ICS 35.020
L 70

团　　体　　标　　准

T/DSAG 004-2025

广东省政务云应用系统上线前风险评估指引

(Guidelines for Risk Assessment before the Launch of Guangdong Provincial Government Cloud Application Systems)

2025 - 01 - 01 发布　　2025 - 01 - 01 实施

广东省数字安全协会　发布

目　　次

前　言

本标准按GB/T 1.1—2020给出的规则起草。

本标准由工业和信息化部电子第五研究所提出并归口。

本标准起草单位：工业和信息化部电子第五研究所、广东省政务服务和数据管理局、数字广东网络建设有限公司、公安部第三研究所、奇安信科技集团股份有限公司、杭州安恒信息技术股份有限公司、深信服科技股份有限公司、亚信安全科技股份有限公司、永信至诚科技集团股份有限公司、广东省信息安全测评中心、广州市政务服务和数据管理局、阳江市政务服务和数据管理局、湛江市政务服务和数据管理局、汕头市政务服务和数据管理局、汕头市信息中心、揭阳市政务服务和数据管理局。

本标准主要起草人：刘北水、观雯玉、罗奇伟、程炜、苏锐生、段彦名、赵弘洋、陈晓、关泳强、贺高戈、张嘉子、容菲菲、戴晨、闵家法、钟林、张志伟、陈耿、王雪凤、叶晖、崔玉刚、江坚强、赵栋良、黄恒、郑楷涛、蒋天翔、刘国栋、张嘉杰、陈晓荣、何栋。

广东省政务云应用系统上线前风险评估指引

1 范围

本标准描述了拟部署到广东省政务云上的政务应用系统在正式上线前开展风险评估的流程、评估内容及通过标准。

本标准适用于广东广东省政务云应用系统上线前风险评估工作，各省有关单位可参考本标准自行开展应用系统上线前风险评估，各地市有关单位可视情况参考执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984-2022 《信息安全技术 信息安全风险评估方法》

GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》

GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》

GB/T 40692-2021 《政务信息系统定义和范围》

3 术语和定义

GB/T 20984-2022 《信息安全技术 信息安全风险评估方法》、GB/T 40692-2021 《政务信息系统定义和范围》和GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》界定的以及下列术语和定义适用于本文件。

3.1 **政务应用系统** e-government application system

指由政府投资建设、政府与社会企业联合建设、政府向社会购买服务或需要政府资金运行维护的，用于支撑政务部门履行管理和服务职能的各类信息系统，包括电子政务网络平台、业务信息系统、数据资源库、信息安全与应用支撑基础设施、政务信息化标准体系以及相关支撑体系等符合《政务信息系统定义和范围》规定的系统。

3.2 **风险评估** risk assessment

包括风险分析和风险评价，即对风险发现并确认风险等级（定级）的过程。

3.3 **核查** examine

评估人员通过对评估对象(如制度文档、各类设备及相关安全配置等)进行观察、查验和分析，以帮助评估人员理解、澄清或取得证据的过程。

3.4 **测试** test

评估人员使用预定的方法/工具使评估对象(各类设备或安全配置)产生特定的结果, 将运行结果与预期的结果进行比对的过程。

3.5 **评估** evaluate

对评估对象可能存在的威胁及其可能产生的后果进行综合评价和预测的过程。

3.6 **评估对象** target of testing and evaluation

风险评估过程中不同评估方法作用的对象，主要涉及相关配置文件、设备设施及业务应用系统等。

3.7 **容器** container

通过名称空间、控制组和切根等技术实现资源、文件、设备、状态和配置的划分和隔离的沙盒技术即容器技术。常见的容器技术有Docker、Kubernetes等。本指引中的容器指通过容器技术构建的实例。

3.8 **宿主机** host machine

运行容器等虚拟化软件或其他系统组件的服务器。

3.9 **数据库系统** database system

用于存储业务应用系统的用户和鉴别信息、重要业务信息的数据库管理系统。常见的数据库系统有MySQL、MariaDB、Oracle、PostgereSQL、SQL Server、MongoDB、达梦数据库、神通数据库、人大金仓等。

3.10 **云数据库** cloud database

基于云计算平台，以“平台即服务（PaaS）”模式提供的数据库服务，允许用户在云端存储、管理和处理数据。本指引中的云数据库特指广东省政务云平台

提供的云数据库服务，如TDSQL、TDATA、TBASE等。3.11 **Web中间件系统**

web middleware system

位于Web应用程序和服务器之间，主要用于处理HTTP请求和响应的独立部署在服务器上的服务组件（不包含框架内置的Web中间件）。常见的Web中间件系统有Apache、Tomcat、Nginx、IIS、Weblogic、金蝶天燕、东方通等。

4 上线前风险评估概述

4.1 评估定位

本指引所述上线前风险评估是对拟部署到广东省政务云上的政务应用系统安全状态的审查。未达到通过标准或经一轮限期整改后仍未达标的应用系统不得上线运行。政务应用系统上线后，政务应用系统建设单位应持续落实网络安全责任，每两年自行组织对已上线政务应用系统的风险评估工作。

4.2 评估范围

新部署到广东省政务云的政务应用系统，包括从广东省政务云以外云平台或物理部署环境迁移至广东省政务云的系统和在广东省政务云上新建的系统，属于上线前风险评估范围。

早期已通过政务应用系统上线前风险评估且已部署在广东省政务云的系统，后续发生在广东省政务云内迁移（由广东省政务云非国产化资源区迁移至国产化资源区的除外）、功能升级、版本迭代、资源扩容，不属于上线前风险评估范围，建议按需自行开展安全测评或风险评估。

部署在广东省政务云非国产化资源区的政务应用系统迁移至广东省政务云国产化资源区时，应用系统部署环境变化较大，且通常需要进行适配性改造或重构，为确认迁移后系统安全性，纳入上线前风险评估范围。

新部署到广东省政务云的政务应用系统，其部分功能或资源部署在广东省政务云以外的，即未部署在广东省政务云上的部分（简称“外部组件”）不属于上线前风险评估范围；但广东省政务云上应用系统调用外部组件所提供的功能视作广东省政务云上应用系统的功能，属于上线前风险评估范围。

广东省政务云应用系统上线前风险评估围绕政务应用开展，应覆盖政务应用系统的运行环境、应用系统自身及安全保障策略等对象，不包含物理环境、相关网络设备和安全设备等。

4.3 角色职责

政务应用系统上线前风险评估，主要涉及政务应用系统建设单位和评估服务机构等角色。

4.3.1 政务应用系统建设单位

政务应用系统建设单位应落实对拟部署在广东省政务云应用系统的安全责任，在提交上线前风险评估申请前需自行做好风险评估及相关整改工作，上线前风险评估期间积极配合评估工作，及时完成安全加固和整改。

