四川科道芯国智能技术股份有限公司

Sichuan Keydom Smart Technology Co., Ltd

标准文件

Standard File

批注 [u1]: 科道芯国 官网上并没有明确给出公司的英文名称。
我们在官网【对外生产与制造】版块找到至少两种不同的说法：
1. Sichuan precision intelligent technology Limited by Share Ltd
此为官网【质量管理】版块的译法。
2. Jing King Technology Holdings Ltd.
此为官网【资质】版块的译法。

但是这两种说法都与科道芯国的商标“KEYDOM”不相符，所以无法确定该公司的正式英文名称，暂时以商标为准，译为：Sichuan Keydom Smart Technology Co., Ltd

安全风险管理标准

Security Risk Management Standard

文 件 编 号: KD-MFX-01

Doc. No.:

编 制:

Prepared by:

审 核:

Reviewed by:

批 准:

Approved by:

版本 /修订状态: A 1

Rev./Revision status:

受 控 状 态:

Controlled status:

2020 年 1 月 1 日发布 **2020 年 1 月 1 日实施**

Issued on 1 / 1 /2020 **Implemented on 1 / 1 /2020**

修订历史记录 Document Changes

序号 No.	日期 Date	修订内容 Description of Change	版本 Version	编制 Made by	审核 Reviewed by	批准 Approved by
01	2019.9.2	初版制定 First edition	A 0	付显兰	刘劲松	陈为明
02	2019.12.29	更改文件格式	A1	付显兰	刘劲松	陈为明
03						
04						
05						
06						
07						
08						
09						
10						

目录 Table of Content

1. 目的 PURPOSE 6

2. 适用范围 SCOPE 6

3. 术语定义 DEFINITION 6

3.1. 安全风险 Security Risk 6

3.2. 安全风险评估 Security Risk Evaluation 6

3.3. 安全风险管理 Security Risk Management 7

3.4. 安全风险处理 Security Risk Treatment 7

3.5. 信息资产 Info Asset 7

3.6. 信息资产价值 Info Asset Value 8

3.7. 威胁 Threat 8

3.8. 脆弱性 Vulnerability 9

3.9. 影响 Consequence 9

3.10. 可用性 Availability 9

3.11. 保密性 Confidentiality 9

3.12. 完整性 Integrity 10

3.13. 安全措施 Security Measure 10

4. 职责 RESPONSIBILITY 10

4.1. 管理者代表 Management Representative 10

4.2. 安全策略部 Security Policy Dept. 10

4.3. 其他各部门 Other Depts. 11

5. 安全风险管理框架 SECURITY RISK MANAGEMENT FRAME 11

5.1. 安全风险管理的内容和过程概述 Overview of Security Risk Management Content and

PROCESS 12

5.2. 安全风险管理的内容和过程 SECURITY RISK MANAGEMENT CONTENT AND PROCESS 12

6. 准备工作 PREPARATION WORK 14

6.1. 准备工作概述 PREPARATION WORK OVERVIEW 14

6.2. 准备工作过程 PREPARATION WORK PROCESS 15

7. 安全风险评估 SECURITY RISK EVALUATION 15

7.1. 安全风险评估的实施流程图 SECURITY RISK EVALUATION PROCESS CHART 16

7.2. 安全风险评估的准备 EVALUATION PREPARATION 16

7.3. 安全风险要素的识别 SECURITY RISK ELEMENT IDENTIFICATION 16

8. 安全风险处理 SECURITY RISK HANDLING 20

8.1. 安全风险处理过程 SECURITY RISK HANDLING PROCESS 20

8.2. 现存风险分析 EXISTING RISK ANALYSIS 21

8.3. 安全风险处理的方式 SECURITY RISK HANDLING MODE 22

9. 批准监督 APPROVAL AND SUPERVISION 24

9.1. 残余安全风险评估 RESIDUAL SECURITY RISK EVALUATION 25

9.2. 持续监督 CONTINUOUS SUPERVISION 28

10. 相关文件 RELEVANT DOCUMENTS 28

11. 相关记录 RELEVANT RECORDS 28

12. 引用相关记录 RELEVANT RECORDS QUOTED 28

1. 目的 Purpose

为防范公司经营活动中的各类安全风险，有效的识别安全风险并制订对应的整改措施，以达到确保公司可持续发展的目的，特制订本管理标准。

Specially establish this standard to prevent all the kinds of security risks, identify security risks and appropriate corrective measures and reach the goal to ensure Keydom's continual development.

