安全风险评估报告

系统名称： xxxxxxxxxxx

评估单位： xxxxxxxxxxxxxxxxxxxx

评估时间：　　年　　月　　日

目　录

1. 威胁识别与分析

1.1. 关键资产安全需求

资产类别	重要资产名称	重要性程度（重要等级）	资产重要性说明	安全需求
	光纤交换机 Brocade 300	非常重要（5）	保证 xxxx 系统数据正常传输到磁盘阵列的设备。	可用性-系统可用性是必需的，价值非常高；保证各项系统数据正常传输到磁盘阵列。
				完整性-完整性价值非常关键，除管理员外其他任何用户不能修改数据。
				保密性-包含组织的重要秘密，泄露将会造成严重损害。
				完整性-完整性价值非常关键，除管理员外其他任何用户不能修改数据。
				保密性-包含组织的重要秘密，泄露将会造成严重损害。
				保密性-包含组织的重要秘密，泄露将会造成严重损害。

资产类别	重要资产名称	重要性程度（重要等级）	资产重要性说明	安全需求
				保密性-包含组织的重要秘密，泄露将会造成严重损害。
				保密性-包含组织的重要秘密，泄露将会造成严重损害。
存储设备	磁盘阵列 HP EVA4400	非常重要（5）	xxxx 系统数据存储设备。	可用性-系统可用性是必需的，价值非常高；保证 xxxx 系统数据存储功能持续正常运行。
				完整性-完整性价值非常关键，除管理员外其他任何用户不能修改数据。
				保密性-包含组织的重要秘密，泄露将会造成严重损害。
保障设备	UPS 电源 SANTAK 3C3 EX 30KS	重要（4）	机房电力保障的重要设备。	可用性-系统可用性价值较高；保证 xxxx 系统供电工作正常。
				完整性-完整性价值较高；除授权人员外其他任何用户不能修改数据。

资产类别	重要资产名称	重要性程度（重要等级）	资产重要性说明	安全需求
				保密性-包含组织内部可公开的信息，泄露将会造成轻微损害。
				完整性-完整性价值较高，除授权人员外其他任何用户不能修改数据。
				保密性-包含组织的重要秘密，泄露将会造成严重损害。
	金农一期业务系统	4（高）	部署在应用服务器上。 任何用户	可用性-系统可用性价值较高；保证 xxxx 数据正常采集。
				完整性-完整性价值较高，除授权人员外其他不能修改数据。
				保密性-包含组织的重要秘密，泄露将会造成严重损害。
	备份管理软件 Symantec Backup	重要（4）	xxxx 系统数据备份管理软件。	可用性-系统可用性价值较高；保证 xxxx 系统数据备份管理功能正常运行。

资产类别	重要资产名称	重要性程度（重要等级）	资产重要性说明	安全需求
				完整性-完整性价值较高，除授权人员外其他任何用户不能修改数据。
				保密性-包含组织的重要秘密，泄露将会造成严重损害。
	内容管理软件 WCM-MUL-V60 网站群版	重要（4）	用户数据采编。	可用性-系统可用性价值较高；保证 xxxx 系统数据的采编。
				完整性-完整性价值较高，除授权人员外其他任何用户不能修改数据。
				保密性-包含组织的重要秘密，泄露将会造成严重损害。
数据	xxxx 系统数据	非常重要（5）	xxxx 系统的核心数据。	可用性-系统可用性是必需的，价值非常高；保证 xxxx 系统的核心数据能够正常读取及使用。
				完整性-完整性价值非常关键，除管理员外其他任何用户不能修改数据。

资产类别	重要资产名称	重要性程度（重要等级）	资产重要性说明	安全需求
				保密性-包含组织的重要秘密，泄露将会造成严重损害。

1.1. 关键资产威胁概要

威胁是一种客观存在的，对组织及其资产构成潜在破坏的可能性因素，通过对“xxxxxxxxxxxxxxxxxxx 信息系统”关键资产进行调查，对威胁来源（内部/外部；主观/不可抗力等）、威胁方式、发生的可能性等进行分析，如下表所示：

