奥星

计算机化系统的验证与风险评估

马义岭
ISPE C&Q讲师
奥星设备与工艺系统事业部 副总经理
peterma@austar.com.cn
151 0011 7027

www.austar.com.cn

目录

第一部分

中国 GMP附录 计算机化系统 解析

范围

第一条 本附录适用于在药品生产质量管理过程中应用的计算机化系统，它由一系列硬件和软件组成，以满足特定的功能。

描述了本附录的适用范围：适用于在药品生产质量管理过程中应用的计算机化系统。同时明确了系统组成“由一系列硬件和软件组成，以满足特定的功能”。按照PIC/S PI011-3指南的定义，计算机化系统（Computerized System）由计算机系统（Computer System）和被其控制的功能或流程组成。

原则

第二条 计算机化系统代替人工操作时，应当确保不对产品的质量、过程控制和其质量保证水平造成负面影响，不增加总体风险。

第三条 风险管理应当贯穿计算机化系统的生命周期全过程，应当考虑患者安全、数据完整性和产品质量。作为质量风险管理的一部分，应当根据书面的风险评估结果确定验证和数据完整性控制的程度。

主要描述了质量风险管理的要求。对于风险管理：一方面是整个生命周期要实施风险管理，自动代替人工操作不会带来负面影响及总体风险增加（必要的时候需进行工艺等同性验证来证明）；另一方面是验证的范围和程度要基于风险评估的结果来确定。

原则

第四条 企业应当针对计算机化系统供应商的管理制定操作规程。供应商提供产品或服务时（如安装、配置、集成、验证、维护、数据处理等），企业应当与供应商签订正式协议，明确双方责任。

企业应当基于风险评估的结果提供与供应商质量体系和审计信息相关的文件。

对于供应商管理：需要制定相应规程，需要有明确的协议明确供应商及制药企业双方职责，需要基于风险评估的结果实施供应商审计并形成文件化的记录。

人员

第五条计算机化系统生命周期中所涉及的各种活动，如验证、使用、维护、管理等，需要各相关的职能部门人员之间的紧密合作。应当明确所有使用和管理计算机化系统人员的职责和权限，并接受相应的使用和管理培训。

应当确保有适当的专业人员，对计算机化系统的设计、验证、安装和运行等方面进行培训和指导。

该章节强调了在系统验证、使用、维护、管理过程中各职能部门人员的紧密配合，并要求明确各自权限和职责；人员要接受相应培训以适合其岗位工作

而且对实施培训和指导工作的人员（即指培训老师）提出了要求

验证

第六条 计算机化系统验证包括应用程序的验证和基础架构的确认，其范围与程度应当基于科学的风险评估。风险评估应当充分考虑计算机化系统的使用范围和用途。应当在计算机化系统生命周期中保持其验证状态。

应用程序的验证与基础架构的确认实际上是按照软件分类的原则（可参考ISPE GAMP5软硬件分类）实施不同生命周期验证活动，其实也是采用风险管理的理念—软硬件类别不同导致其系统复杂性和新颖性带来的风险不同，从而验证的程度（或深度）不同 。