4.3.2 评估服务机构

评估服务机构对拟部署到广东省政务云上的政务应用系统开展风险评估工作，对应用系统是否达到通过标准给出判断，出具评估报告，并对评估结果负责。

5 评估流程

广东省政务云应用系统上线前风险评估整体流程如下：

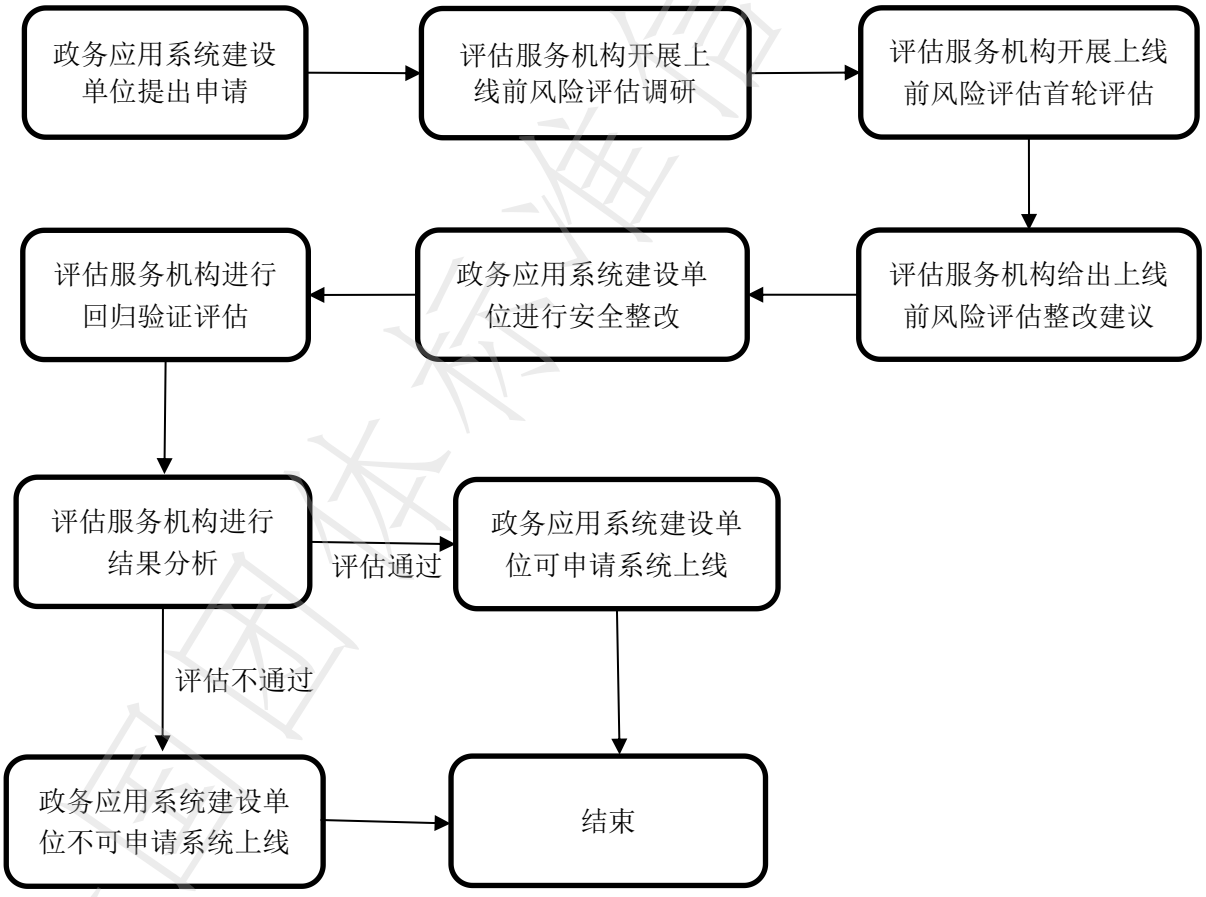

图 1 上线前风险评估整体流程

5.1 评估申请

应用系统上线前风险评估申请由政务应用系统建设单位提出。

为保证上线前风险评估工作效果，政务应用系统建设单位应合理划分应用系统边界。宜以承担相对独立的业务，使用较为独立的资源，有明确且独立的责任主体（如开发责任、维护责任、使用责任）为原则划定应用系统边界。无法独立提供服务的功能模块，不宜作为应用系统；包含多个独立业务的服务平台，宜按照业务划分为多个应用系统。

政务应用系统建设单位提出上线前风险评估申请前，应确保系统已完成开发且在政务云上完成部署和调试[1]，自行委托第三方评估服务机构开展风险评估并落实整改，确保系统安全能力已满足系统上线要求。

政务应用系统建设单位提出评估申请时，应提供准确的系统名称、系统类型、系统类别等系统信息，并将政务应用系统风险评估报告（含问题整改记录）一并提交。

5.2 评估实施

上线前风险评估实施包括系统调研、首轮评估、安全问题整改、回归评估、评估总结和报告编制等环节。整个评估实施过程原则上不超过60个工作日。

5.2.1 系统调研

[1] 指在政务云的特定安全区或测试区完成上线前所有开发、部署和调试，开通相应网络策略后即可对外提供服务。

评估服务机构对政务应用系统开展信息调研，政务应用系统建设单位配合提供调研信息，并确保系统相关组件正常运行。评估工作需要开通网络访问策略的，由政务应用系统建设单位协助开通。评估服务机构在政务应用系统建设单位配合下对调研信息进行核验、完善，形成最终调研结果，确认具备开展后续评估工作的环境条件。

系统调研信息应包括系统基本信息、相关人员联系方式、系统拓扑、系统相关组件信息及必要的身份认证信息等内容。

系统调研一般不超过5个工作日。

5.2.2 首轮评估

评估服务机构基于调研结果，对政务应用系统开展首轮评估，对评估记录进行分析，形成包含安全问题清单、风险评价及整改建议的首轮评估结果，并将首轮评估结果及时反馈给政务应用系统建设单位。

首轮评估时，若政务应用系统存在多个同类型、同功能的服务器及组件，可通过抽样的方式进行评估。抽样需覆盖系统所有不同类型组件。

首轮评估一般不超过10个工作日。若政务应用系统规模较大、较复杂或评估实施难度较大，首轮评估时间可适当延长，相关方应保持充分沟通。

5.2.3 安全问题整改

政务应用系统建设单位收到首轮评估结果后，应对风险项和漏洞进行整改，并对整改措施及过程做详细记录说明。特别的，当首轮评估采取了抽样方式评估，首轮评估中未覆盖到的服务器及组件可能存在的同类问题也应当