关键资产名称	威胁类型	关注范围
核心交换机 Quidway S3300 Series	操作失误（维护错误、操作失误）	维护人员操作不当，导致交换机服务异常或中断，导致金农一期系统无法正常使用。
	社会工程（社会工程学破解）	流行的免费下载软件中捆绑流氓软件、免费音乐中包含病毒、网络钓鱼、垃圾电子邮件中包括间谍软件等，引起系统安全问题。
	物理破坏（断电、消防、盗窃和破坏）	物理断电导致关键设备停止工作，服务中断。
		火灾隐患威胁系统正常运行。

关键资产名称	威胁类型	关注范围
	滥用授权（非授权访问网络资源、滥用权限非正常修改系统配置或数据）	管理地址未与特定主机进行绑定，可导致非授权人员访问核心交换机，修改系统配置或数据，造成网络中断。
	意外故障（设备硬件故障、传输设备故障）	硬件故障、传输设备故障，可能导致整个中心机房网络中断，造成业务应用无法正常运行。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。
光纤交换机 Brocade 300	操作失误（维护错误、操作失误）	维护人员操作不当，导致交换机服务异常或中断，导致金农一期数据无法正常保存到磁盘阵列。
	物理破坏（断电、消防、盗窃和破坏）	物理断电导致关键设备停止工作，服务中断。
		火灾隐患威胁系统正常运行。
	滥用授权（非授权访问网络资源、滥用权限非正常修改系统配置或数据）	管理地址未与特定主机进行绑定，可导致非授权人员访问光纤交换机，修改系统配置或数据，造成数据存储任务失败。
	意外故障（设备硬件故障、传输设备故障）	硬件故障、传输设备故障，可能导致磁盘阵列无法连

关键资产名称	威胁类型	关注范围
		接到网络，造成数据存储失败。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。
电信接入交换机 Quidway S3300 Series	操作失误（维护错误、操作失误）	维护人员操作不当，导致交换机服务异常或中断，导致金农一期系统无法通过互联网访问。
	物理破坏（断电、消防、盗窃和破坏）	物理断电导致关键设备停止工作，服务中断。
		火灾隐患威胁系统正常运行。
	滥用授权（非授权访问网络资源、滥用权限非正常修改系统配置或数据）	管理地址未与特定主机进行绑定，可导致非授权人员访问电信接入交换机，修改系统配置或数据，造成网络中断。
	意外故障（设备硬件故障、传输设备故障）	设备硬件故障、传输设备故障，可能导致所有终端的网络传输中断，影响各办公室用户接入网络。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。
电信出口路由器	操作失误（维护错误、操作失	维护人员操作不当，导致出

关键资产名称	威胁类型	关注范围
	误）	口路由器服务异常或中断，影响地市州访问金农一期系统。
	物理破坏（断电、消防、盗窃和破坏）	物理断电导致关键设备停止工作，服务中断。
		火灾隐患威胁系统正常运行。
	滥用授权（非授权访问网络资源、滥用权限非正常修改系统配置或数据）	管理地址未与特定主机进行绑定，可导致非授权人员访问电信出口路由器，修改系统配置或数据，造成互联网通信线路中断。
	意外故障（设备硬件故障、传输设备故障）	设备硬件故障、传输设备故障，可能导致所有终端的网络无法接入互联网。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。
数据库服务器	漏洞利用（利用漏洞窃取信息、利用漏洞破坏信息、利用漏洞破坏系统）	非法入侵者利用漏洞侵入系统篡改或破坏，可能导致数据不可用或完整性丢失。
		系统漏洞导致信息丢失、信息破坏、系统破坏，服务不可用。
	恶意代码（病毒、木马、间谍软件、窃听软件）	系统可能受到病毒、木马、间谍软件、窃听软件的影响。

关键资产名称	威胁类型	关注范围
	物理破坏（断电、消防、盗窃和破坏）	物理断电导致关键设备停止工作，服务中断。
		火灾隐患威胁系统正常运行。
	意外故障（设备硬件故障）	硬件及系统故障导致系统不可用，服务中断。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。
数据库备份服务器	漏洞利用（利用漏洞窃取信息、利用漏洞破坏信息、利用漏洞破坏系统）	非法入侵者利用漏洞侵入系统篡改或破坏，可能导致备份数据不可用或完整性丢失。
	恶意代码（病毒、木马、间谍软件、窃听软件）	系统可能受到病毒、木马、间谍软件、窃听软件的影响。
	物理破坏（断电、消防、盗窃和破坏）	物理断电导致关键设备停止工作，数据备份服务中断。
		火灾隐患威胁系统正常运行。
	意外故障（设备硬件故障）	服务器系统本身软硬件故障导致数据备份不可用。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。

