ICS 11.020

T/CSBT

中 国 输 血 协 会 团 体 标 准

T/CSBT 003—2019

血站信息系统确认指南

Blood Establishment Computer System Validation Guideline

2019-04-12 发布　　2019-04-12 实施

中 国 输 血 协 会 发 布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件发布机构不承担识别这些专利的责任。

本标准由中国输血协会血液质量专业委员会提出。

本标准起草单位：上海市血液中心、上海市血液管理办公室、江苏省血液中心、浙江省血液中心。

本标准主要起草人：邹峥嵘、叶小凡、高瑜、张统宇、孔长虹、周春、方漪、靳晓倩。

血站信息系统确认指南

1 范围

本标准规定了血站信息系统确认的要求。

本标准适用于血站信息系统终端用户对血站信息系统的确认。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 19000 质量管理体系 基础和术语

GB/T 11457 信息技术 软件工程术语

GB/T 9385 计算机软件需求规格说明规范

GB/T 32423 系统与软件工程 验证与确认

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 20988 信息安全技术 信息系统灾难恢复规范

GB/T 19025 质量管理 培训指南

3 术语和定义

GB/T 19000和GB/T 11457确立的以及下列术语和定义适用于本标准。

3.1 血站信息系统（Blood Establishment Computer System）

对血站业务流程实施计算机管理的信息系统，包括计算机硬件、软件、外围设备、网络、人员和文档（如用户手册和标准操作程序）。

3.2 血站信息系统确认（Validation of Blood Establishment Computer System）

对血站信息系统中的特定内容进行检查和提供客观证据，以证实特定需求已得到满足的认定。

4 基本要求

4.1 总体要求

确保血站信息系统的可用性、安全性、稳定性和可靠性。

4.2 人员职责

确认小组组织和实施确认。测试和评估工作可委托有资质的第三方机构实施。

确认小组由血站的管理人员、业务人员、信息技术人员以及产品或服务的供方人员组成，由血站分管信息负责人担任组长。

4.3 文档管理要求

4.3.1 管理要求

应建立、实施文档管理程序，记录并保存确认过程所产生的结果和数据，使其具有可追溯性，以证实确认状态有效。

4.3.2 文档内容

文档必须完整，应至少包括用户需求说明书、风险评估报告、确认方案、测试和评估报告、确认报告。

4.3.3 文档保存要求

文档保存期限应符合国家相关规定，涉及血液采集、血液检测、血液隔离与放行、血液保存发放的确认文档应至少保存十年。文档应安全保管和保存，防止篡改、丢失、老化、损坏、非授权接触、非法复制。应对文档进行分类管理，并建立检索系统。

5 实施流程

5.1 流程的划分

血站信息系统确认流程包括需求确认、开发验证、变更确认、发布管理、跟踪评价五个部分。确认流程图参见附录E。

5.2 需求确认

5.2.1 需求说明书要求

血站信息系统用户需求说明书应由业务部门提出，以书面形式提交。应详尽说明需求的真实意图，相关图片、表格应作为附件提交。用户需求说明书编制应参考GB/T 9385。

5.2.2 风险评估内容

信息管理部门对用户需求进行风险评估，编制风险评估报告。风险评估报告应包括风险评估汇总表、深度等级表、广度等级表、频度等级表、关键因素加权值表和风险等级表。血站信息系统风险评估方法参见附录A。信息管理部门主管依据评估结果提出建议。

5.2.3 评估结果审核要求

由业务部门主管对风险评估报告进行审核。当风险评估等级为中、高风险，应由血站分管负责人最终审核。

5.2.4 需求确认结果

信息管理部门依据通过评审的用户需求说明书立项开发。

5.3 开发验证

5.3.1 开发验证内容

开发验证包括供方选择、系统验证、文档编制（含版本说明书、用户手册）。

5.3.2 开发验证要求

自行开发或外部供方提供的信息系统在开发过程中应参考GB/T 32423实施系统与软件工程的验证和确认。交付血站终端用户时，应提交版本说明书和用户手册。如用户需求中存在压力测试要求的，应提交压力测试报告。

