archival and disposal of electronic data" should be restructured and clearly differentiate between "backup", "archival", "disposal". The terms "data transfer" and "migration" are not consistently used according to Annex 11, Items #4.8 (migration) #5 (transfer; i.e. interfaces). This remark particularly impacts on Section 9.2.2 "Data transfer between systems", item 2; since this item describes data migration, including archived data. Generally, the term "legacy system" should be replaced with "existing system"; clarification to be made in the Glossary. Generally, the terms "procedural control" and "technical control" should be preferably used and defined in the Glossary. Risk management principles should be applied for defining when and where an audit trail entry is required. As soon as audit trails are generated, they should be reviewed.

All			**Q2**. Are there any sections of the guidance that introduce unreasonable or onerous expectations?	There are many pragmatic, practical and useful strategic statements included, such as not being intended to increase regulatory burden, facilitating adoption of innovative technologies, and that risk assessments should focus on the business process, and such intentions are t be applauded. In practice, however, if some of the text in the guide is accepted literally and prescriptively, the regulatory burden may actually be significantly increased. The Guidance is sound when discussing principles of data management and data integrity. Problems arise where it suggests prescriptive detail for computerized system technical and compliance activities, primarily Section 9. Examples are detailed in the relevant responses that follow. Even if the guide represents a support for GMDP inspectors during inspection, technical expectations should be carefully mentioned since they may be inadequate within a particular context. Section 5 - Data Governance: Line 303; It should be possible to enable companies flexibility to meet data integrity requirements through automated, semi- automated or procedural controls by including reasons other than technical reasons, for example cost, schedule or complexity. Line 784: Item 1 second paragraph in Column 1: It is recommended to only list the data integrity requirements that companies should mee and to remove the recommendation to purchase or upgrade older systems. This will provide greater flexibility of approach.
All			**Q3**. Is the document format sufficiently generic to clearly apply to the range of GMP and GDP operations subject to inspection?	The guidance should better highlight the application of data integrity and data management within the scope of GDP operations. Many years after the publication of 21CFR11 and EU Annex 11, there are many examples of system/equipment suppliers who still do not provide systems capable of fully meeting or supporting e-compliance / data integrity requirements. Even with pressure from regulated user for the suppliers to support e-compliance, it would be surely useful if the regulators - in this case PIC/S - would emphasise the importance of selecting solutions (systems/equipment) capable of achieving compliance and data integrity by design. For this reason, PI-041 should strongly advocate for a better and consistent compliance awareness on supplier side.
All			**Q4.** Is any further (specific) guidance required?	Yes - there are many prescriptive approaches described in the guidance but as noted in the following responses, these may not be practical or reflective of current industry best practice and therefore a more pragmatic level of guidance may need to be considered. A specifc example is in section 9.3 - "Firewall rules should be subject to periodic reviews against specifications in order to ensure that they are set as restrictive as necessary, allowing only permitted traffic. The reviews should be documented." A Firewall would not be enough for full network security. IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) mentioned in NIST SP 800-35 would also need to be considered.
All			**Q5.** Are there any sections of the guidance that appear contradictory?	Text refers to Annex 15 in some cases, where Annex 11 would be the most appropriate reference. Generally throughout the document the term 'raw data' has been avoided with only 'data' being used. This is welcome. However, 'raw dat still appears in 5.5.3 (final bullet; line 294); 5.6.2 (second bulet, line 326); 8.10.2 (lines 647, 652 and 654); 9.6 (1; second paragraphs of both expectations and risks/items to check columns); 10.2.1 (line 817); definition of 'Data Lifecycle' (line 1047). Since 'raw data' is not defined, it is suggested that the term should be fully eliminated. The new requirements in 8.6.1 and 8.10.5 to retain the original record even after making and certifying a true copy seem to undermine the status of a true copy and even imply that a true copy cannot be trusted. The content of section 8 and section 9 should be restructured to clarify expectations: - General Good Documentation Practice - General record review expectation - Expectations to paper related record - Expectations to electronic record
Sections 3 and 4			**Q6.** Is the purpose and scope of the document clear?	Generally they are clear, however Section 3.6 should place further emphasis that good data management practices are an integral part of the "Pharmaceutical Quality System" not an "add-on" in a similar fashion to the earlier description used in section 3.4. when discussing GMP/GDP (e.g. GxP).