关键资产名称	威胁类型	关注范围
业务应用服务器	漏洞利用（利用漏洞窃取信息、利用漏洞破坏信息、利用漏洞破坏系统）	非法入侵者利用漏洞侵入系统篡改或破坏，可能导致系统业务中断。
		入侵者利用系统漏洞攻击系统，导致服务中断。
	恶意代码（病毒、木马、间谍软件、窃听软件）	系统可能受到病毒、木马、间谍软件、窃听软件的影响。
	物理破坏（断电、消防、盗窃和破坏）	物理断电导致关键设备停止工作，服务中断。
		火灾隐患威胁系统正常运行。
	意外故障（设备硬件故障、应用软件故障）	硬件及系统故障导致系统不可用，服务中断。
		应用软件故障导致服务中断。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。
部级下发服务器	漏洞利用（利用漏洞窃取信息、利用漏洞破坏信息、利用漏洞破坏系统）	非法入侵者利用漏洞侵入系统篡改或破坏，可能导致下发数据丢失。
		入侵者利用系统漏洞攻击系统，导致部级数据无法接收。
	恶意代码（病毒、木马、间谍软件、窃听软件）	系统可能受到病毒、木马、间谍软件、窃听软件的影

关键资产名称	威胁类型	关注范围
		响。
	物理破坏（断电、消防、盗窃和破坏）	物理断电导致关键设备停止工作，部级数据无法接收。
		火灾隐患威胁系统正常运行。
	意外故障（设备硬件故障、应用软件故障）	硬件及系统故障导致系统不可用，部级数据无法接收。
		应用软件故障导致部级数据无法接收。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。
数据采集前置机	漏洞利用（利用漏洞窃取信息、利用漏洞破坏信息、利用漏洞破坏系统）	非法入侵者利用漏洞侵入系统篡改或破坏，可能导致数据不可用或完整性丢失。
		系统来宾帐号密码为空，具有一定安全风险。
	恶意代码（病毒、木马、间谍软件、窃听软件）	系统可能受到病毒、木马、间谍软件、窃听软件的影响。
	物理破坏（断电、消防、盗窃和破坏）	物理断电导致关键设备停止工作，服务中断。
		火灾隐患威胁系统正常运行。
	意外故障（设备硬件故障、应	硬件及系统故障导致系统

关键资产名称	威胁类型	关注范围
	用软件故障）	不可用，服务中断。
		应用软件故障导致服务不可用。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。
应用支撑平台服务器	漏洞利用（利用漏洞窃取信息、利用漏洞破坏信息、利用漏洞破坏系统）	非法入侵者利用漏洞侵入系统篡改或破坏，可能导致数据不可用或完整性丢失。
		入侵者利用系统漏洞攻击系统，导致服务中断。
	恶意代码（病毒、木马、间谍软件、窃听软件）	系统可能受到病毒、木马、间谍软件、窃听软件的影响。
	物理破坏（断电、消防、盗窃和破坏）	物理断电导致关键设备停止工作，服务中断。
		火灾隐患威胁系统正常运行。
	意外故障（设备硬件故障、应用软件故障）	硬件及系统故障导致系统不可用，服务中断。
		应用软件故障导致服务中断。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。
	管理不到位（管理制度和策略	安全管理制度不完善，策略