5.4 变更确认

5.4.1 变更确认流程

变更确认的流程包含变更确认准备、编制确认方案、实施确认方案、编制和审核确认报告五个部分。

5.4.2 变更确认准备

对变更确认所需资料进行汇总，应包括通过评审的用户需求说明书、风险评估报告、版本说明书、用户手册等。

5.4.3 编制确认方案

确认方案宜包含安装鉴定（IQ，又称安装确认）计划、操作鉴定（OQ，又称操作确认）计划、性能鉴定（PQ，又称性能确认）计划、业务持续性评估计划、信息安全风险评估计划、培训内容评估计划。参见附录B。确认方案应由确认小组组长批准。所有操作人员在开展确认活动前应进行确认方案的培训。

5.4.4 实施确认方案

信息系统开发完成后，应根据确认方案进行确认。 测试时间不少于5个工作日，包含安装鉴定、操作鉴定和性能鉴定。测试和评估报告应包括测评项目检查表、偏离报告、测评结论，以及相关支持文档。确认测试和评估报告参见附录D。

5.4.5 编制确认报告

确认报告宜包含安装鉴定报告、操作鉴定报告、性能鉴定报告、培训内容评估报告、业务持续性评估报告及信息安全风险评估报告。参见附录C。

5.4.6 审核确认报告

确认报告由确认小组组长审核和签发。确认小组组长应审核确认方案规定的各项内容的符合性，并审核报告的完整性、正确性、规范性。确认结论分为通过、有条件通过或不通过。确认结论为不通过或有条件通过时，应记录理由并提出解决方案。对于风险等级为高的需求，在测评过程中出现偏差的，应终止确认过程；对于风险等级为中的需求，在测评过程中出现偏差的，应采取额外措施，以降低风险。

5.5 发布管理

5.5.1 用户培训要求

信息管理部门应发放用户手册，组织用户培训。培训完成后应评价胜任程度及保存用户培训反馈表。

5.5.2 发布要求

发布前，信息管理部门应编制并向相关用户通报发布计划。发布计划应包含应急回退计划。

发布完成后，信息管理部门应编制发布报告。

5.6 跟踪评价

5.6.1 跟踪评价要求

发布完成后，业务部门应及时反馈使用中出现的情况。信息管理部门负责追踪业务部门的反馈。

发布完成后，信息管理部门宜在6周至6个月的时间段内组织业务部门对变更内容进行实施后的评价。

5.6.2 跟踪评价结果

在跟踪评价过程中，对于高风险项出现偏差的，信息管理部门应对用户需求重新确认。

附　录　A
（资料性附录）
血站信息系统风险评估方法

风险评估贯穿血站信息系统生命周期的各阶段。在建设验收阶段，通过风险评估以确定信息系统的安全目标是否达成。在运行维护阶段，应针对变更进行风险评估，以识别系统变更造成的风险。

血站信息系统风险评估的目的是鉴别需求和需求实施衍生出的风险，并在后续工作中进行风险控制。血站应遵循风险识别、风险分析和风险评估结果判定三个步骤进行风险评估。

A.1　风险识别

风险识别阶段的任务是将需求中潜在的风险查找出来。风险评估人员首先应将用户需求说明书分解为独立需求项，然后逐项分析可能存在的潜在风险，完成风险评估汇总表的用户需求单元和风险识别单元。风险评估汇总表的风险识别单元中应注明风险的来源、产生条件及其特征。表A.1提供了一种风险评估汇总表的参考。

表 A.1　风险评估汇总表

用户需求单元		风险识别单元					风险分析单元					结果判定
需求编号	内容	风险编号	风险项说明	风险来源	产生条件	风险特征	深度	广度	频度	评估理由	风险评估指数	风险等级

A.2　风险分析

风险分析的关键因素包括风险造成后果的深度、广度和频度。风险分析阶段的任务是按风险后果的深度、广度和频度，对识别出的风险逐项分析，以便采取控制措施。

在血站信息系统确认过程中，采用风险分析指数法进行定性风险估算。风险分析指数法依据风险后果的深度、广度和频度，按其特点分级。风险评估人员依据血站自身特点对三种关键因素赋以一定的加权值，定性地衡量三种关键因素的关系。对风险评估汇总表进行逐项评估后，依据风险分析指数换算公式计算风险分析指数，完成风险评估汇总表的风险分析单元。风险分析单元中应注明风险分析的评估依据。