得到整改。政务应用系统建设单位应确保整改后的政务应用系统达到风险评估通过标准。

安全问题整改一般不超过15个工作日。若安全问题整改难度较大，政务应用系统建设单位可向评估服务机构申请延长整改时间，整改时间累计不超过25个工作日。

5.2.4 回归评估

政务应用系统建设单位向评估服务机构提出回归评估申请，同时提供详细的整改记录文件。评估服务机构对安全问题的整改情况进行验证，确保所有安全问题都得到全面、妥善处置。

特别的，当首轮评估采取了抽样方式评估，在回归评估环节应对可能存在同类问题、但在首轮评估中未覆盖到的服务器及组件进行验证。

回归评估一般不超过5个工作日。

5.2.5 评估总结和报告编制

评估服务机构根据首轮评估结果、安全问题整改情况及回归评估结果等内容，对政务应用系统面临的安全风险进行综合分析，形成评估结果（通过或不通过），编制风险评估报告。

评估总结和报告编制一般不超过15个工作日。

6 评估内容

6.1 评估对象选择

广东省政务云应用系统上线前风险评估应覆盖政务应用系统的运行环境、应用系统自身及安全保障策略等对象。应用系统运行环境包括应用系统相关的服务器操作系统、数据库系统、中间件系统。应用系统自身包括应用系统自身与安全相关的功能、应用代码。安全保障策略包括数据安全及备份恢复策略等。针对不同的评估对象采用不同的方法及相应的评估指标。

评估方法包括配置核查、渗透测试、漏洞扫描、恶意代码扫描。不同的评估对象应对应不同的评估方法，如下表所示。

评估对象		评估方法			
		配置核查	渗透测试	漏洞扫描	恶意代码扫描
应用系统运行环境	服务器操作系统	√		√	
	数据库系统*	√		√	
	中间件系统*	√		√	
	其它相关组件**			√	
应用系统自身***	安全相关功能	√	√	√	
	应用代码				√
安全保障策略	数据安全及备份恢复策略	√			

√表示对于该评估对象，以相应评估方法开展评估。

*对于广东省政务云上以“平台即服务（PaaS）”模式提供的相关组件，上线前风险评估中仅考察能够由政务应用系统建设单位管理配置的相关功能；

**其它相关组件指支撑应用系统正常运行的其它组件，如 ZooKeeper、ElasticSearch、Kafka、Zabbix 等，其它相关组件是否采用配置核查的评估方法取决于该组件对应用系统安全性是否有直接影响，由评估服务机构结合应

用系统部署情况研判后确定；

***对于以多个微服务形式构建的应用系统，重点以应用系统整体作为评估对象，单一微服务不作为评估对象，微服务对应用系统安全性有直接影响的除外；单一微服务是否列为评估对象由评估服务机构结合应用系统部署情况研判后确定；

若政务应用系统存在多个同类型、同功能的评估对象，可通过抽样的方式进行评估。抽样需覆盖系统所有不同类型组件。

6.2 系统配置核查

6.2.1 评估对象及内容

6.2.1.1 服务器操作系统（通用）

序号	评估对象	评估单元	评估项要求	备注
1	服务器操作系统	身份鉴别	应采用账户名密码、生物技术、动态口令等一种或多种相结合的身份认证方式。	配置修改
2	服务器操作系统	身份鉴别	操作系统用户口令应具有复杂度要求并定期更换，要求账户口令长度应至少为 8 位，口令必须为大小写字母（a-z，A-Z）、数字（0-9）、符号（~!@#$%^&*()_<>）的组合。	配置修改
3	服务器操作系统	身份鉴别	应具有登录失败处理功能，应限制非法登录次数，并配置登录会话超时自动退出。	配置修改
4	服务器操作系统	身份鉴别	对服务器操作系统进行远程管理时应采取必要措施防止鉴别信息在网络传输过程中被窃听。	配置修改
5	服务器操作系统	身份鉴别	应确保用户名唯一性。	配置修改
6	服务器操作系统	访问控制	应重命名或删除系统默认账户，修改默认账户的默认口令，合理限制默认账户的访问权限。	配置修改
7	服务器操作系统	访问控制	应定期审查操作系统账户，及时删除或禁用多余、过期的账户。	配置修改
8	服务器操作系统	访问控制	应对重要系统文件的访问权限进行限制。	配置修改
9	服务器操作系统	安全审计	应开启操作系统日志审计功能，或通过第三方审计系统对操作系统进行审计，审计策略应覆盖到所有用户。	配置修改

序号	评估对象	评估单元	评估项要求	备注
10	服务器操作系统	安全审计	审计日志记录必须保存至少六个月，应避免日志文件受到未预期的删除、修改或覆盖等。	配置修改
11	服务器操作系统	安全审计	应设定日志系统配置文件权限和日志文件权限。	配置修改
12	服务器操作系统	入侵防范	操作系统应遵循最小安装原则，仅安装需要的组件和应用程序；并应能发现可能存在的已知漏洞，及时修补漏洞。	配置修改 补丁安装
13	服务器操作系统	入侵防范	应关闭操作系统的默认共享服务，并关闭多余的服务端口。	配置修改
14	服务器操作系统	入侵防范	应限制远程登录终端的接入方式和网络地址范围。	配置修改
15	服务器操作系统	入侵防范	应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	组件安装
16	服务器操作系统	恶意代码防范	操作系统应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。	组件安装

6.2.1.2 数据库系统（通用）

序号	评估对象	评估单元	评估项要求	备注
1	数据库系统	身份鉴别	应采用账户名密码、生物技术、动态口令等一种或多种相结合的身份认证方式。	配置修改
2	数据库系统	身份鉴别	数据库系统用户口令应具有复杂度要求并定期更换，要求账户口令长度应至少为 8 位，口令必须为大小写字母（a-z，A-Z）、数字（0-9）、符号（~!@#$%^&*()_<>）的组合。	配置修改 （组件安装）
3	数据库系统	身份鉴别	应具有登录失败处理功能，应限制非法登录次数，并配置登录会话超时自动退出。	配置修改
4	数据库系统	身份鉴别	对数据库系统进行远程管理时应采取必要措施防止鉴别信息在网络传输过程中被窃听。	配置修改
5	数据库系统	访问控制	应在宿主操作系统中设置本地数据库专用账号，并赋予该账户除运行数据库服务外的最低权限。	配置修改
6	数据库系统	访问控制	应用系统账户权限分配应遵循最小权限的原则，严禁应用系统账户具有 DBA 权限。	配置修改
7	数据库系统	访问控制	应重命名或删除默认账户，修改默认账户的默认口令。	配置修改
8	数据库系统	访问控制	应定期审查数据库账户，及时删除或禁用多余、过期的账户。	配置修改
9	数据库系统	安全审计	应开启数据库审计功能，或通过第三方审计系统对数据库进行审计，审计范围应覆盖到数据库所有账户。	配置修改/组件安装

