**中国外汇交易中心**

**系统变更合规风险评估规程**

**第一章 总则**

1. 为规范中国外汇交易中心（以下简称交易中心）系统变更合规风险评估工作，提高系统变更交付件质量，根据《中国外汇交易中心IT风险管理办法》等相关规定，制定本规程。
2. 本规程所称系统变更是指在变更签报中明确的生产环境普通变更和快速变更，包括新建应用系统，升级已投入生产环境运行的应用系统，基础设施升级改造以及下线系统。
3. 合规风险评估不通过的版本，将在变更签报中提示风险。

**第二章 职责分工**

1. 风险管理部负责合规风险评估检查工作，负责对拟部署事项进行合规风险评估，包括交付物的完整性，交付内容的合规性，流程的完备性，以及变更安全性评估工作，相关部门应配合及时提交相应的评估材料。
2. 系统主管部门负责验收测试环境准入准出验收工作，对提交的交付件质量和合规控制进行把关，若版本无法满足验收准出标准，该版本将不得提交至模拟测试环境。
3. 工程运行部负责制定模拟测试环境准入标准，依据准入标准进行审核评估，不符合准入标准的软件版本不得进入后续的测试阶段。同时对模拟准出交付件合规控制进行评估检查，若版本无法满足模拟准出标准，该版本将不得提交至后续流程。
4. 各相关部门须在《系统业务技术风险评估报告》中明确提交版本的相关交付件。（相关评估项见附件）
5. 在变更合规风险评估工作前，工程运行部变更经理应召集发布例会，讨论本周拟部署变更的发布构建情况和风险情况，以及变更的测试和准备情况。发布例会中，应用系统发布包存在发布包不完整、测试中发现致命或严重缺陷、测试用例通过率不足、测试不通过、扫描报告中存在高危漏洞且无应对措施、工程运行部审核交付件不通过等情形的，工程运行部和风险管理部应提出风险警示。

**第三章 应用系统变更合规风险评估工作**

1. 在变更签报中明确的生产环境变更需提交如下交付材料，用于交付件合规性审核：

（一）需求规格说明书或技术改动说明 ；

（二）概要设计/详细设计（如有）；

（三）项目技术方案/总体技术方案（如有）；

（四）测试范围及方案（如有）；

（五）验收测试报告；（功能测试、性能测试（如有）和高可用测试（如有））

（六）模拟测试报告；（安装测试、功能测试、性能测试（如有）和高可用测试（如有））

（七）遗留缺陷清单及应对措施（如有）；

（八）关联系统变更影响评估和说明（如有）；

（九）关联系统联测报告（如有）；

（十）安全漏洞扫描报告（如有）；

（十一）版本发布说明（如有）；

（十二）应用变更实施方案；

（十三）运行维护手册（如有）；

（十四）数据初始化或数据迁移步骤文档（如有）；

（十五）风险评估报告（如有）；

（十六）软件升级包（如有）；

（十七）其它变更交付件（如有）。

交付件原则上应在上线前两个工作日提交齐全，供合规风险评估工作开展，同时提交物应与《系统业务技术风险评估报告》评估内容相一致。没有提交齐全的，上线日期应顺延至下个变更窗口；多提交的应确认之前评估内容是否错误。

第三、四、五章中评估条目如无特殊说明，系统主管部门在验收测试环境准出、工程运行部在模拟测试环境准出以及风险管理部在变更合规性评估工作中都须进行检查。

1. 风险管理部负责检查全流程平台流程中，相关部门负责人签字是否有遗漏，系统上线前，签字须齐全，否则上线日期应顺延至下个变更窗口。
2. 测试报告评估项包括以下内容：

（一）测试报告应有测试结论：测试通过；

（二）测试报告结论为“测试完成”的与“测试通过”不等价；

（三）测试报告中测试用例通过率应在90%以上。测试用例通过率低于90%，但报告中测试结论为“测试通过”的，合规风险评估不予通过；

（四）测试报告中无测试结论的合规风险评估工作应要求其在上线前补充测试结论；

（五）变更窗口前一工作日下午4点测试报告仍未提交至合规风险评估工作流程处的应予以风险警示；

（六）除了 E 类缺陷，要求在《遗留问题清单及应急措施》中针对其他遗留缺陷均需有应对措施；

（七）测试报告中显示有B类缺陷的，原则上不予通过；如测试报告中确认“测试通过”，且模拟准出通过，则要求在《遗留问题清单及应急措施》中针对所有B类缺陷提供应对措施；

（八）测试报告中测试结论“测试不通过”的，合规风险评估不予通过。

1. 交付件中工作秘密文档须评估是否注明“工作秘密”和保密期限等警示信息，没有注明的应在上线前予以补充。
2. 变更操作步骤评估中如存在以下内容，合规风险评估工作不予通过：