2. 适用范围 Scope

本管理标准适用于四川科道的安全风险评估和管理。

This standard is applicable for security risk evaluation and mgt. of Keydom.

3. 术语定义 Definition

3.1. 安全风险 Security Risk

公司在实现经营目标的活动中，会遇到各种不确定性安全事件，这些事件发生的概率及其影响程度是无法事先预知的，这些事件将对经营活动产生影响，从而影响公司目标实现的程度。这种在一定环境下和一定限期内客观存在的、影响企业目标实现的各种不确定性安全事件就是安全风险。

In course of business operating, uncertain security incidents may happen which will influence Keydom's normal operation and goals achievement, Keydom cannot forecast their probability and impact level. These uncertain security incidents which exist objectively in certain circumstances are Security Risk.

3.2. 安全风险评估 Security Risk Evaluation

对信息资产的保密性、完整性和可用性等安全属性进行评价的过程。识别信息资产所面临的威胁和系统存在的脆弱性，评估威胁利用脆弱性导致安全事件的可能性，和判断安全事件一旦发生对公司造成的影响。

A process to evaluate the security attributes of info asset, such as confidentiality, integrity and availability, to identify threat may face and vulnerability may exit, to assess likelihood of accident caused by vulnerability being utilized by threat and the consequence of incident.

3.3. 安全风险管理 Security Risk Management

识别、控制、消除或最小化可能影响生产经营的不确定因素的管理过程。

A process of identifying, controlling, eliminating or minimizing uncertainties that may affect production operation.

3.4. 安全风险处理 Security Risk Treatment

选择并且执行适宜的措施来降低风险的过程。

A process of selecting and executing appropriate measures to reduce the risks.

3.5. 信息资产 Info Asset

指公司内任何具有商业或交换价值的信息或资源，是安全策略保护的对象。本制度中的信息资产指：对公司有价值的知识或数据，存储或处理知识或数据的信息载体，及保障知识和数据的保密性、完整性和可用性的保障硬件。信息资产分为 5 大类：数据资产、软件资产、实物资产、人员资产及服务资产。详见《信息资产安全管理标准》内容。

It refers to all info and resource being with business or exchange value, it is the protected objective of security policies. In this standard, it refers to the knowledge or data valuable to Keydom and their carrier and the safeguarding hardware securing their confidentiality, integrity

and availability. Info asses is divided into 5 types: data asset, software asset, physical asset, personnel asset and service asset. Please refer to Info. Asset Security Mgt. Standard for more details.

3.6. 信息资产价值 Info Asset Value

信息资产的重要程度或敏感程度的表征。资产价值是资产的属性，也是进行资产识别的主要属性。价值不仅仅是以资产的经济价值来衡量，而是取决于，资产在保密性、完整性、可用性这三个安全属性上的完善程度，或者其安全属性不满足时所造成的影响程度。It represent the level of importance and sensitivity of assets. Asset Value is a feature of asset which can be the main feature to identify assets. Not only can economic value determine its value, but it also be determined by the level of perfection of security features (confidentiality, integrity and usability). At same time, consequence resulted from failure of security feature implementation will also be an important element to determine asset value.

3.7. 威胁 Threat

可能对系统/经营活动等产生损失、负面影响的事件的，潜在起因、活动、环节。可以通俗的理解为，围绕某个信息资产发生的一系列会导致损失的活动、因素等。

It refers to potential origin, activities and processes may cause incidents which will generate damage and adverse impact to systems and operations. Popularly, it could be understood as all activities and elements occurring around one info asset which are able to lead loose.

通常一个信息资产上，会有多种威胁，在评估时需要列出各种威胁。

There will be many threats to one info asset. Al possible threats should be identified when risk evaluation.

3.8. 脆弱性 Vulnerability

可能被威胁所利用的，资产或管理体系的薄弱环节，针对某一威胁，当前控制措施的有效性，通常也反映某威胁发生的可能性。

It refers a vulnerable spot which may be utilized by some threat. For someone threat, the effectiveness of corresponding control measures will reflect the likelihood of occurrence for some threat.

3.9. 影响 Consequence

威胁的结果，包括对企业经营活动造成的损失、伤害或负面影响。有可能一个威胁关联多种结果。

It refers to the result of threats, including the loss, damage or negative effects to company operations. One threat may be related to many results.