采用基于科学的风险评估来确认计算机化系统确认验证的范围和程度（比如：通过GxP关键性评估确定验证的范围，通过功能性风险评估确定验证的程度）；

确保整个生命周期内系统处于验证的受控状态（可供参考的方法是在系统运行维护阶段遵循变更和配置管理，安全管理，对系统实施定期评估等）

验证

第七条 企业应当建立包含药品生产质量管理过程中涉及的所有计算机化系统清单单，标明与药品生产质量管理相关的功能。清单应当及时更新。

制定计算机化系统的系统清单，内容包括系统名称、系统编号、系统GMP功能等内容，可以参照或者用SIA报告的形式。并及时更新。

验证

第八条 企业应当指定专人对通用的商业化计算机软件进行审核，确认其满足用户需求。

在对定制的计算机化系统进行验证时，企业应当建立相应的操作规程，确保在生命周期内评估系统的质量和性能。

需要对通用商用软件进行审核确保满足用户需求（即实施设计确认时需对通用商用软件进行确认）；需要制定针对定制系统（即5类软件系统）验证实施规程。

验证

第九条 数据转换格式或迁移时，应当确认数据的数值及含义没有改变。

在确认验证过程中，对于系统数据出现转换及迁移情况需确认数据的值及意义没有改变（举例比如：发酵罐PLC设备将罐压数据通过通讯协议转移至DCS系统，则在DCS系统的OQ检查时需要确认二者数值一致性；信号转换的I/O测试）

系统

第十条 系统应当安装在适当的位置，以防止外来因素干扰。

对安装计算机化系统的物理环境做出规定，制药企业制定URS和进行系统设计时需要考虑进去，IQ中对系统的安装位置进行确认，保证系统的安装环境是不受外来因素干扰的。

系统

第十一条 关键系统应当有详细阐述系统的文件（必要时，要有图纸），并须及时更新。此文件应当详细描述系统的工作原理、目的、安全措施和适用范围、计算机运行方式的主要特征，以及如何与其他系统和程序对接。

对关键系统的技术资料提出需求（比如功能说明、硬件设计说明、软件设计说明、电路图、网络结构图等），这些技术资料要及时更新保证和实际状态一致。

系统

第十二条 软件是计算机化系统的重要组成部分。企业应当根据风险评估的结果，对所采用软件进行分级管理（如针对软件供应商的审计），评估供应商质量保证系统，保证软件符合企业需求。

软件分级管理与供应商审计要求（同上所述，参见第四条和第六条解析）

系统

第十三条 在计算机化系统使用之前，应当对系统进行全面测试，并确认系统可以获得预期的结果。当计算机化系统替代某一人工系统时，可采用两个系统（人工和计算机化）平行运行的方式作为测试和验证内容的一部分。

针对软件的全面测试，根据软件级别的不同其测试的程度也将不同（比如：针对五类软件系统的源代码审核和模块测试，针对四类软件系统的配置测试，然后是基于黑盒的功能测试、需求测试，以及包括结合实际工艺或流程的性能测试）

EU GMP 附录11 2008年版时有“人工和计算机平行运行”要求，2011年版正式已经去掉。

系统

第十四条只有经许可的人员才能进入和使用系统。企业应当采取适当的方式杜绝未经许可的人员进入和使用系统。应当就进入和使用系统制定授权、取消以及授权变更的操作规程。必要时，应当考虑系统能记录未经许可的人员试图访问系统的行为。对于系统自身缺陷，无法实现人员控制的，必须具有书面程序，相关记录本及相关物理隔离手段，保证只有经许可的人员方能进行操作。

对系统的访问权限控制提出要求，并且要求制定规程定期检查授权的使用、变更与取消。验证时需要测试访问权限功能。值得提出来引起注意的是，CFDA也许出于国内实际国情出发，做出了硬件不足软件补的让步—“对于系统自身缺陷，无法实现人员控制的，必须具有书面程序、相关记录本及相关物理隔离手段，保证只有经许可的人员方能进行操作”。欧盟和FDA没有作出过类似表述。

大部分的企业目前不是硬性缺陷的问题，而是制定规程进行有效管理的问题。

系统

第十五条 当人工输入关键数据时，应当复核输入记录以确保其准确性。这个复核可以由另外一个操作人员完成，或采用经验证的电子方式。必要时，系统应当设置复核功能，确保数据输入的准确性和数据处理过程的正确性。

对人工输入数据的准确性提出复核的要求，复核的方式可以是另外的操作人员或者是经过验证的电子方式。（比如经过验证的称量配料系统通过报警提示能够完成“超重”、“欠重”、“批号错误”、“忘记去皮”等关键信息复核，则岗位无需配备另一名用于复核的操作人员）