序号	评估对象	评估单元	评估项要求	备注
10	数据库系统	安全审计	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	配置修改
11	数据库系统	安全审计	应保护审计记录，避免其受到未预期的删除、修改或覆盖等，审计记录要求至少保存六个月。	配置修改
12	数据库系统	安全审计	应限制日志系统配置文件权限和日志文件权限。	配置修改
13	数据库系统	入侵防范	数据库应遵循最小安装的原则，仅安装需要的组件；并应能发现可能存在的已知漏洞，及时修补漏洞。	配置修改 补丁安装
14	数据库系统	入侵防范	应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	配置修改

6.2.1.3 数据库系统（云数据库）

序号	评估对象	评估单元	评估项要求	备注
1	数据库系统	身份鉴别	数据库系统用户口令应具有复杂度要求并定期更换，要求账户口令长度应至少为 8 位，口令必须为大小写字母（a-z，A-Z）、数字（0-9）、符号（~!@#$%^&*()_<>）的组合。	配置修改 （组件安装）
2	数据库系统	身份鉴别	应具有登录失败处理功能，应限制非法登录次数，并配置登录会话超时自动退出。	配置修改
3	数据库系统	身份鉴别	对数据库系统进行远程管理时应采取必要措施防止鉴别信息在网络传输过程中被窃听。	配置修改
4	数据库系统	访问控制	应用系统账户应按照最小权限的原则，严禁应用系统账户具有 DBA 权限。	配置修改
5	数据库系统	安全审计	应开启数据库审计功能，或通过第三方审计系统对数据库进行审计，审计范围应覆盖到数据库实例所有账户。	配置修改/组件安装
6	数据库系统	安全审计	应保护审计记录，避免其受到未预期的删除、修改或覆盖等，审计记录要求至少保存六个月。	配置修改

6.2.1.4 Web 中间件系统（通用）

序号	评估对象	评估单元	评估项要求	备注
1	Web 中间件系统	身份鉴别	应采用账户名密码、生物技术、动态口令等一种或多种相结合的身份认证方式。	配置修改 （一般禁用控制台）
2	Web 中间件系统	身份鉴别	中间件系统用户口令应具有复杂度要求并定期更换，要求账户口令长度应至少为 8 位，口令必须为大小写字母（a-z，A-Z）、数字（0-9）、符号（~!@#$%^&*()_<>）	配置修改 （一般禁用控制台）

序号	评估对象	评估单元	评估项要求	备注
			的组合。	
3	Web 中间件系统	身份鉴别	应具有登录失败处理功能，应限制非法登录次数，并配置登录会话超时自动退出。	配置修改（一般禁用控制台）
4	Web 中间件系统	身份鉴别	对 Web 中间件系统进行远程管理时应采取必要措施防止鉴别信息在网络传输过程中被窃听。	配置修改（一般禁用控制台）
5	Web 中间件系统	访问控制	应在宿主操作系统中设置本地中间件专用账户，并赋予该账户除运行中间件服务外的最低权限。	配置修改
6	Web 中间件系统	访问控制	应重命名或删除默认账户，修改默认账户的默认口令，更改默认端口。	配置修改（一般禁用控制台）
7	Web 中间件系统	访问控制	应定期审查 Web 中间件系统账户，及时删除或禁用多余、过期的账户。	配置修改（一般禁用控制台）
8	Web 中间件系统	安全审计	应启用中间件系统的日志审计功能，并对审计进程进行保护。	配置修改
9	Web 中间件系统	安全审计	应保护审计记录，避免其受到未预期的删除、修改或覆盖等，审计记录至少保存六个月。	配置修改
10	Web 中间件系统	安全审计	应限制日志系统配置文件权限和日志文件权限，更改中间件 Web 日志默认路径。	配置修改
11	Web 中间件系统	入侵防范	应对中间件系统敏感信息进行隐藏；并对中间件系统错误页面进行重定向处理，错误页面应不泄露系统信息。	配置修改
12	Web 中间件系统	入侵防范	应禁止中间件系统目录遍历。	配置修改
13	Web 中间件系统	入侵防范	应对中间件管理后台进行登录源限制。	配置修改（一般禁用控制台）

6.2.1.5 应用系统（通用）

序号	评估对象	评估单元	评估项要求	备注
1	应用系统	身份鉴别	应具有专用的登录控制模块对系统用户进行身份鉴别。	应用设计（代码）
2	应用系统	身份鉴别	应用系统用户口令应具有复杂度要求并定期更换，要求账户口令长度应至少为 8 位，口令必须为大小写字母（a-z，A-Z）、数字（0-9）、符号（~！@#$%^&*()_<>）的组合，涉及口令设置之处均需进行口令复杂度校验。	应用设计（代码）
3	应用系统	身份鉴别	应用系统用户身份鉴别信息应不在登录页面或者系统代码中固定。	应用设计（代码）

序号	评估对象	评估单元	评估项要求	备注
4	应用系统	身份鉴别	登录时应用系统应附加随机码验证。	应用设计（代码）
5	应用系统	身份鉴别	应具有登录失败处理功能，应统一模糊化登录失败提示信息，限制非法登录次数，并配置登录会话超时自动退出。	应用设计（代码）
6	应用系统	访问控制	应重命名或删除系统默认账户，修改默认账户的默认口令。	配置修改
7	应用系统	访问控制	应对应用系统用户进行权限限制。	配置修改
8	应用系统	访问控制	应及时删除或停用多余的、过期的应用系统账户。	应用设计（代码）
9	应用系统	访问控制	应限制单个账户的多重并发会话数。	应用设计（代码） 配置修改
10	应用系统	安全审计	应启用应用系统日志审计功能，审计日志内容应至少包含用户登录、登出、失败登录日志；管理员授权操作日志；创建、删除（注销）用户操作日志；重要业务操作日志。	应用设计（代码） 配置修改
11	应用系统	安全审计	日志记录应包括主体、客体、事件类型、日期时间、描述、结果等。	应用设计（代码）
12	应用系统	安全审计	应对日志记录进行保护，禁止非授权删除或修改日志记录，日志记录应至少保存六个月。	应用设计（代码）
13	应用系统	入侵防范	应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	应用设计（代码）或 配置修改
14	应用系统	入侵防范	应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度等内容符合安全要求。	应用设计（代码）
15	应用系统	入侵防范	应具备文件上传白名单过滤功能，禁止上传 asp、jsp、exe、vbs、com 等可执行类型文件。	应用设计（代码）
16	应用系统	数据完整性	应采用校验技术或密码技术保证重要数据在传输过程中的完整性。	应用设计（代码）或 配置修改
17	应用系统	数据保密性	应采用密码技术保证敏感数据在传输过程中的保密性。	应用设计（代码）或 配置修改