A.2.1 编制风险评估关键因素等级表

由风险评估人员依据血站自身特点，分别依据深度、广度和频度划分等级，编制风险分析关键因素等级表。对于已采取控制措施的风险，可降低其风险等级。

A.2.1.1 编制风险分析深度等级表

血站信息系统中，风险深度一般指风险的严重程度。严重风险，可能产生灾难的后果，包括造成献血者或用血者人身伤害、产生公共社会安全事件、破坏血站质量目标完成。表A.2提供了一种深度等级表的参考。

表 A.2 深度等级表

分值	等级说明	影响程度
5	灾难	可能导致血液安全事件和人身伤害，对血站质量目标的实现产生灾难影响。
3	严重	可能造成血液浪费，对血站质量目标的实现产生严重影响。
1	轻度	可能造成经济损失，对血站质量目标的实现产生轻度影响。
0	轻微	对血站质量目标的实现产生轻微影响。

A.2.1.2 编制风险分析广度等级表

风险广度一般指风险造成损害波及的范围，即风险发生后，受影响的血站业务部门。关键业务部门至少包括涉及血液采集、血液检测、血液隔离与放行和血液保存发放与运输流程的血站业务部门。表A.3提供了一种广度等级表的参考。

表 A.3 广度等级表

分值	等级说明	影响程度
5	灾难	影响整个血站业务部门
3	严重	影响一个（含一个）以上关键业务部门
1	轻度	影响一个（含一个）以上非关键业务部门
0	轻微	业务部门日常工作几乎没有影响