(比如数据输入的有效性符合：范围和小数点位数，超出指定范围和有效位数的数据无法输入）

系统

第十六条 计算机化系统应当记录输入或确认关键数据人员的身份。只有经授权人员，方可修改已输入的数据。每次修改已输入的关键数据均应当经过批准，并应当记录更改数据的理由。应当根据风险评估的结果，考虑在计算机化系统中建立一个数据审计跟踪系统，用于记录数据的输入和修改以及系统的使用和变更。

对审计跟踪提出要求（根据“风险评估的结果来考虑”给系统加入此功能），注意“每次修改已输入的关键数据均应当经过批准，并应当记录更改数据的理由”，这里记录更改数据的理由容易被制药企业所忽视。

如果第十四条“存在硬性缺陷”，则此条其实是无法实现的。

欧盟、美国和中国的态度还是存在较大差异的。

系统

第十七条 计算机化系统的变更应当根据预定的操作规程进行，操作规程应当包括评估、验证、审核、批准和实施变更等规定。计算机化系统的变更，应经过该部分计算机化系统相关责任人员的同意，变更情况应有记录。

对计算机化系统的变更做出详细规定。制药企业应制定针对计算机化系统的变更管理规程，并按照既定的规程实施变更活动。

系统

第十八条 对于电子数据和纸质打印文稿同时存在的情况，应当有文件明确规定以电子数据为主数据还是以纸质打印文稿为主数据。

对于记录的形式（电子的、物理的或者混合的）做出说明。“应当有文件明确规定以电子数据为主数据还是以纸质打印文稿为主数据”容易被制药企业忽视。

企业采用“誊抄”纸质版的做法，并不能规避对“电子记录”的监管要求，此时纸质和电子的一致性也是检查员关注的重点，这也是数据完整的问题。

系统

第十九条 以电子数据为主数据时，应当满足以下要求：

（一）为满足质量审计的目的，存储的电子数据应当能够打印成清晰易懂的文件。

（二）必须采用物理或者电子方法保证数据的安全，以防止故意或意外的损害。日常运行维护和系统发生变更（如计算机设备或其程序）时，应当检查所存储数据的可访问性及数据完整性。

（三）应当建立数据备份与恢复的操作规程，定期对数据备份，以保护存储的数据供将来调用。备份数据应当储存在另一个单独的、安全的地点，保存时间应当至少满足本规范中关于文件、记录保存时限的要求。

对于采用电子数据作为主数据的情况，提出管理要求，包括不限于：电子数据要能打印成清晰易懂的物理文稿（即一般人可读的物理文件）；物理**或**电子的方式储存以及定期检查可读性和完整性；起草备份恢复规程按照记录的既定时限要求进行数据的备份管理等。

EU GMP Annex 11 是“和”

系统

第二十条 企业应当建立应急方案，以便系统出现损坏时启用。应急方案启用的及时性应当与需要使用该方案的紧急程度相关。例如，影响召回产品的相关信息应当能够及时获得。

第二十一条 应当建立系统出现故障或损坏时进行处理的操作规程，必要时对该操作规程的相关内容进行验证。

包括系统故障和数据错误在内的所有事故都应当被记录和评估。重大的事故应当进行彻底调查，识别其根本原因，并采取相应的纠正措施和预防措施。

对制定应急方案、制定故障处理规程、实施纠正预防措施提出要求。可参考ISPE GAMP5的附录O4“突发事件管理”和附录O10“业务连续性管理”。需在OQ中进行报警测试以及系统的挑战性测试，如断电再恢复测试、通讯中断恢复测试、灾难恢复等确认，确认系统的各种报警能够被准确记录，系统具有一定的可靠性。

系统

第二十二条 当采用计算机化系统放行产品时，应当能明示和记录放行产品人员的身份。

对采用计算机化系统进行产品放行的情形作出明确规定。这其实就是前面提及的“审计跟踪”在产品放行环节的一个特定应用而已。

对比EU GMP 附录11的第15条：当计算机化系统被用于记录认证和批放行时，系统应仅仅允许质量受权人来对该批次进行放行，同时应明确识别和记录放行批次的人。此过程应通过使用电子签名来实现。