6.2.1.6 数据安全及备份恢复策略

序号	评估对象	评估单元	评估项要求	备注
1	数据安全及备份恢复策略	数据完整性	应采用校验技术或密码技术保证鉴别信息和重要业务数据在传输过程中的完整性。	配置修改

序号	评估对象	评估单元	评估项要求	备注
2	数据安全及备份恢复策略	数据保密性	应采用密码技术或其他保护措施实现鉴别信息的存储保密性。	应用设计（代码）或配置修改
3	数据安全及备份恢复策略	备份和恢复	应能够对应用系统及其业务产生的业务数据以及应用系统个人信息等进行备份和恢复。	备份策略与恢复性测试
4	数据安全及备份恢复策略	备份和恢复	应通过提供数据处理系统的热冗余等方式，保证系统的高可用性。	冗余策略

6.2.2 评估方法

a) 通过人工核查方式，核查系统配置是否存在配置错误的风险。

b) 通过风险评估与管理工具，核查系统配置是否存在配置错误的风险。

6.2.3 通过评估要求

a) 评估项的符合程度由评估人员根据实际场景综合研判，风险级别参考GB/T 20984 判定；

b) 不存在高风险项，每个评估对象允许遗留不会带来实质性安全风险的中和低风险项总数为三个，具体允许遗留数量可视系统实际情况酌情调整，但不能遗留会带来实质性安全风险的中、低风险项。

6.3 应用渗透测试

6.3.1 评估对象及内容

渗透测试针对应用系统开展，内容上包括但不限于以下评估项，提交结果时只提交发现的安全问题。

序号	评估对象	评估项	评估项要求
1	应用系统	登录密码是否加密	检验密码字段在传输过程是否使用不可逆的 hash 算法，禁止使用 MD5、Base64 等弱算法。

序号	评估对象	评估项	评估项要求
2	应用系统	是否可猜解用户名	检验系统是否存在接口可以检测用户是否存在。
3	应用系统	是否存在可暴力破解的用户密码	检验系统是否采取安全措施防止密码暴力破解或猜解。
4	应用系统	是否可批量注册用户	检验系统是否采取安全措施防止注册的时候批量提交注册信息。
5	应用系统	验证码有效性	检验验证码是否和登录或注册接口一起提交检验，验证码是否为一次性使用；若为手机验证码，是否长度达到六位，有效期是否能在 3 分钟以内。
6	应用系统	修改密码处是否验证旧密码	检验用户更改密码功能是否要求用户输入当前的密码进行校验，且密码修改成功后，之前的登录的会话是否已失效。
7	应用系统	初始密码强制修改	检验系统是否存在默认的初始密码，若存在，则需强制用户在首次登录后修改密码。
8	应用系统	密码强度要求	应用系统特别是后台类应用系统应有密码强度控制，密码强度强制要求 8 位以上，为大小写字母、特殊符号、数字的组合，避免用户设置弱口令。
9	应用系统	是否固定登录会话	检验登录前后会话 ID 是否存在变化，每次登录会话 ID 是否存在变化。
10	应用系统	注销功能是否有效	检验注销系统后，会话是否仍然有效。
11	应用系统	Cookie 中是否存在敏感信息	检验 cookie 中是否存在敏感信息如密码或者加密的密码或者验证码的值。
12	应用系统	cookie 是否设置 http only	检验 Web 是否设定 http only 属性应用在 Cookie。
13	应用系统	是否存在中间件错误页面	检验应用系统在处理异常页面时是否已自定义错误页面，禁止使用中间件的默认错误页面，错误码需包括 400，401，402，403，404，405，500，501，502，503，500。
14	应用系统	是否暴露异常处理报错信息	检验在接口或页面在异常处理时是否会暴露错误信息如 SQL 语句或开发主键信息。
15	应用系统	是否存在源代码泄露	检验 WEB 目录是否存在源代码备份文件，.git、.svn、.DS_Store 等版本管理或者系统管理的隐藏文件。
16	应用系统	源代码注释信息	检验在前端代码中是否存在注释的敏感信息，如开发过程中的 token，账号密码，内网 IP 地址。
17	应用系统	是否存在用户敏感信息明文传输	检验在前端以及接口中是否存在用户敏感信息明文传输，如：用户身份证、地址、手机号、密码等。后端需要掩码返回敏感信息，前端传递信息到后端需要加密使用 RSA、SM2 等非对称加密算法。
18	应用系统	banner 信息泄露	中间件系统、web 容器 banner 信息等需进行屏蔽。

序号	评估对象	评估项	评估项要求
19	应用系统	是否存在中间件管理后台弱口令	检验中间件的管理后台是否存在弱口令；中间件系统管理后台不应解析到互联网中。
20	应用系统	是否存在目录浏览	检验系统是否存在目录浏览。
21	应用系统	是否存在任意文件上传漏洞	检验系统是否采取措施防范用户上传恶意文件，措施至少包括： 1、文件类型检查：客户端初步检测文件大小（防止容量攻击）、文件扩展名；服务端重新检测文件大小、文件扩展名，禁止上传任意后缀文件； 2、文件特征码检查：在检查文件后缀的基础上，进一步检查文件内容特征码以判断文件的真实性。
22	应用系统	是否存在任意文件下载漏洞	系统下载或者读取文件的时若采取相对路径的方法读取文件，后台是否有限定在固定的目录下，防止通过../的方法读取系统的文件。
23	应用系统	是否存在文件包含漏洞	检验关键文件操作功能是否存在远程/文件包含类漏洞。
24	应用系统	是否存在跨站脚本攻击漏洞	检验是否采取措施防范跨站脚本攻击，输出转义/编码应应用于所有用户输入在其屏幕上显示之前。
25	应用系统	是否存在 SQL 注入漏洞	检验是否采取措施防范 SQL 注入漏洞，禁止通过拼接 SQL 语句的方法执行 SQL 查询。
26	应用系统	是否存在 URL 跳转漏洞	检验系统的跳转接口，是否采取措施限制跳转的地址。
27	应用系统	是否存在跨站请求伪造漏洞	检验系统的重要操作如修改密码是否验证表单来源以防止恶意欺骗的操作。