A.2.1.3 编制风险分析频度等级表

风险频度指风险发生的频率。表A.4提供了一种频度等级表的参考。

表 A.4 频度等级表

分值	等级说明	发生情况
5	频繁	频繁发生
3	有时	有时发生
1	极少	不易发生，但有可能发生
0	不可能	很不容易发生

A.2.2 设定关键因素的加权值

风险评估人员依据血站自身特点对三种关键因素赋以一定的加权值，定性地衡量三种关键因素的关系。三种关键因素权值合计为1。表A.5提供了一种关键因素加权值表的参考。

表 A.5　关键因素加权值表

关键因素	加权值
深度	0.4
广度	0.3
频度	0.3
合计	1

A.2.3　编制风险分析指数换算公式

根据设定的关键因素加权值，完成风险评估指数换算公式。

风险评估指数 = 深度分值×深度加权值 + 广度分值×广度加权值 + 频度分值×频度加权值

A.2.4　逐项进行风险分析，完成风险评估汇总表的风险分析单元

对各风险项进行关键因素评估，并依据风险评估指数换算公式计算风险评估指数。

A.3　风险评估结果判定

风险评估汇总表是制定确认方案以及审核确认报告的依据。

A.3.1　设定风险等级的风险评估指数范围

全面审查风险评估汇总表，依据血站自身特点，设定风险等级对应的风险评估指数范围。表A.6提供了一种风险等级表的参考。

表 A.6　风险等级表

风险等级	风险评估结果	风险评估指数范围
高	不可接受风险	3.1-5.0
中	不希望有的风险	1.1-3.0
低	可接受的风险	0-1.0

A.3.2　完成风险评估汇总表的结果判定单元

依据风险等级表填写风险评估汇总表的风险等级项，最终完成风险评估汇总表。

附 录 B
（资料性附录）
血站信息系统测试和评估办法

B.1 血站信息系统的测试

B.1.1 安装鉴定（IQ，又称安装确认）

在新建系统或系统大规模调整时，依据供方提供的系统安装相关资料，对系统安装和配置进行鉴定，以证明系统被正确安装和配置。在安装鉴定中需要来自供方的支持。

安装鉴定工作应按以下步骤进行：

a)制订安装鉴定方案；

b)搜集与系统安装有关的资料；

c)鉴定系统安装情况与资料无差异；

d)对于软件的安装鉴定，在完成安装配置后，应冻结所有配置和软件代码，测试血站信息系统是否能够运行，以鉴定软件配置是否正确；

e)对于硬件的安装鉴定，在完成安装配置和初始化配置后，应冻结所有配置，测试血站信息系统是否能够运行，相应的安全措施是否得到落实；

f)编写安装鉴定报告。

安装鉴定报告应包括以下文件：

a)测试方案；

b)安装鉴定结论；

c)安装条件和环境条件记录；

d)交付清单；

e)资料文档和软件备份；

f)安全性措施（供电、备份、环境、安全控制措施）。

B.1.2 操作鉴定（OQ，又称操作确认）

在完成安装鉴定的基础上，应依据用户需求说明书要求，对系统功能进行测试，以证明系统功能符合用户需求。操作鉴定应进行压力测试，以证明极限状态能够满足用户需求。

操作鉴定应按以下步骤进行：

a)依据用户需求说明书，编制项目检查表，完成测试方案；

b)依据测试方案，对鉴定项目检查表内容逐项进行测试，对测试中出现的偏差，记录在测试偏移表中；

c)评估测试结果；

d)编写操作鉴定报告。

操作鉴定报告应包括以下文件：

a)测试方案；

b)系统预设参数配置说明；

c)功能测试记录；

d)特定功能的压力测试报告；

e)操作鉴定结论。

B.1.3 性能鉴定（PQ，又称性能确认）

在完成操作鉴定的基础上，应依据用户需求，通过相对较长时间的模拟运行，以证明系统在正常操作条件下能稳定可靠地工作。性能测试应考虑系统切换后，历史数据的使用和整合。

性能鉴定应按以下步骤进行：

a)依据用户需求，设计用户测试方案；

b)对参与测试的人员进行培训；

c)依据测试方案，进行模拟运行；

d)评估测试结果；

e)编写测试报告。

性能鉴定报告应包含以下文件：

a)性能鉴定方案；

b)模拟运行测试报告；

c)性能鉴定结论。

B.2 血站信息系统的评估

B.2.1 业务持续性评估

建立业务持续性计划的作用在于确保血站的主要业务和血站信息系统服务能够长期稳定运行。应对新建或业务流程变更带来的风险进行评估，并制定相应的应急预案，以减少系统故障对日常业务的影响。业务持续性评估应参考GB/T 22239和GB/T 35273实施。

B.2.1.1 血站信息系统预防性方案

对于血站信息系统，必须建立预防性方案，以减少系统故障的风险。血站信息系统预防性方案应在系统设计规划时建立，在系统功能变更时再次进行评估和确认。

血站信息系统预防性方案应包含以下内容：

a)硬件冗余设计方案；

b)系统维护方案；

c)系统监控方案；

d)数据备份和恢复方案；

e)培训；

f)安保措施。

B.2.1.2 灾难恢复方案

血站信息系统灾难恢复方案是业务持续计划的一个重要组成部分。在新建或业务变更时，应对可能出现的灾难事件进行预先的风险评估，建立和实施血站信息系统灾难恢复方案。

血站信息系统风险评估方法可参考GB/T 20984。血站信息系统灾难恢复方案可参考GB/T 20988。

B.2.1.3 业务应急预案

血站必须建立业务应急预案，以保证在血站信息系统瘫痪时的血液供应，确保血液供应工作的连续性，并规范这一时期需要遵守的业务行为准则。业务应急预案应定期进行演习，以确保其持续有效。

业务应急预案应包含以下内容：

a)识别关键业务点；

b)制订业务行为准则；

c)制订应急操作方案；

d)规划操作流程；

e)制定并实施应急演习计划。

B.2.2 信息安全风险评估

信息安全风险评估是血站信息系统安全保障机制建立过程中的一种评价方法。血站信息系统风险评估具体方法可参考GB/T 20984。

B.2.3 培训内容评估

培训内容评估的作用在于确保本次变更的相关文档完整、准确，并且以用户能够正确理解的语言编写。培训内容评估方法可参考GB/T 19025。

附 录 C
（资料性附录）
血站信息系统确认报告

确认项目名称			
项目基本情况			
确认目的、范围			
确认开始日期		确认结束日期	
测试和评估情况			
测评项目	测评结论	偏移报告概要	最低期望结果
安装鉴定			
操作鉴定			
性能鉴定			
业务持续性评估			
信息安全风险评估			
培训内容评估			
附件清单			
确认小组成员名单			
姓名	工作部门（单位）	职务（职称）	签字
确认结论	组长： 日期：		

附　录　D
（资料性附录）
血站信息系统测试和评估报告

测评项目名称			
测评目的、范围			
测评开始日期		测评结束日期	
测评过程			
测评项目检查表			
检查项编号	检查项内容	检查结果	
偏离报告			
检查项编号	偏离情况	风险评估	处置意见
测评人员名单			
姓名	工作部门（单位）	职务（职称）	职责
测评结论	测评人员： 日期：		

附　录　E
（资料性附录）
血站信息系统确认流程图