Section 5			**Q7.** Does the description of the 'data governance system' provide sufficient background to the requirements for achieving an enabling environment?	Yes, the description is generally adequate and clear. It makes many good points, particularly regarding use of a risk based approach. However the term "routine data verification" is not clear and should be explained by examples and information on the expectations, for example readability, reprocessability, would be helpful. Insection 5.1.1 the phases "archiving" and "decommissioning" should be described in the text and in sections 5.2.3 and 5.3.1 it should be noted that sufficient personnel resources should be provided.
Section 5			**Q8.** Are the principles of data lifecycle, data criticality and data risk clearly described?	Generally yes, but data risk is discussed in sections 5.3.4 and 5.5.1. In both it refers to "data alteration and deletion" - the risk is broader and perhaps 5.3.4 could refer instead to data which are 'complete consistent and accurate', and then 5.5.1 refer simply to "...involuntary or deliberate falsification, and the likelihood of detection of such actions"? More explanitory examples would be helpful. Some definitions are missing, e.g. data ownership, Data Goverernance and should be provided in the separate defintion section. A note should be added that the data criticality has to be specified by the company according to its GxP environment

Section 5			**Q9.** Is it clear as to how these can be applied in practice?	Some modifications could be applied to improve clarity but these are not substantive faults: Line 218: Following "criticality" add the text "and data risk throughout the data lifecycle" Line 221: Revised final sentence to "This encourages good data management practices and behaviours and reduces....." Line 229: Revise the text to "Contract Givers should perform an assessment of the Contract Acceptor's data management policies and control stragegies and establish formal agreements to cover responsibilites for ensuring data integrity ". This is a more reflective descriptio of current practice and terminology. Line 233: Add "patient safety" after "product quality". Line 254: Add another bullet for "Data Aging" Line 257: It is recommend to define term “Data criticality”, e.g. “Data of regulatory concern and the extent to which data potentially impacts patient safety, product quality and data integrity” Line 265: Revise “safety” to “patient safety” Line 270: Improve consistent phrasing by replacing the word “involuntary” with “unintentional” (as used in Line 197)
Section 5			**Q10.** Is the difference between ‘data governance system review’ and ‘data review’ clearly explained?	It is explained that they are different but it could be made more explicit, For example, by adding words to 5.6.1 to stress that the self-inspection/periodic review processes that review the data governance system to ensure that control over the data lifecycle are operating a intended are in addition to expectations for routine (critical) data reviews.
Section 5			**Q11.** Is the guidance relating to the use of quality risk management in data management and integrity sufficiently clear?	Yes, but it should be clarified whether "risk" also includes "criticality" when referring to risk-based approaches later in the document.
Section 6			**Q12.** Does the description of organisational influences help to explain the impact of management behaviour on data integrity control measures?	Yes. It would be helpful in general to explain the "intended purpose" or "intended benefit" of the particular reviews. This would allow greater understanding of the requirements with respect to implementation and to their acceptance. Suggested modification at Line 490: Add the following text "Such automation programmes should be aligned with business process / data management improvement programmes in order to avoid digitizing exisiting poor practices."
Section 6			**Q13.** Are there any concepts that are not clearly described?	No. However some suggested modifications for further clarity / consistancy: Line 379: After “regulators, customers” add “, or regulations related to privacy e.g. GDPR” Line 412: After “without consequence” add “for the informer/employee”. The performance indicators (KPIs) in section 6.5 are not clearly described. Some examples could be given.
Section 6			**Q14.** Does the guidance for dealing with data integrity issues (sections 6.7 and 12) adequately outline the expectations for and management of the risk of data integrity issues?	Yes. Suggested modification at Line 511: “product” should be revised to “patient safety and product quality”
Section 6	6.6.3		**Q15**. Is the importance of appropriately configured modern equipment/software used for management of GMP / GDP data clearly described?	Generally Yes. Section 6.6.3 refers to "appropriate" equipment/software, rather than explicitly talking about it's configuration (which is addressed more explicitly in section 9.2). Section 6.6.3 could have further explanation, to ensure it is clearer, or reference section 9.2 which contains more details. Suggested modification at Line 489: Add reference to section 7.5 or explain the abbreviation ALCOA+ as this is the first time it appears in the text
Section 6	6.6.4		**Q16.** Is the need for sufficient numbers of personnel to permit appropriate segregation of duties described in a manner relevant to large and small organisations?	Section 6.6.4 refers to qualification and training rather than the impact of staff numbers on segregation of duties. However, sections 6.6.1 and 6.6.2 cover numbers of personnel, and section 9.3 exemplifies this further, particularly for small organisations. It may be helpful to separate training and segregation of duties as separate bullets, to make it clearer.