3.10. 可用性 Availability

数据或资源的特性，被授权实体，按要求能访问和使用数据或资源。

It is a character of data or resource which could allow the authorized entity to access as required.

3.11. 保密性 Confidentiality

数据所具有的特性，即表示数据所达到的，未提供或未泄露给非授权的个人、过程或其他实体的程度。

It is a character of data. It refers to the level of prevent from providing and disclosing to unauthorized personnel, process or other entity.

3.12. 完整性 Integrity

保证信息及信息系统不会被非授权更改或破坏的特性。包含数据完整性和系统完整性。

It refers to a character to prevent info and info system from unauthorized modification and destroy, including data integrity and system integrity.

3.13. 安全措施 Security Measure

保护资产、抵御威胁、减少脆弱性、降低安全事件影响的各种实践、规程和机制。

It refers to all the practices, standards and mechanism which protect assets, prevent threat, decrease vulnerability and consequence of security incidents.

4. 职责 Responsibility

4.1. 管理者代表 Management Representative

- 负责批准公司年度安全风险评估计划；To approve annual security risk evaluation plan;
- 负责批准公司年度安全风险评估管理报告；To approve annual security risk evaluation management report;
- 负责批准公司年度安全风险评估与总结管理计划。To approve Security risk assessment summary and mgt. plan.

4.2. 安全策略部 Security Policy Dept.

- 负责按此文件制定公司年度安全风险评估计划；To make annual security risk evaluation plan according to this standard,

- 负责组织公司内部各部门进行全面的安全风险评估；To organize other depts. of Keydom to conduct overall security risk evaluation;
- 负责依据各部门提供的安全风险评估结果，形成安全风险评估报告；To make security risk evaluation report on base of other depts.' evaluation result.
- 负责制定安全风险评估与总结管理计划，提交公司管理层批准审核；To make Security risk assessment summary and mgt. plan and submit to mgt. to review and approve.
- 负责组织各部门针对不可接受的风险，制定安全风险处置计划并评估残余风险，实施风险管理。To organize other depts. to make resolution plan for unacceptable risk of their dept., evaluate the residual risk and carry out the resolution plan.
- 负责安全风险管理过程、成本和结果的监视和控制。To monitor and control the process, cost and results of security risk management.

4. 3. 其他各部门 Other Depts.

- 负责依据公司年度风险评估计划，进行部门内部安全风险评估，提交风险评估结果。To conduct internal dept. security risk evaluation and submit evaluation result according to annual security risk evaluation plan.
- 负责针对不可接受的风险，制定风险控制措施并进行残余风险估值。To make resolution plan for unacceptable risk of their dept., evaluate the residual risk and carry out the resolution plan.
- 负责执行本部门的安全风险处置措施。Implement security risk management measures of the department.

5. 安全风险管理框架 Security Risk Management Frame

5.1. 安全风险管理的内容和过程概述 Overview of Security Risk Management Content and Process

安全风险管理包括准备工作、风险评估、风险处理、批准监督、监控审查和沟通咨询 6 个方面的内容。准备工作、风险评估、风险处理和批准监督是安全风险管理的 4 个基本步骤，监控审查和沟通咨询则贯穿于这 4 个基本步骤中，如图 1 所示。

Security risk management includes 6 aspects of preparation work, risk evaluation, risk handling, approval and supervision, monitoring and review, and communication and consultation. Preparation work, risk evaluation, risk handling, approval and supervision are the 4 basic steps of security risk management, and monitoring and review, communication and consultation run through these 4 basic steps, as shown in figure 1.