序号	评估对象	评估项	评估项要求
28	应用系统	是否存在越权风险	1、检验系统是否存在横向或纵向越权； 2、检验权限控制是否做到前端页面功能和后端功能一致。
29	应用系统	是否存在逻辑绕过	检验系统是否已采取措施防止用户通过修改参数实现流程跳跃：登录、找回密码缺陷、审核流程绕过等。
30	应用系统	是否存在未授权访问	1、检验应用系统是否在服务端进行身份验证以及权限验证，检验非登录的用户是否可以访问需要登录方可访问的资源； 2、检验应用系统相关的组件是否存在未授权访问风险。
31	应用系统	是否存在中间件组件漏洞	检验运行应用的中间组件是否已升级到最新的稳定版本，若因依赖关系不能跨版本升级，也需升级当前版本的最新的子版本。已不在维护的组件版本，必须升级到最新版本。中间组件包括但不限于以下范围： 1、JBOSS 2、Tomcat 3、Apache 4、Webshpere 5、IIS 6、Weblogic 7、Jetty 8、ColdFusion 9、Nginx 10、Glasshfish
32	应用系统	是否使用低版本数据库	检验数据库是否已升级到最新的稳定版本，若因依赖关系不能跨版本升级，也需升级当前版本的最新的子版本。已不在维护的组件版本，必须升级到最新版本。数据库包括但不限于以下范围： 1、Oracle 2、Mysql 3、Microsoft SQL Server 4、DB2 5、Sybase 6、Redis 7、Mongodb 8、Memcache 9、Postgresql

序号	评估对象	评估项	评估项要求
33	应用系统	是否存在开发组件漏洞	检验开发过程中是否已经将开发组件升级到最新的稳定版本，若因依赖关系不能跨版本升级，也需升级当前版本的最新的子版本。已不在维护的组件版本，必须升级到最新版本。开发组件包括但不限于以下范围： 1、Fastjson 2、struts2 3、thinkphp 4、spring 5、Apache MQ 6、asix2 7、shiro 8、Django
34	应用系统	是否存在短信炸弹漏洞	检验系统中存在的短信发送功能是否已采取措施限制发送的频率。若是已登录的状态下发送短信，应针对用户限制发送频率；非登录状态应添加验证码以限制发送频率。
35	应用系统	是否存在邮件炸弹漏洞	检验应用系统中存在的邮件发送功能是否已采取措施限制发送的频率。若是已登录的状态下发送邮件，应针对用户限制发送频率；非登录状态应添加验证码以限制发送频率。
36	应用系统	是否存在微信推送炸弹漏洞	检验应用系统中存在的微信推送功能是否已采取措施限制发送的频率。若是已登录的状态下发送微信推送，应针对用户限制发送频率。
37	应用系统	是否合理使用 HTTP 传输方法	HTTP 传输过程中，对用户的敏感数据如身份证、手机号、id 等禁止使用 GET 方法传输，过长的数据也应通过 POST 方法传递。
38	应用系统	是否存在危险的 HTTP 方法	检验系统是否已禁用非常规的 HTTP 请求方法如 DEL、TRACE 等，若非需要应只使用 GET、POST。
39	应用系统	是否合理配置 CORS	检验系统是否已限制接口的跨域请求，禁止配置 Access-Control-Allow-Origin:*。
40	应用系统	后台地址是否复杂	后台类的应用系统，登录 url 应使用复杂的路径，避免被攻击者利用，禁止使用：/admin/、/manager/、/backend/、/guanli/、/wwwroot/等。
41	应用系统	是否存在接口请求未鉴权	接入网关的应用是否已配置对所有的接口进行签名校验，接入网关的应用，拒绝所有非网关发起的请求。

6.3.2 评估方法

通过以人工渗透方式为主，评估工具为辅的方式，核查系统是否存在脆弱性。

6.3.3 评估通过要求

a) 评估项的符合程度由评估人员根据实际场景综合研判，风险级别参考GB/T 20984判定；

b) 不允许遗留超高危、高危漏洞，每个评估对象允许遗留不会带来实质性安全风险的中危和低危漏洞总数为不超过两个，低危漏洞遗留数可根据系统实际情况酌情调整。

6.4 主机漏洞扫描

6.4.1 评估对象及内容

主机漏洞扫描为利用主机脆弱性扫描工具针对服务器上运行的服务实施扫描，内容上包括但不限于以下评估项，提交结果时只提交发现的安全问题。

序号	评估对象	评估项要求	备注
1	服务器当前服务	操作系统账户口令强度测试（空口令检测、弱口令检测）	配置修改
2	服务器当前服务	操作系统账户身份认证测试（合法用户身份检测、非法用户身份绕过检测）	配置修改
3	服务器当前服务	操作系统账户访问控制测试（普通用户身份访问非授权资源检测）	配置修改
4	服务器当前服务	操作系统安全漏洞测试（操作系统本身安全漏洞扫描和安全检测，如操作系统缓冲区溢出漏洞检测）	补丁安装
5	服务器当前服务	数据库账户口令强度测试（空口令检测、弱口令检测）	配置修改
6	服务器当前服务	数据库账户身份认证测试（合法用户身份检测、非法用户身份绕过检测）	配置修改
7	服务器当前服务	数据库账户访问控制测试（普通数据库用户身份访问非授权资源检测）	配置修改
8	服务器当前服务	数据库安全漏洞测试（数据库管理系统本身安全漏洞扫描和安全检测，如数据库连接管道协议漏洞检测）	补丁安装
9	服务器当前服务	专用中间件账户（如存在）口令强度测试（空口令检测、弱口令检测）	配置修改

序号	评估对象	评估项要求	备注
10	服务器当前服务	专用中间件账户（如存在）身份认证测试（合法用户身份检测、非法用户身份绕过检测）	配置修改
11	服务器当前服务	专用中间件账户（如存在）访问控制测试（普通中间件用户身份访问非授权资源检测）	配置修改
12	服务器当前服务	中间件安全漏洞测试（中间件本身安全漏洞扫描和安全检测，如中间件运行所需服务的漏洞缺陷检测）	补丁安装
13	服务器当前服务	系统组件账户口令强度测试（空口令检测、弱口令检测）	配置修改
14	服务器当前服务	系统组件账户身份认证测试（合法用户身份检测、非法用户身份绕过检测）	配置修改
15	服务器当前服务	系统组件账户访问控制测试（普通用户身份访问非授权资源检测）	配置修改
16	服务器当前服务	系统组件安全漏洞测试（系统组件本身安全漏洞扫描和安全检测）	补丁安装