Section 7			**Q17.** Is the explanation of general principles, including ALCOA+ requirements, clear?	Generally Yes. Section 7.5, in the description of the ALCOA+ elements, the description of" Consistent" does not seem to reflect the theme of data being self-consistent (e.g. time stamps supporting the chronology of events as described). The table should also further differentiate between paper records and electronic records (see WHO's TRS 996 Annex 5, Appendix 1).
Section 7			**Q18.** Can these principles be understood in the context of different GMP activities (e.g. quality system, production QC, warehousing, etc.) and data formats (paper or digital)?	Yes, however to enable the definitions to be understood in context it does help to exemplify them, although it is noted that sections 8 and 9 provide helpful exemplification. Suggested modification at Line 544: Revise “critical decisions” to “critical risk-based decisions” so as to be aligned with sections 5.2.2. an 5.3

Section 8			**Q19.** Are the expectations for control of paper-based records clear?	No - Further explanation required of which record types are applicable - should be differentiated between GxP-critical and non-critical records and not all requirements e.g. for reconciliation of form sheet, should apply to less critical data. Suggested modification at Line 564: Add "retirement" to list in second bullet point. Line 669: Item 1: Bullet point : “Creating pdf versions of electronic data should be discouraged”; this doesn’t align with the text in Line 648 “It is conceivable for… paper or pdf format”. Section 8.4 Table Item 1 - may also want to expand on the line "The use of temporary recording practices (e.g. use of scrap paper) should be prohibited" to include cell phones as another, modern example. In 8.4 Generation (2) the statement that 'Data should not be completed on the reverse (unused side) of existing pages...' could be read as meaning GxP documents can only used or printed single-sided. It could be made clearer that what is being flagged here is the risk of using a side not designated for use, rather than a statement that double-sided documents should not be used for GxP purposes.
			Q19 Continued	The term 'soft copy' is used in 8.4 Generation (4) which is not a commonly used term; presume this is 'electronic copy' or 'electronic file'? In 8.4 Distribution and Control (1) it might be useful to spell out why 'master copies of authorised copies should be preserved': so that it is possible to retrospecticely refer to the control document that was current at the time the work was performed. 8.12.2 (4): What is the intended meaning of 'disaster recovery' in the case of paper records? Is the disaster a situation that requires the recovery of the record from the archive, or is it the loss of the archived record?
Section 8			**Q20.** Do the requirements place an unreasonable burden on industry?	Yes. In 8.4 Distribution and Control (1) it might be useful to spell out why 'master copies of authorised copies should be preserved' so that it is possible to retrospecticely refer to the control document that was current at the time the work was performed. Controlled issuance and reconciliation should only be required for primary GxP-relevant data that directly influence product quality. Specifically, requirements in "Distribution and Control" Item 2 should be restricted to these critical records and data.
Section 8			**Q21.** Do the concepts of ‘true copy’, ‘static data’ and ‘dynamic data’ create technical difficulty in retaining data throughout the required retention period?	Yes. Section 8.10.2: Since the term "static" and "dynamic" are not sufficiently defined in the document it can only be assumed what a static record might be. A separate secton on data conversion and clarification of terms would be helpful. 8.12.2 (4): What is the intended meaning of 'disaster recovery' in the case of paper records? Is the disaster a situation that requires the recovery of the record from the archive, or is it the loss of the archived record?
Section 8	8.6.1		**Q22.** Are expectations clear in regard to recording sequential manufacturing steps at the time of operation?	The definition of contemporaneous is explicit (actions "recorded as they take place") - it may be helpful to add this in to the text in 8.6.1, Item 2? Use of text from 9.4 (2) might be useful in clarifying that the points at which paper records prompt for entry should depend on criticality - depending on the criticality, a paper batch record may require an action/check entry following each raw material addition, or it may be sufficient to have a single action/check entry to state that all raw materials have been added.
Section 8	8.10.2		**Q23.** Is the description of metadata clear?	Yes the general content of this sub-section and the subsequent sub-section 8.10.3 is good, however there is a risk of confusion as they are both discussing electronic records, and section 8.0 is about specifc DI considerations for paper records. Perhaps some added context is required for the inclusion of these sub-sections. This potential confusion is further heightened by the mixing of considerations for true copies of both paper and electronic records.