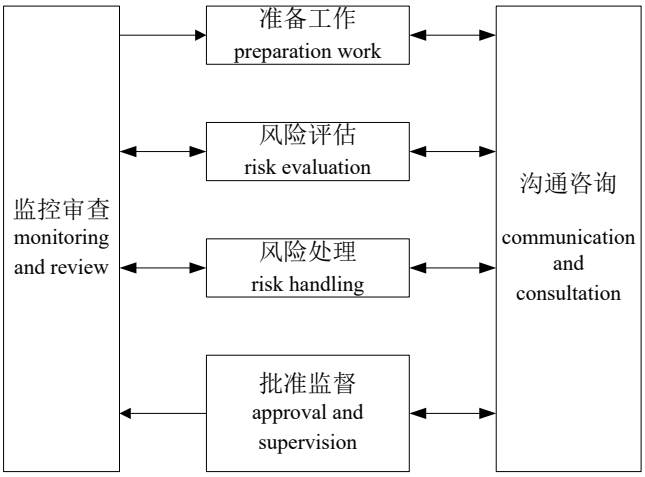


图 1 安全风险管理的内容和过程

Figure1: Security risk management content and process

5.2. 安全风险管理的内容和过程 Security Risk Management Content

and Process

第一步骤是准备工作，确定安全风险管理的对象和范围，确立实施风险管理的准备，拟订评估计划，进行相关信息的调查和分析。

The first step, preparation work, is to confirm the object and scope of the security risk management, establish the preparation for the implementation of risk management, and carry out the investigation and analysis of relevant information.

第二步骤是风险评估，针对确立的风险管理对象所面临的风险进行识别、分析和评价。

The second step, risk evaluation, is to identify, analyze and evaluate the risks faced by established risk management objects.

第三步骤是风险处理，依据风险评估的结果，选择和实施合适的安全措施。

The third step, risk handling, is to select and implement appropriate safety measures based on the results of risk evaluation.

第四步骤是批准监督，管理者代表依据风险评估和风险处理的结果是否满足安全要求，做出是否认可风险管理活动的决定。

The fourth step is approval and supervision, and the management representative will make decisions on risk management activities based on whether the results of risk evaluation and risk handling meet the security requirements.

当业务目标和特性发生变化或面临新的风险时，需要再次进入上述 4 个步骤，形成新的一次循环。

When business goals and features change or face new risks, it needs to re-enter these four steps to create a new cycle.

监控审查是对上述 4 个步骤进行监控和审查。监控是监视和控制上述 4 个步骤的过程有效性和成本适宜性；审查是跟踪系统自身或所处环境的变化，以保证上述 4 个步骤的结果有效性和符合性。

Monitoring and review is to monitor and review these four steps. Monitoring is to monitor and control the process effectiveness and cost effectiveness of the above four steps; the review is to track the changes in the system itself or the environment to ensure the effectiveness and compliance of the results of the above four steps.

沟通咨询的目的是为上述 4 个步骤的相关人员提供沟通和咨询，用以提高人员的风险意识和知识，配合实现安全目标。

Communication and consultation provide communication and consultation for relevant personnel of the above four steps to improve the risk awreness and knowledge, and to meet the security objectives.

上述 6 个步骤构成了一个往复不断的循环，使整个系统在自身和环境的变化中能够不断应对新的安全需求和风险。

These six steps constitute a spiral upward cycle that allows the whole system to constantly respond to new security requirements and risks in its own and environmental changes.

6. 准备工作 Preparation Work

6.1. 准备工作概述 Preparation Work Overview

准备工作是安全风险管理的第一步骤，确定风险管理的对象和范围，确立实施风险管理的准备，进行相关信息的调查和分析。国家、地区或行业的相关政策、法律法规和标准以及公司业务目标和特性都是准备工作的必要依据。

The preparation work is the first step of security risk management, to confirm the object and scope

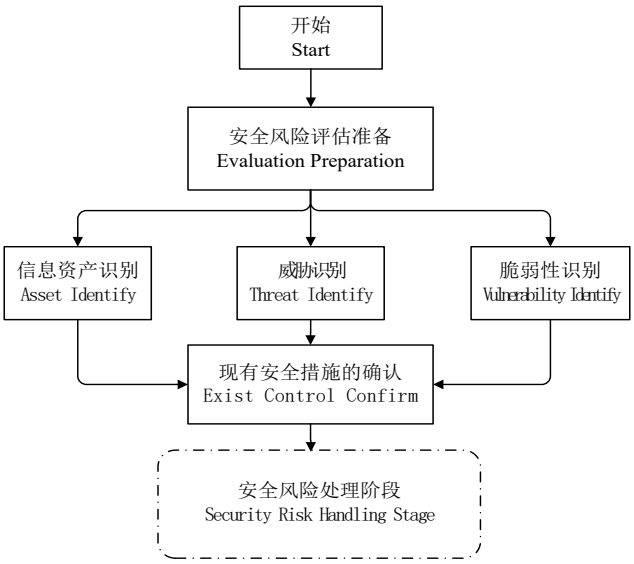
of risk management, establish the preparation for implementation of risk management, and carry out the investigation and analysis of relevant information. National, regional or industry policies, laws and regulations and standards, as well as the company's business objectives and features are neseccary grounds for preparation.