（一）变更操作步骤中存在明文密码的；

（二）变更操作步骤与签报中对是否有灾备变更信息不一致的；

（三）变更操作步骤中无验证步骤的；

（四）变更操作步骤中无回退步骤的；

（五）变更操作步骤中缺少其它必选项的。

1. Web应用安全扫描报告/系统漏洞扫描报告等安全测试报告中显示的本版本引入的高危漏洞，应在上线前予以修复；或制定应对措施并由需求提出人员签字，在签报正文中说明并由中心领导批准后方可实施。

Web应用安全扫描报告/系统漏洞扫描报告等安全测试报告中显示的非本版本（非外购类产品）引入的、生产环境已有的高危漏洞，应在漏洞发现后的14天内予以修复；或随本系统未进入模拟环境的最近一次版本上线时（不应超过 30 天）予以修复，超期未修复的，下一版本变更合规性评估不予通过。如确因业务紧急等原因必须上线，则应在签报中注明，提交中心领导批示。

外购类产品的高危漏洞，修复时间取决于交易中心与原厂商的合同条款。

Web扫描报告/安全测试报告中显示的中危漏洞要求进行排期，在后续版本中予以修复。

1. 交付物的版本应与签报版本一致；交付物的文档标题或版本号与文档内容应一致；同时应确保交付的是最新有效的文件版本。
2. Web应用安全扫描报告和系统漏洞扫描报告等安全测试报告的扫描人员与电子签名人员应一致。
3. 交付物文档中相关岗位不应有离职或转岗人员姓名。

**第四章 快速流程变更合规风险评估工作**

1. 需求提出部门应按照《应用系统快速流程管理办法》要求，申请进入快速流程白名单。
2. 需求单中重要性为“高”和“中”的快速流程版本，应保留《应用系统建设管理办法》和《生产运行系统变更与发布管理办法》中的要求，在变更签报中予以明确，须进行合规风险评估工作。
3. 变更发布例会后，如确认包含快速流程变更版本，工程运行部和需求提出部门应按照《应用系统快速流程管理办法》要求进行报备和变更管理。

**第五章 其他变更合规风险评估工作**

1. 新系统上线应有单独的上线签报，同时须评估测试报告、《系统上线信息安全评估检查表》、《漏洞扫描报告/Web应用安全扫描报告》、《新上线系统信息登记表》、《总体技术方案》和升级工作确认单（如有）。
2. 系统下线应有单独的下线签报，同时须评估《下线技术方案》和下线操作步骤，还须评估包括网络，防火墙，商业软件许可收回等内容。
3. IT基础设施普通变更应有相关签报，须评估升级实施方案和测试报告。

**第六章 附则**

1. 本规程由风险管理部负责解释。
2. 本规程自发布之日起施行。

附 件：

**《系统业务技术风险评估报告》评估项**

**（评估项按现有制度由不同部门负责，在全流程平台中体现部门职责。如部门间职能有调整，全流程平台依据制度进行调整。）**

1、本需求是否影响系统架构、系统主要性能、系统可靠性指标、灾备和安全等保级别等？如有，相应的解决方案是否经过评审？

2、软件需求规格说明书、概要设计文档等是否经过评审？

3、系统测试方案是否进行过评审？

4、本系统及关联系统是否按测试方案进行测试？

5、系统测试中是否发生需求变更？如有，相关需求规格说明书、概要设计文档、详细设计、编码、系统测试等流程的操作是否合规？

6、是否进行性能测试？其测试是否符合性能需求？

7、需交付的服务器端和客户端的升级步骤（含回退步骤）是否进行过测试?

8、是否对用户手册进行更新？如更新，是否经过业务人员评审？

9、是否对系统运维文档进行更新？如更新，是否经过运维人员评审？

10 、是否有遗留缺陷？如有，是否进行了遗留缺陷影响分析和评估，且制定了有效应对措施？

11、是否更新用户操作文档？如更新，是否经过测试检验？

12、是否更新应急手册、应急预案等？如更新，是否经过测试检验？

13、是否需要数据初始化或历史数据迁入（非应用数据库导入）?如需要，是否经过测试检验？

14、是否进行过性能测试（用户体验方面）？其测试是否符合性能需求？

15、是否有遗留缺陷？其应对措施是否经业务人员测试检验？

16、对外服务的应用系统是否需要制定重大改造或新系统上线上线首日运行应急方案？如是，是否经过测试检验？

17、系统上线是否可能存在的其他业务风险？ 如有，是否经过评估并采取风险管控？

18、系统上线存在的其他业务风险已经过评估并采取风险管控？

19、高可用测试方案是否通过评审？

20、模拟环境性能测试方案是否通过评审？

21、是否需要通过安全测试（如漏洞扫描等）？

22、是否是应用系统下线？应用系统下线整体方案是否经过评审？

23、是否对技术运维手册进行更新？如更新，是否经过测试检验？

24、验收测试方案是否进行过评审？

25、验收测试中是否存在因需求变更导致更改软件需求规格说明书的情况？如存在，软件需求规格说明书是否经过评审？

26、验收测试中是否存在因需求变更导致更改概要设计等文档的情况？如存在，概要设计等文档是否按规定经过评审？

27、是否进行过性能测试（服务器方面），其测试是否符合性能需求？

28、历史数据是否需迁入新应用系统系统？如是，其迁移安装步骤是否经过测试检验？

29、是否有遗留缺陷？如有，是否进行了遗留缺陷影响分析和评估，且制定了有效的应对措施？