Section 8	8.10.2		**Q24.** Would examples be helpful to aid understanding?	Yes For instance: Section 8.6.1 line 618 Item 3 and section 8.12.2 line 710 Item 2: If original data are printed on thermal paper such generating a non-permanent original a verified true copy must be retained. In this case why is it requested to retain the non-permanent original as well?
Section 9			**Q25.** Are the expectations for control of electronic systems clear?	The requirements for verification of records (secondary checks) in the sub-section 8.8 on paper-based records seem lacking in 9.6 (review of data within computerised systems). This is especially noticeable with the new text in sub-section 8.8 relating to review of laboratory data when there is current industry impetus to review laboratory data such as chromatography data as original, dynamic, electronic records within the computerised system. Suggested modifications to improve clarity: Line 775: Item 1: Should “appropriate systems” be referred to as “appropriate controls”? Line 775: Item 3; Column 2: "System configuration and segregation of duties (e.g. authorisation to generate data should be separate to authorisation to verify data) should be defined prior to validation, and verified as effective during testing." In many cases the best people to verify data are the same SME's that generate it. More recent guidances are now more clearly saying that review of records (especially aud trails) should be done by people who understand the data, and peer review is a valid process. This sentence indicates that peer review should not be used. Likely not what they meant, but this is how it reads.

			Q25. Continued	Line 780: Item 1: “Systems should be able to generate a list of users with actual access to the system, including user names and roles”. Disagree with the need for "name". What is needed is something which is uniquely identifiable and linked to an individual at any given time Line 780: Item 1: “Systems should be able to generate a list of successful and unsuccessful login attempts, including: User name, User role”. Previously in same Item (page 22), user role is phrased as “user access roles”. Recommend term harmonization Line 780: Item 1: “Date and time of the attempt” add “either in local time or traceable to local time” Line 780: Item 2 - add text as follows: "Conduct periodic vulnerability scans of the IT infrastructure to identify potential security weaknesses Ensure operating systems are maintained with current security measures." Expectations on restrictions on USB devices are very detailed and prescriptive. Are these realistic and achievable? Text suggests that the audit trail should include the name of any person authorizing the change. This goes significantly further than either Part 11 or Annex 11, and is not current accepted practice.
Section 9			**Q26.** Do the requirements place an unreasonable burden on industry?	The discussion of Validation Summary Report is very prescriptive and does not reflect currentl industry good practice. This level of detail is very rarely included, or even referred to, in the VR. This information is usually maintained in other project life cycle or operational procedures, documents or tools. The Guidance prescribes specific old-fashioned IQ, OQ, PQ terminology, which has proved burdensome and is not mandatory. Annex 11 does not prescribe such terminology and approaches, and along with GAMP 5, and ASTM E2500, Annex 11 allows a more flexible approach. Furthermore, as described in GAMP 5, FAT/SAT/UAT, etc. will, if applied correctly, meet the requirements for OQ/PQ, and activities should not be duplicated unnecessarily. Any suggestion that particular activities and terminology are mandatory in all cases is unhelpful and ideally should be avoided, as also should be any suggestion that activities such as FAT/SAT must always be followed by further OQ/PQ. Section 9.2 line 775 Item 2: the inclusion of "data criticality" into the system inventory presents a new requirement which is not required by regulations (and therefroe is contradictory to the declared purpose of this document not to introduce new requirements). Line 780: Item 1: “Systems should be able to generate a list of successful and unsuccessful login attempts, including: User name, User role”. Previously in same Item (page 22), user role is phrased as “user access roles”. Recommend term harmonization
Section 9			**Q27.** Is any difficulty foreseen in applying data integrity principles for computerised systems to a range of in-use electronic systems in different GMP activities (quality system, production QC, warehousing)? - For example: Are requirements for audit trails clearly described, including their purpose and role in data verification? - Is the difference between GMP audit trails and other audit trails sufficiently explained?	Repeatedly there is the requirement that changes to data must be approved / authorized by a second person and this person also needs t be stated in the audit trail. While it is accepted that there are critical changes where a 2nd person needs to authorize the change immedately, this should not be a general requirement. Rather the decision should be based on risk the review of changes at a later stage (controlled by procedures) during regular or periodic audit trail review. Line 780: Item 1: “Date and time of the attempt” add “either in local time or traceable to local time”
Section 9			**Q28.** Is the concept of the ‘business process’ clear with respect to computerised systems, and computer system validation?	Yes.