6.2. 准备工作过程 Preparation Work Process

准备工作是一次安全风险管理主循环的起始，为风险评估提供输入，监控审查和沟通咨询贯穿其 4 个阶段。准备工作的输出为《安全手册》，包括了管理方针、风险应对、管理质量目标、支持的资源、安全环境等内容。 Preparation which provides input for risk evaluation is the beginning of the main cycle of security risk management. The output of preparation work is Safety Manual, which includes management guidelines, risk response, management quality objectives, supported resources and security environment.

7. 安全风险评估 Security Risk Evaluation

7.1. 安全风险评估的实施流程图 Security Risk Evaluation Process Chart



7.2. 安全风险评估的准备 Evaluation Preparation

每年制定当年度《安全风险评估计划》，明确安全风险评估目标、范围及进度安排等内容。

Security risk evaluation plan should be made annually to specify objective, scope and schedule of security evaluation.

7.3. 安全风险要素的识别 Security Risk Element Identification

7.3.1. 信息资产识别 Info Asset Identification

信息资产识别的过程，参见《信息资产安全管理标准》。

Theprocess of info asset identification could be found in Info. Asset Security Mgt. Standard.

7.3.2. 威胁识别 Risk Identification

识别公司面临的威胁，形成威胁清单并赋值。

Identify threat Keydom facing to make threat list and evaluate value of each threat.

7.3.2.1. 威胁分类 Classification of Threat

造成威胁的因素可分为人为因素和环境因素。人为因素又可分为恶意和非恶意两种。在识别威胁时，应从如下来源进行全面的威胁识别：The reason of threat could be human factor and environmental factor. There are malicious and negligent human factors. Overall threat identification should be conducted from origins described as below:

来源 Origin		描述 Description
环境因素 Environmental factor		断电、静电、灰尘、潮湿、温度、鼠蚁虫害、洪灾、火灾、地震、意外事故等环境危害或自然灾害，以及软件、硬件、通讯线路等方面的故障 Environmental impacts or natural disasters: power failure, static, dust, humidity, temperature, damage by insects, flood, fire, earthquake etc. Breakdown related to software, hardware and communication line etc.
人为因素 Human factor	恶意人员 Malicious	不满的或有预谋的内部人员，对系统或资产进行恶意破坏；采用自主或内外勾结的方式盗窃信息、资产或进行篡改 Malcontent or premeditated employees: to maliciously destruct system or asset; to collude with external parties to stole or modify info and assets. 外部人员利用脆弱性，对资产或系统的保密性、完整性和可用性进行破坏 External parties utilize vulnerability existing, to sabotage the confidentiality, integrity and accessibility of asset or system.
	非恶意人员 Negligent	内部人员由于缺乏责任心、不关心或专注，或者没有遵循规章制度和操作流程而导致系统故障或信息损坏 System or info breakdown caused by employees' negligent acts which are for lacking of responsibility or concentration or not following working regulation and instruction. 内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致信息系统故障或被攻击 System or info breakdown caused by that employees do not have suitable ability.

7.3.2.2. 威胁可能性估值 Threat Likelihood Valuation

判断威胁的可能性，是威胁估值的重要内容，评估者应根据有关的统计数据来进行判断。下表为详细的威胁可能性估值说明：

It is a key part to estimate likelihood of threat. Assessor should estimate basing on relevant statistical data. Below is detail valuation description:

估值 Value	范围 Scope
3	非常可能会发生的情况，容易执行（触发），无资本（投入）或特殊的具体知识。5≤年度发生次数＜10 It could happen without any cost and special knowledge.5≤Annual frequency＜10
2	会经常发生。1≤年度发生次数＜5 Often happens. 1≤Annual frequency＜5
1	根据统计不太可能发生，或需要高昂高代价和高级别技能才会导致发生。年度发生次数=0 According to the statistical data, it is unlikely to happen without high cost and technology. Annual frequency =0

7.3.3. 脆弱性识别

7.3.3.1. 脆弱性识别 Vulnerability Identification

威胁总是要利用信息资产的脆弱性才可能造成危害。信息资产的脆弱性具有隐蔽性，有些脆弱性只有在一定条件和环境下才能显现，不正确的、起不到应有作用的，或没有正确实施的安全措施本身就可能是一个脆弱性。应参考下表内容进行全面的脆弱性识别：Threat always utilize the vulnerability of info assets to cause damage. The vulnerability of info assets are concealed, some of them will appear only under specific conditions and environment. Security measures themselves are vulnerabilities while they are improper, useless or not been carried out properly.