6.4.2 评估方法

通过使用脆弱性扫描工具，扫描主机是否存在脆弱性风险。

6.4.3 通过评估要求

a) 漏洞的风险级别由脆弱性扫描工具判定；脆弱性扫描工具输出的结果存在偏差时，由评估人员根据实际情况并参考 GB/T 20984 进行综合研判。

b) 不存在会带来实质性安全风险的中危、高危漏洞。

6.5 恶意代码检查

6.5.1 评估对象及内容

针对待上线的系统开展恶意代码检查，避免存在 Webshell 等恶意文件。

6.5.2 评估方法

通过使用终端安全扫描软件或恶意软件扫描脚本对应用目录扫描，判断是否存在恶意代码。

6.5.3 通过评估要求

不存在恶意代码文件。

7 通过评估要求

政务应用系统分别满足本指引6.2至6.5章节各环节通过评估要求，经综合分析不存在可能带来高等及以上级别实质性安全风险的问题，可通过评估。

此外，以下情况按不通过评估处理：

a) 系统已完成首轮评估，由于建设单位原因系统不再需要上线，经与相关各方确认后，按不通过处理；

b) 安全问题整改阶段，系统超过 15 个工作日未完成整改且未申请延长整改时间的，或申请延长整改时间但累计超过 25 个工作日未完成整改的，按不通过处理。

c) 系统经一次回归评估后，评估仍不通过的，按不通过处理。

政务应用系统未通过上线前风险评估的，政务应用系统建设单位需完成整改后重提评估申请。同一政务应用系统第二次申请上线前风险评估而仍未通过的，政务应用系统建设单位或将被通报。

附 录 A

（资料性）

评估对象选择示例

表 B.1 规定了传统系统的评估对象。

表 B.1 传统系统的评估对象

序号	评估对象	类型版本
1	服务器操作系统	Centos-7.3
2	数据库系统	DM-8
3	中间件系统	Tomcat-9
4	应用系统	Https://xxx
5	数据安全及备份恢复策略	/

表 B.2 规定了容器化部署系统（服务器归属系统所属单位）的评估对象。

表 B.2 容器化部署系统（服务器归属系统所属单位）的评估对象

序号	评估对象	类型版本
1	服务器操作系统	Centos-7.3
2	数据库系统	DM-8
3	中间件系统	Tomcat-9
4	应用系统	Https://xxx
5	数据安全及备份恢复策略	/

表 B.3 规定了容器化部署系统（系统所属单位无服务器）的评估对象。

表 B.3 容器化部署系统（系统所属单位无服务器）的评估对象

序号	评估对象	类型版本
1	数据库系统	DM-8
2	中间件系统	Tomcat-9
3	应用系统	Https://xxx
4	数据安全及备份恢复策略	/

表 B.4 规定了涉及大量第三方组件的系统的评估对象

表 B.4 涉及大量第三方组件的系统的评估对象

序号	评估对象	类型版本
1	服务器操作系统	Centos-7.3
2	数据库系统 1	DM-8
3	数据库系统 2	Mysql-8
4	中间件系统 1	Tomcat-9
5	中间件系统 2	Nginx-21
6	应用系统 1	Https://xxx
7	应用系统 2	Https://xxx
8	数据安全及备份恢复策略	/

为业务应用系统提供业务数据存储的数据库系统、部署业务应用系统或者代理业务应用系统的中间件系统、提供系统业务功能的自研系统或第三方组件均为评估对象。

附 录 B

（资料性）

调研表示例

序号	组件名称	组件类型及版本	关联资产	用途	IP/URL	登录信息	备注
1	前端应用服务器操作系统	windows server 2008r2	前端应用服务器	部署业务应用系统前端	业务弹性 IP	RDP:63333 管理员用户名： 密码：	需提供管理员权限的账户密码
2	后台应用服务器操作系统	centos-7.3	后台应用服务器	部署业务应用系统后台	业务弹性 IP	SSH:22 管理员用户名： 密码：	需提供管理员权限的账户密码 若限制管理员直接登录 ssh，需提供可登录的账户密码、管理员账户密码
3	数据库服务器操作系统	centos-7.3	数据库服务器	部署数据库系统	业务弹性 IP	SSH:22 管理员用户名： 密码：	
4	数据库系统	tdsql	/	云平台数据库服务	业务弹性 IP	端口： 用户名：root@% 密码：mysqlpass	使用的数据库实例： 存储用户身份鉴别信息的表：
5	数据库系统 1	mysql-5.5	数据库服务器	业务应用系统数据库	业务弹性 IP	端口： 数据库管理员用户名：root@% 密码：mysqlpass 应用账户(应用系统用来连接数据库那个)用户名： 密码：	需提供管理员账户、应用账户（应用系统用来连接数据库那个） 配置文件路径： 使用的库： 存储用户身份鉴别信息的表：
6	数据库系统 3	redis-版本	数据库服务器	缓存数据	业务弹性 IP	端口： 密码：	配置文件路径： 是否存储用户身份鉴别信息或其他较敏感信息：

7	前端应用中间件系统	nginx-1.19.0	前端应用服务器	部署业务应用系统前端	业务弹性 IP	/	部署路径：
8	后台应用中间件系统	tomcat-7.0.3	后台应用服务器	部署业务应用系统后台	业务弹性 IP	/	部署路径： 配置文件路径： 如果是内嵌，未有实际部署的则说明是否是 jar 包启动
9	中间件系统 2	weblogic-版本	后台应用服务器	部署应用	业务弹性 IP	控制台：url 控制台管理员账户密码：	部署路径： 配置文件路径：
10	XXX 系统	应用系统当前提测版本	前端应用服务器	业务应用系统前端	http://19.15.x.12/web/index.aspx	管理员：admin；密码：admin@123 普通用户：user；密码 user@123 至少提供管理员和普通权限账户 若无，则根据系统实际情况说明。	应用系统部署路径： 前端：服务器业务弹性 IP+服务器中的具体路径 后端：服务器业务弹性 IP+服务器中的具体路径 若不分前后端部署，说明即可。 若是通过域名访问，需提供域名对应的业务弹性地址
11	XXX 系统后台管理系统	应用系统当前提测版本	后台应用服务器	业务应用系统后台	http://19.15.x.13:8080/portal.jsp	管理员：admin；密码：admin@123 普通用户：user；密码 user@123 至少提供管理员和普通权限账户 若无，则根据系统实际情况说明。	应用系统部署路径： 前端：服务器业务弹性 IP+服务器中的具体路径 后端：服务器业务弹性 IP+服务器中的具体路径 若不分前后端部署，说明即可。