Section 9			**Q29.** Are there technical difficulties in retaining electronic data throughout the required retention period?	Yes, there are technical difficulties in retaining electronic data throughout the required retention period. Many systems do not have a mechanism of converting data into a storable form that can be archived - meaning that if the software becomes obsolete or unsupported o an operating system the data may not be able to be read. Whilst the requirement to keep hardware/software to enable reading of data that cannot be converted to a new format seems reasonable, but can it be assured in practice, especially with R&D data which may be kept for 30 years or more? How far would we be expected to go to safeguard against possible fault in the retained hardware/software throughout the retention period? Not only the hardware, but a full back-up or full set of parts to cover any possible failure mode? The Guidance appears to confuse the topics of "backup" with "archive and retention", specifically in 9.7, table item 1. In 9.7, table item 4, the text states that it should be possible to print out a legible and meaningful record of all the data generated by a computerised system (including metadata). This is unrealistic (impossible in most cases), impractical and unnecessary, e.g. in the case of LIMS, ERP, PAT, EBR, DCS, MES, and many other systems

Section 9			**Q30.** If ‘yes’, do the technical challenges differ between legacy equipment and modern equipment?	Potentially yes, Legacy systems may not have been purchased to the standards of today, and modern, leading-edge systems may not have full functionality to enable compliance. However, as long as the original system can be virtualised, data retention does not represent a significant technical challenge for both legacy as well as "modern" equipment.
Section 9			**Q31.** Are expectations for hybrid systems clear regarding what should be achieved in practice?	Generally Yes Sections 8 and 9 describe the requirements for paper and electronic systems and, for a hybrid sytem, the relevant elements of requirements for paper and electronic apply. It would be helpful to have further guidance for these elements for hybrid systems. For example, Section 8.8C speaks to review of laboratory data, and this could reflect the review of the electronic record (if parts of record are also electronic) and source data on the equipment.
Section 9	9.2.2, table item 1 (system validation and maintenance)		**Q32.** Are the expectations for legacy computerized systems clear in terms of need for gap analysis, risk assessment and remediation plans to address good data management and integrity practices?	Yes, however it is clear that legacy systems should be evaluated, although further exemplification of the acceptable "additional controls" would be helpful.
Section 10			**Q33.** Are there any items in this section that appear ambiguous or unclear?	Generally No however some terminology is not used consistently. A supplier is not a contractor. Within the scope of PE-009, Chapter 7, the contractor executes the contract giver's process. The contract giver remains process owner and data owner of the outsourced process. A supplier owns its process and does not have to report all process relevant data to the customer. Clearly Section 10 is related to outsourcing as described in Chapter 7. Therefore "supplier" must be removed from section 10, excepted at 10.3.3 which concerns supplier as well. In the table related to 10.3.4, it should be clarified if "material testing" is related to "material testing" at supplier's site or to material receptio control at customer's site. Please include all aspects around Quality Agreements into this section instead of spreading them out throughout the document. It should be clarified to which acitivities the requirements apply as in previous sections where the statements are general. In 10.3.2 it is limited to CMOs. The need for a complete listing of data and records and assigned responsibilities is missing. The assignments should be defined througout the entire data life cycle, specifying also exit strategies in case of contract terminations and special responsibilities for root cause analyses
Section 10			**Q34.** Are there any practical restrictions/considerations relating to the review of data from contract providers that have been overlooked?	No but ensuring the alignment of Section 10 with PE-009 Chapter 7 would be helpful.
Section 12			**Q35.** Are there any elements of a data integrity remediation plan that require further explanation?	Although Section 11 differentiates degrees/classifications of deficiency, this is not consistent with the terminology used in Section 12. The retrospective evaluation states it is an evaluation of the 'nature' of the deficiencies. More guidance could be given on the retrospective evaluation of the data including how deep to look, how far back to look, etc. The section seems to be written with respect to manufacturing. It should be extended to cover all GxP regulated areas, especially GDP. Is it really reasonable to interview former employees? This makes sense for criminally relevant cases only. The definition of "significant data interity issues" is missing. Activities of companies and inspectors are mixed. Why should inspectors write policies (see 12.1.3) - isn't that the task of companies?
Section 12			**Q36.** Are the expectations for remediation sufficient?	Yes
Section 12			**Q37.** Are any expectations onerous or unrealistic?	No However the request for external forensic experts and interviews of former empoyees seems unenforcable and possibly not compliant with EU law. At least the statements should say "whenever possible" or limit the cases to significant data integrity issues.