类型 Type	识别对象 Object	识别内容 Matters should be considered
技术脆弱性 Technical Vulnerabilit	物理环境 Physical Environment	场地防护、防火、供配电、关键设备设施接地与防雷、线路保护、安防系统与设施等方面 Physical security, fire, power-supply, ground-connection and anti-thunder of key

y		equipment, line protection, security system and devices etc.
	网络结构 Network	网络结构设计、访问控制策略、网络设备安全配置等方面 Network topology, access policies, security configuration of network devices etc.
	系统软件 System and software	补丁安装、病毒防护、用户账号、口令策略、资源共享、新系统配置、事件审计等方面 Patching, anti-virus, ID&password, password policy, resource sharing, new system configuration, event audit etc.
	数据管理 Data mgt.	数据完整性鉴别机制、机密保护等方面 Data integrity authentication, confidentiality etc.
管理脆弱性 Mgt. Vulnerability	技术管理 Tech Mgt.	物理和环境安全、操作管理、访问控制、系统维护、业务连续性等方面 Physical and logical security, behavior mgt., access control, system maintenance, BCP etc.
	组织管理 Org Mgt.	安全策略、资产分类与控制、人员控制、法律法规合规性等方面 Security policy, asset classification and control, personnel control, compliance to laws and regulations etc.

7.3.3.2. 脆弱性等级 Vulnerability Value

可以根据脆弱性对信息资产的暴露程度、技术实现的难易程度、流行程度等，采用等级方式对已识别脆弱性的严重程度进行估值。下表为详细的脆弱性等级估值说明：Value the seriousness of the vulnerabilities by classification according to exposure degree of assets, complexity and prevalence of technology implementation resulting from the vulnerabilities. Below is detail valuation description:

估值 Value	范围 Scope
3	控制缺乏、不适当、过时或不实用 Controls are scarce, improper, untimely or useless.
2	整体控制效率低下、不足或不适当 Overall controls are insufficient, inappropriate and with low efficiency.
1	某些控制不足或不适当 Some controls are insufficient and inappropriate.
0	控制适当、有效和高效率 Controls are appropriate, effective and with high efficiency.

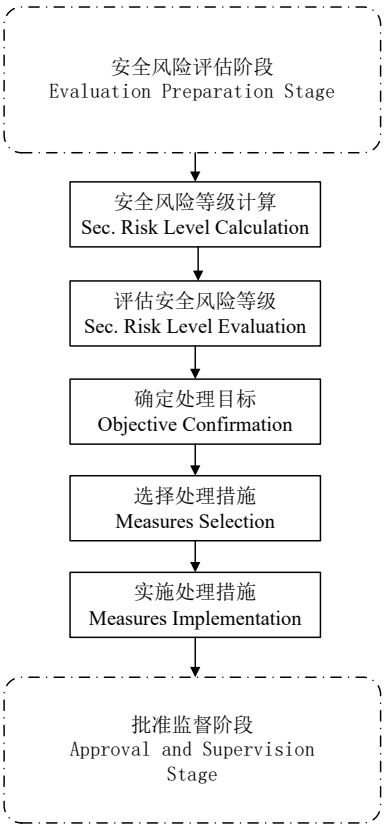
7.3.4. 现有安全控制措施的确认 Existing Security Controls Confirmation

在识别脆弱性的同时，确认目前已有的安全措施，是否真正地减少了脆弱性并抵御了威胁。有效的安全措施继续保持，无效的安全措施，应进行适当地调整或替换。

To confirm if the existing security controls have decreased vulnerability and withstand the threat while identify vulnerability. To keep effective security controls and improve or displace the useless.