关键资产名称	威胁类型	关注范围
	不完善、管理规程遗失、职责不明确、监督控管机制不健全）	执行无序，造成安全监管漏洞和缺失。
磁盘阵列 HP EVA4400	物理破坏（断电、消防、盗窃和破坏）	物理断电导致关键设备停止工作，服务中断。
		火灾隐患威胁系统正常运行。
	意外故障（设备硬件故障、存储媒体故障）	硬件故障，可能导致征金农一期业务数据的错误、异常、丢失，进而导致所有业务中断。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。
UPS 电源 SANTAK 3C3 EX 30KS	操作失误（无作为）	UPS 若损坏，该设备功能失效。
	电源中断（备用电源中断）	电源中断导致 UPS 停止工作，无法正常储备电源。
	意外故障（设备硬件故障）	硬件故障，遇到机房供电问题，导致应用服务中断。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞。
		UPS 无专人对其定期进行充放电操作，可导致 UPS 能效降低。
千兆防火墙	操作失误（操作失误）	千兆防火墙配置管理由外

关键资产名称	威胁类型	关注范围
绿 盟 SG1200Series		包公司维护，当系统发生故障时，系统恢复不可控，易引发操作失误。
	社会工程（社会工程学破解）	流行的免费下载软件中捆绑流氓软件、免费音乐中包含病毒、网络钓鱼、垃圾电子邮件中包括间谍软件等，引起系统安全问题。
	物理破坏（断电、消防、盗窃和破坏）	物理断电导致设备停止工作。
		火灾隐患威胁系统正常运行。
	滥用授权（非授权访问网络资源、滥用权限非正常修改系统配置或数据）	管理地址未与特定主机进行绑定，可导致非授权人员访问防火墙。
		管理地址未与特定主机进行绑定，可导致非授权人员修改系统配置或数据，造成网络中断。
	意外故障（设备硬件故障、传输设备故障）	硬件故障、传输故障，可能导致中心机房与互联网的通信中断，或中心机房与电子政务外网的通信中断，或网络边界安全防护服务功能丧失，造成中心机房各服务器和业务数据的安全威胁。
	管理不到位（管理制度和策略	安全管理制度不完善，策略

关键资产名称	威胁类型	关注范围
	不完善、管理规程遗失、职责不明确、监督控管机制不健全）	执行无序，造成安全监管漏洞和缺失。
IDS 入侵检测系统 绿 盟 NIDS1200Series	操作失误（维护错误、操作失误）	设备管理由外包公司维护，当系统发生故障时，系统恢复不可控，易引发操作失误。
	物理破坏（断电、消防、盗窃和破坏）	物理断电导致设备停止工作。
		火灾隐患威胁系统正常运行。
	滥用授权（非授权访问网络资源、滥用权限非正常修改系统配置或数据）	管理地址未与特定主机进行绑定，可导致非授权人员访问 IDS。
		管理地址未与特定主机进行绑定，可导致非授权人员修改系统配置或数据。
	意外故障（设备硬件故障）	硬件故障，可能导致 IDS 无法正常使用，无法监控网络中的入侵和攻击行为。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。
入侵防护系统 绿盟 NIPS 1000 Series	操作失误（操作失误）	设备管理由外包公司维护，当系统发生故障时，系统恢复不可控，易引发操作失误。

关键资产名称	威胁类型	关注范围
	物理破坏（断电、消防、盗窃和破坏）	物理断电导致设备停止工作。
		火灾隐患威胁系统正常运行。
	滥用授权（非授权访问网络资源、滥用权限非正常修改系统配置或数据）	管理地址未与特定主机进行绑定，可导致非授权人员访问应用安全管理系统。
		管理地址未与特定主机进行绑定，可导致非授权人员修改系统配置或数据。
	意外故障（设备硬件故障）	硬件故障，可能导致入侵防护系统无法正常使用，无法防御网络入侵。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。
SQL Server2008 标准版	操作失误（操作失误）	数据库管理由外包公司维护，当系统发生故障时，系统恢复不可控，易引发操作失误。
	意外故障（数据库软件故障）	数据库软件故障，可导致系统的核心数据严重损失。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。

关键资产名称	威胁类型	关注范围
金农一期应用系统		系统具备数据备份与恢复机制，但应加强管理，以备恢复使用。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，造成安全监管漏洞和缺失。
	操作失误（维护错误、操作失误）	系统软件可能在维护中出现错误。
	身份假冒（用户身份伪装和欺骗）	身份被冒用，产生欺骗行为。
	口令攻击（嗅探口令、暴力破解）	对互联网用户发布，可能遭到口令攻击，如口令嗅探和暴力破解。
	社会工程（社会工程学破解）	流行的免费下载软件中捆绑流氓软件、免费音乐中包含病毒、网络钓鱼、垃圾电子邮件中包括间谍软件等，引起系统安全问题。
	意外故障（应用软件故障）	软件故障，可能导致 xxxx 业务无法正常使用。
	管理不到位（管理制度和策略不完善、管理规程遗失、职责不明确、监督控管机制不健全）	安全管理制度不完善，策略执行无序，无相关记录，造成安全监管漏洞和缺失。