欧盟比中国的严格

系统

第二十三条 电子数据可以采用电子签名的方式，电子签名应当遵循相应法律法规的要求。

对电子数据可采用电子签名的做法及其要求作出说明，“电子签名应当遵循相应法律法规的要求”。对于制药领域可供借鉴的相关法规，一般均采用US FDA的21CFR Part11美国联邦法规第21篇第11条款，此标准之下FDA将认为电子记录、电子签名、和在电子记录上的手签名是可信赖的、可靠的并且通常等同于纸质记录和在纸上的手写签名。

术语

（一）电子签名：是指电子数据中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

（二）电子数据：也称数据电文，是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。

（三）基础架构：为应用程序提供平台使其实现功能的一系列硬件和基础软件，如网络软件和操作系统。

（四）计算机化系统生命周期：计算机化系统从提出用户需求到终止使用的过程，包括设计、设定标准、编程、测试、安装、运行、维护等阶段。

（五）数据审计跟踪：是一系列有关计算机操作系统、应用程序及用户操作等事件的记录，用以帮助从原始数据追踪到有关的记录、报告或事件，或从记录、报告、事件追溯到原始数据。

（六）数据完整性：是指数据的准确性和可靠性，用于描述存储的所有数据值均处于客观真实的状态。

（七）应用程序：安装在既定的平台/硬件上，提供特定功能的软件。

对专用术语进行诠释。