8. 安全风险处理 Security Risk Handling

8.1. 安全风险处理过程 Security risk handling process



8. 2. 现存风险分析 Existing Risk Analysis

8.2.1 安全风险等级的计算

在完成了信息资产、威胁、脆弱性识别后，将确定安全事件发生导致的保密性安全风险损失、完整性安全风险损失，以及可用性安全风险损失，综合安全事件所作用的信息资产价值、威胁的可能性及脆弱性的严重程度，判断安全事件造成的损失对组织的影响，即安全风险等级。下表为详细的计算说明：

Confirm the confidentiality, integrality and availability damage of security risks resulting from their exposures after completed the info assets, threats and vulnerability identification. Combine thelevel of asset value and vulnerability affected by security incidents to evaluate the consequence to organization resulting from the security incidents, namedas Security Risk.

安全风险评估 Evaluation	计算依据 Calculation Basis	计算公式 Calculation Formula
安全事件发生率 Likelihood value of incident	威胁可能性、脆弱性等级 Value of likelihood of threat and vulnerability	威胁可能性估值+脆弱性等级估值-1 Value of likelihood of threat + value of vulnerability-1
保密性安全风险损失 Security risk damage level of confidentiality	信息资产保密性、安全事件发生率 Value of info asset confidentiality and Likelihood value of incident	保密性估值×安全事件发生率估值 Value of info asset confidentiality × Likelihood value of incident
完整性安全风险损失 Security risk damage level of integrity	信息资产完整性、安全事件发生率 Value of info asset integrity and Likelihood value of incident	完整性估值×安全事件发生率估值 Value of info asset integrity × Likelihood value of incident
可用性安全风险损失 Security risk damage level of availability	信息资产可用性、安全事件发生率 Value of info asset availability and Likelihood value of incident	可用性估值×安全事件发生率估值 Value of info asset availability × Likelihood value of incident
安全风险等级 Security risk level	保密性安全风险损失、完整性安全风险损失、可用性安全风险损失 Security risk damage level of confidentiality, integrity and availability	Max(保密性安全风险损失，完整性安全风险损失，可用性安全风险损失) Max one among Security risk damage level of confidentiality, integrity and availability

8.2.2 评估安全风险等级 Security Risk Level Evaluation

可接受的安全风险等级通常在 9 以下，但最终是由四川科道的管理者们协商决定的。并且在以后可调整可接受安全风险的等级。

Acceptable security risk level is less than 9 and decided by Keydom's administrators. It can be down-regulate.

8. 3. 安全风险处理的方式 Security Risk Handling Mode

安全风险处理主要有如下 4 种方式：There are 4 modes to deal with security risks:

- 规避：通过不使用面临风险的资产来避免风险。比如，在没有足够保障的信息系统中，不处理特别敏感的信息，从而防止敏感信息的泄露。Avoid: To avoid security risks by not using risk assets. For example, it does not deal with particularly sensitive information in an information system without adequate safeguards, thus preventing the leakage of sensitive information.
- 转移：通过将面临风险的资产或其价值转移到更安全的地方来避免或降低风险。Transfer: Transfer assets or its value faced the risk to a safer place to avoid or reduce risks.
- 降低：通过对面临风险的资产采取保护措施来降低风险。保护措施可以从构成风险的 4 个方面（即保密性、完整性、可用性、脆弱性）来降低风险。Reduce: Reduce risks by taking measures of assets protection. The protection measures can reduce risks from 4 aspects (i.e. threat source, threat behavior, vulnerability, assets and influence).
- 接受：根据风险等级，选择对风险不采取进一步的处理措施，接受风险可能带来的结果。Accept: Take risks without further proceesing, and accept the consequences of risks.

8.3.1 确定处理目标 Confirmation of Handling Objectives

8.3.1.1. 分析安全风险处理需求 Analyze Security Risk Handling Requirement

依据信息系统的安全要求、风险评估报告和风险等级划分表，从技术层面（物理、通信、网络、应用等）、组织层面（即结构、岗位和人员）和管理层面（即策略、规章和制度），分析安全风险处理的需求。

On the basis of information system security requirements, risk evaluation report and risk level table, analyze security handling requirements from technical level (physical, communication, network, application, etc), organization level (such as structure, position and personnel) and management level (i.e. policy, rule and regulation).

8.3.1.2. 确立安全风险处理目标 Establish Security Risk Handling Objective

依据风险等级划分表和风险处理需求分析，确立风险处理的目标，包括处理对象及其最低保护等级，形成风险处理目标列表。

According to the risk level table and risk handling requirement analysis, establish the target of risk handling, including the treatment object and its minimum protection level, and form a list of risk management targets.