1.2. 威胁描述汇总

威胁种类	威胁子类	存在的威胁描述	影响（完整性修改、机密性暴露、可用性遗失描述）	威胁发生频率（很高5/高4/中3/低2/很低1）	作用对象
	利用漏洞破坏信息	系统数据易通过漏洞被破坏。	数据库遭受网络攻击，如数据完整性被修改，可能会发生安全事件。	4（高）	数据库服务器、数据库备份服务器、业务应用服务器、部级下发服务器、数据采集前置机、应用支撑平台服务器。

威胁种类	威胁子类	存在的威胁描述	影响（完整性修改、机密性暴露、可用性遗失描述）	威胁发生频率（很高5/高4/中3/低2/很低1）	作用对象
	利用漏洞破坏系统	系统数据易通过漏洞被破坏。	服务器遭受网络攻击，可能使内部网络、服务器设施的因攻击而产生通信中断故障或安全服务中断，从而导致可用性遗失。	4（高）	数据库服务器、数据库备份服务器、业务应用服务器、部级下发服务器、数据采集前置机、应用支撑平台服务器。
	管理规程缺失	管理规程缺失，易造成安全监管漏洞。	管理规程存在缺陷，可能导致针对关键资产的日常运维管理方面出现漏洞。	3（中）	所有资产

威胁种类	威胁子类	存在的威胁描述	影响（完整性修改、机密性暴露、可用性遗失描述）	威胁发生频率（很高5/高4/中3/低2/很低1）	作用对象
	职责不明确	职责不明确，易造成安全监管漏洞。	职责不明确，可导致安全监管漏洞。	3（中）	所有资产
	监督控管机制不健全	监督控管机制不健全，易造成安全监管漏洞。	监督控管机制等方面存在缺陷，导致完整性或可用性的遗失。	3（中）	所有资产

1.1. 威胁赋值

资产名称	威胁																	
	操作失误	滥用授权	行为抵赖	身份假冒	口令攻击	密码分析	漏洞利用	拒绝服务	恶意代码	窃取数据	物理破坏	社会工程	意外故障	通信中断	数据受损	电源中断	灾害	管理不到位	越权使用
核心交换机	2	4									2	4	4					3	
光纤交换机	2	4									2		4					3	
电信接入交换机	2	4									2		4					3	

资产名称	威胁																	
	操作失误	滥用授权	行为抵赖	身份假冒	口令攻击	密码分析	漏洞利用	拒绝服务	恶意代码	窃取数据	物理破坏	社会工程	意外故障	通信中断	数据受损	电源中断	灾害	管理不到位	越权使用
电信出口路由器	2	4									2		4					3	
数据库服务器							4		2		2		4					3	
数据库备份服务器							4		2		2		4					3	
业务应用服务器							4		2		2		4					3	
部级下发服务器							4		2		2		4					3	
数据采集前置机							4		2		2		4					3	
应用支撑平台服务器							4		2		2		4					3	
磁盘阵列											2		4					3	
UPS 电源	2												4				2	3	
千兆防火墙	2	4									2	4	4					3	
IDS 入侵检测系统	2	4									2		4					3	
入侵防护系统	2	4									2		4					3	
SQL Server2008	2												2					3	

资产名称	威胁																	
	操作失误	滥用授权	行为抵赖	身份假冒	口令攻击	密码分析	漏洞利用	拒绝服务	恶意代码	窃取数据	物理破坏	社会工程	意外故障	通信中断	数据受损	电源中断	灾害	管理不到位	越权使用
备份管理软 件	2												2					3	
内容管理软件 WCM-MUL-V60 网站群版	2												2					3	
xxxx 系统数据	4														2			3	
金农一期业务系统	4			3	4							4	3					3	