第二部分

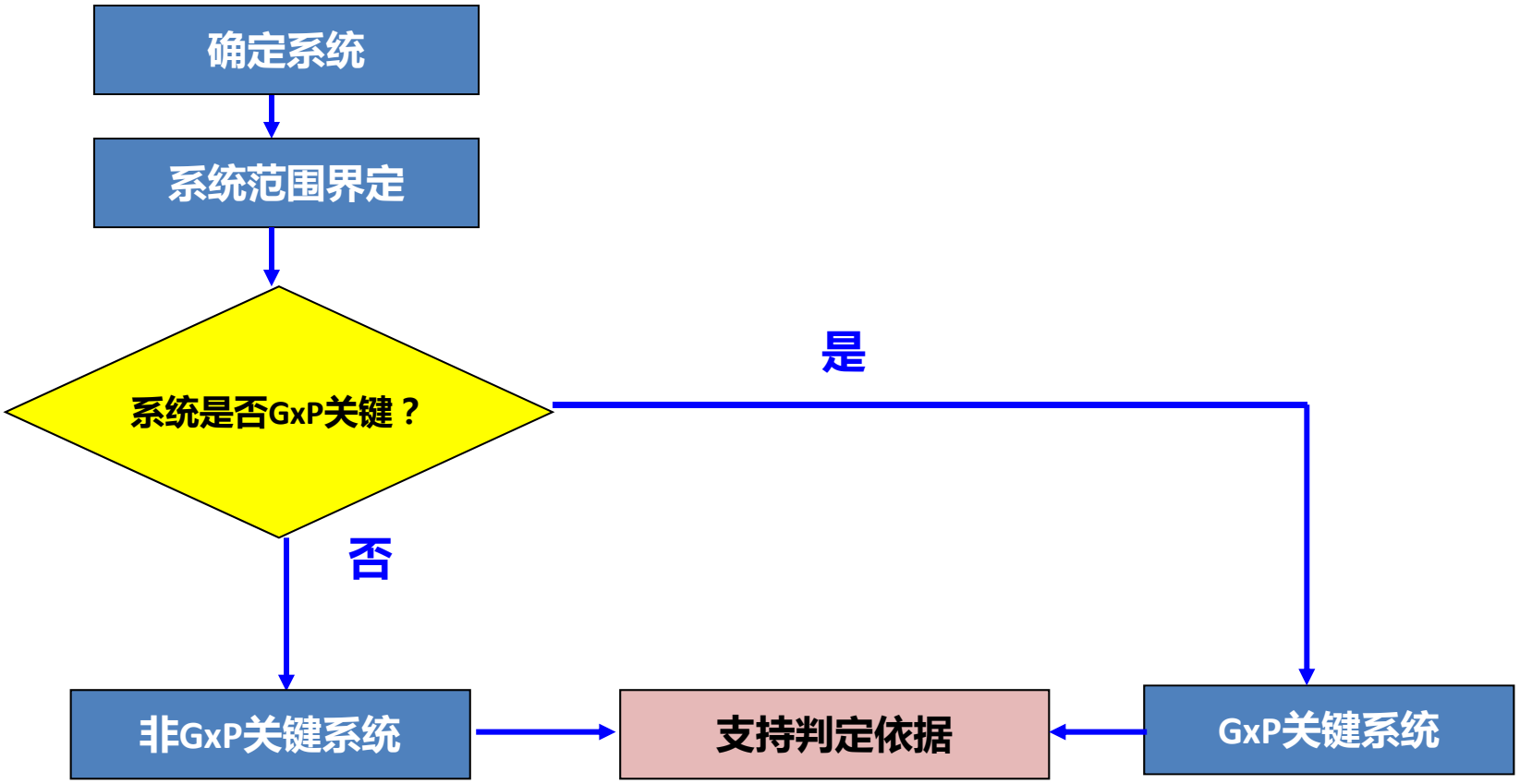
计算机化系统的风险评估

GAMP5 质量风险管理流程图

- Is it GxP?是否属于GxP
- What hazards?有什么危害？
- Impact level?影响级别？

- Probability of a failure?
- 故障可能性？
- Delectability of a failure?
- 故障可检测性？
- How risk managed?
- 风险如何控制

GxP关键性分类评估流程



GxP关键性分类评估目的及意义

GxP关键系统→GEP调试+GMP确认

如：生产DCS系统；WMS仓储管理系统；EMS环境监视系统

非GxP关键系统→ GEP调试即可

如：电梯控制系统；消防控制系统；制冷控制系统

通过GxP关键性分类评估，确定出确认验证工作的范围；将工作重点放到风险高的系统上

硬件类别

类别	说明	典型示例	典型方法
标准硬件部件	通过厂家、规格、型号、材质、序列号等技术参数直接可以通过市售渠道采购的硬件	•变频器 •PLC •显示器 •记录仪 •温度传感器	•通过文件记录下生产厂家或供应商的详情、序列号和版本号 •确认正确的安装 •适用配置管理和变更控制
定制制造的硬件部件	需要经过供应商定制设计建造的硬件部件	•网路、电路、气路 •配电柜及元器件 •传感器安装 •线缆及桥架	上述内容再加上： •设计说明 •验收测试 •适用配置和变更控制