							若是通过域名访问，需提供域名对应的业务弹性地址
12	xx app	应用系统当前提测版本	/	用途	提供安装包	用户 1 账号密码： 用户 2 账号密码：	提供 app 代码包 提供后台接口 url
13	xx 小程序	应用系统当前提测版本	/	用途	提供小程序	用户 1 账号密码： 用户 2 账号密码：	提供小程序代码包 提供后台接口 url

附　录　C

（资料性）

评估报告模板

C.1 上线前风险评估报告封面

[单位名称_TAG]
[被评估系统_TAG]
上线前风险评估报告

[受托单位_TAG]

[报告日_TAG]

C.2上线前风险评估报告声明模板

声　明

1. 本评估报告仅适用于[委托单位_TAG]委托[受托单位_TAG]针对[单位名称_TAG][被评估系统_TAG]开展的上线前风险评估工作。
2. 本评估报告结论的有效性建立在本次评估工作所使用评估环境的真实性基础上。
3. 本评估报告中给出的评估结论仅对被评估信息系统当时的安全状态及部署环境有效。当评估工作完成后，若信息系统状态发生变化，则本报告不再适用。
4. 本评估报告中给出的评估结论不能作为对信息系统内部署的相关系统构成组件（或产品）安全性的评估结论。
5. 在任何情况下，若需引用本报告中的评估结果或结论，都应保持其原有的意义，不得对相关内容擅自进行增加、修改、伪造或掩盖事实。
6. 本报告的结论，仅表明该系统达到了上线前的安全要求，并不保证该系统是绝对安全的。
7. 本评估报告涂改无效。
8. 未经书面同意不得部分复制本报告。
9. 本报告不具有社会证明作用。

C.3 评估结论模板

<table>
<tr><th colspan="2">评 估 结 论</th></tr>
<tr><td>评 估 对 象</td><td>[被评估系统_TAG]</td></tr>
<tr><td>评 估 对 象
责 任 单 位</td><td>[单位名称_TAG]</td></tr>
<tr><td>评 估 时 间</td><td>[调研日_TAG] 至 [报告日_TAG]</td></tr>
<tr><td>评 估 地 点</td><td>[评估地点_TAG]</td></tr>
<tr><td>评 估 人 员</td><td>[评估人员_TAG]</td></tr>
<tr><td>评 估 结 果</td><td>本次上线前风险评估进行了首轮和回归两轮评估，每轮评估分为配置核查、渗透测试、漏洞扫描和恶意代码扫描四个环节。
配置核查环节首轮评估、回归评估结果如下：
➢ 首轮评估中发现 x 个高风险项、x 个中风险项、x 个低风险项，共计 x 个问题项；
➢ 回归评估后，首轮评估中发现的高风险项已全部修复，首轮评估中发现的 x 个中风险项中 x 个已修复，遗留 x 个中风险项；首轮评估中发现的 x 个低风险项中 x 个已修复，遗留 x 个低风险项；共计遗留 x 个问题项。
渗透测试环节首轮评估、回归评估结果如下：
➢ 首轮评估中未发现超危、中危、低危漏洞，发现 x 个高危漏洞，共计 x 个安全漏洞；
➢ 回归评估后安全漏洞均已修复。
漏洞扫描环节首轮评估、回归评估结果如下：
➢ 首轮评估中未发现超危漏洞，发现 x 个高危、x 个中危、x 个低危漏洞，共计 x 个安全漏洞；
➢ 回归评估后遗留 x 个低危漏洞。
恶意代码扫描环节首轮评估、回归评估结果如下：
➢ 首轮评估中未发现恶意代码；
➢ 回归评估中未发现恶意代码。

目前该系统仍存在 x 个中风险项、x 个低风险项、x 个低危漏洞，未发现恶意代码，经分析确认，这些风险项或漏洞不会导致信息系统面临高等级安全风险。</td></tr>
<tr><td>评 估 结 论</td><td>通过</td></tr>
</table>

C.4系统上线前风险评估报告主要内容

1、范围
1.1 标识
说明报告的标识号。
1.2 文档概述
说明文档的主要用途以及主要内容。
1.3 评估工作概述
说明本次评估的委托方与被委托方，以及被评估单位、系统名称等信息。
1.4 被评估系统概述
描述被评估系统相关情况。
1.4.1 基本情况
描述被评估系统基本情况。
1.4.2 网络拓扑
被评估系统的网络拓扑示意图。
1.4.3 资产清单
被评估系统资产列表。
2、评估依据
本次评估涉及的评估依据。
3、评估过程
3.1 评估内容
本次评估内容以及通过标准。
3.1.1 配置核查
配置核查所涉及的评估内容及方式。
3.1.2 渗透测试
渗透测试所涉及的评估内容及方式。
3.1.3 漏洞扫描
漏扫扫描所涉及的评估内容及方式。
3.1.4 恶意代码扫描
恶意代码扫描所涉及的评估内容及方式。
3.2 评估对象
描述评估对象的选择原则，描述评估对象和评估范围。
3.3 评估环境
描述本次评估所使用的环境。
3.4 评估设计
描述各评估内容的评估项。
3.5 评估实施过程
说明本次评估工作的时间进度安排，描述各阶段评估工作等内容。
3.5.1 系统调研
3.5.2 首轮评估
3.5.3 安全问题整改
3.5.4 回归评估

3.5.5 评估总结与报告编制
4、评估结果
本次评估工作各评估内容的评估结果展示。
4.1 配置核查结果详情
4.1.1 服务器操作系统配置核查
4.1.2 数据库系统配置核查
4.1.3 中间件系统配置核查
4.1.4 业务应用系统配置核查
4.1.5 数据安全及备份恢复配置核查
4.2 渗透测试结果详情
4.3 漏洞扫描结果详情
4.4 恶意代码扫描结果详情
5、安全风险及建议
针对本报告第 4 章发现的问题隐患，进行风险评价，提出整改建议。
5.1 安全风险
5.2 安全建议

参考文献

GB/T 20984-2022 信息安全技术 信息安全风险评估方法
GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
GB/T 20269-2006 信息安全技术 信息系统安全管理要求
GB/T 22080-2016 信息技术 安全技术 信息安全管理体系要求
GB/T 24364-2023 信息安全技术 信息安全风险管理实施指南
GB/T 28453-2012 信息安全技术 信息系统安全管理评估要求