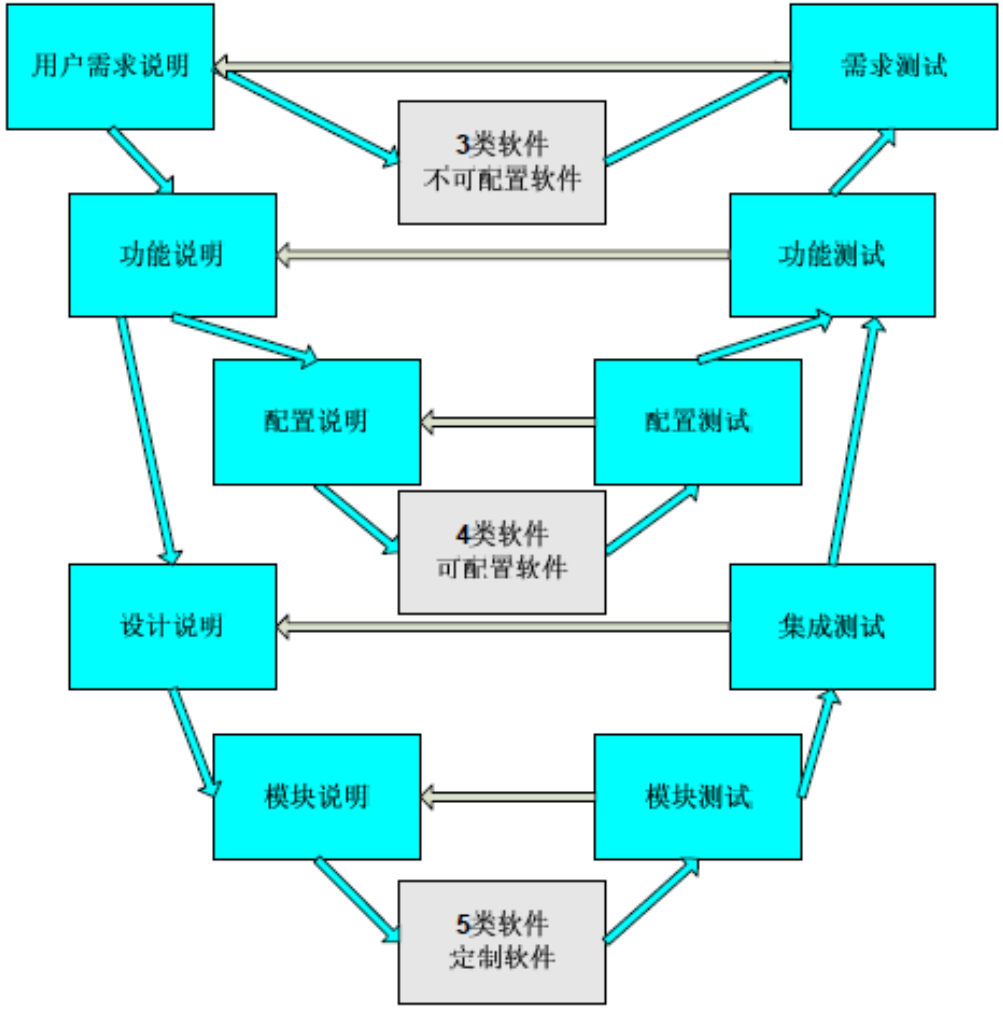
软件类别（1）

类别	说明	典型示例	典型方法
1, 基础设施软件	•分层式软件 •用于管理操作环境的软件	•操作系统 •数据库引擎 •编程语言 •电子制表软件 •版本控制工具 •网络监控工具	记录版本号，按照所批准的安装规程验证正确的安装方式。
3, 非配置软件	•可以输入并储存运行参数，但是并不能对软件进行配置以适合业务流程	•基于固件的应用程序 •COTS软件	•简化的生命周期法 •URS 用户需求说明 •基于风险的供应商评估 •记录版本号，验证正确的安装方式 •基于风险进行测试 •有用于维持系统符合性的规程

软件类别（2）

类别	说明	典型示例	典型方法
4, 可配置	这种软件通常非常复杂，可以由用户来进行配置以满足用户具体业务流程的特殊要求。这种软件的编码不能更改。	•SCADA •DCS •BMS •HMI •LIMS •ERP •Clinical trail monitoring	•生命周期法 •基于风险的供应商评估法 •供应商的质量管理系统 •记录版本号，验证正确的安装方式 •在测试环境中根据风险进行测试 •在业务流程中根据风险进行测试 •具有维持符合性的规程
5, 定制	定制设计和编码以适于业务流程的软件	•内部和外部开发的IT应用程序 •内部和外部开发的工艺控制应用程序 •定制功能逻辑 •定制固件 •电子制表软件（宏）	与第4类相同，再加上 •更严格的公用设施评估，包括可能进行供应商审计 •完整的生命周期 •设计和源代码回顾

软硬件分类与验证



通过软硬件分类评估，判定出复杂性与新颖性，从而确定出确认验证工作的程度；基于风险采取可增减的生命周期策略

Thank you!