8.3.2. 选择处理措施 Selection of Handling Measures

依据信息系统的安全要求、风险处理需求和风险处理目标列表，充分分析和平衡成本效益，选择合适的风险处理方式（包括接受、规避、转移和降低），并说明选择的理由及使用方法和注意事项等。

Select appropriate risk handling mode (including accept, avoid, trsfer and reduce) and explain the reason, using methods and attention factors according to information system security requirements, risk handling requirement, risk level table, and full cost benefit analysis and balance.

8.3.3. 实施处理措施 Implementation of Handling Measures

8.3.3.1. 安全风险处置计划 Security Risk

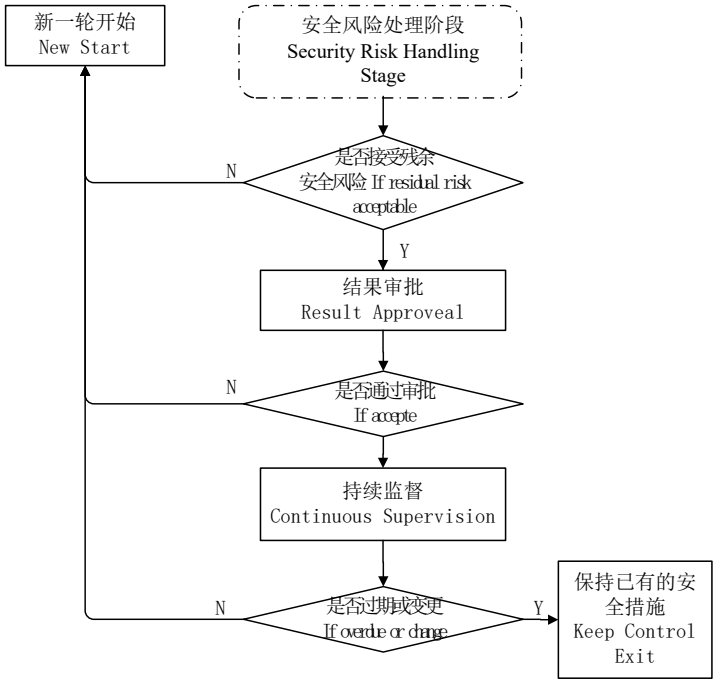
- 对不可接受的安全风险，各部门应结合现有安全措施的有效性评估，制定《安全风险处置计划》。For unacceptable security risks, every dept. should make a resolution plan considering exist security controls
- 安全风险处置计划中，应明确安全风险控制的管理措施、控制实施（是/否/计划）、责任人、截止日期、是否完成（是/否）等。Specify mgt. measures, implementation status (Y/N/Planned), responsibility, due date and completion status etc. inresolution plan.
- 安全风险控制管理措施的选择，应从管理与技术两个方面考虑。The mgt. measures for security risk should be made considering both from management and technology.
- 安全风险控制管理措施的选择与实施，应参照安全管理的相关标准进行。The mgt. measures for security risk should be made referring relevant security mgt. standards.

8.3.3.2. 实施安全风险处理措施 Implement Security Risk Handling Measures

依据安全风险处置计划，实施风险处理措施，并记录实施的过程和结果，形成风险处理实施记录。

Carry out risk management measures according to the risk management plan, record the process and result of the implementation, and form a record.

9. 批准监督 Approval and supervision



批准监督包括批准和持续监督两部分：批准是对残余安全风险的评估结果是否满足安全要求，做出是否认可安全风险管理活动的决定；持续监督是指检查环境有无变化，监督变化因素是否有可能引入新的安全隐患并影响到安全保障级别。

Approval and supervision include two parts: the approval is the decision on whether the evaluation of residual risks meets the security requirements and whether accept the decision of security risk management activities; Continuous supervision is to check whether the environment changed, and is it possible to monitor the changing factors to introduce new security hazards and affect the security level.

9.1. 残余安全风险评估 Residual Security Risk Evaluation

在对于不可接受的安全风险，实施适当的整改措施后，为确保安全风险控制措施的有效

性，可进行再评估，以判断实施安全风险控制措施后的残余安全风险等级，是否已经降低到可接受的水平。一般来说，安全风险控制措施的实施是以减少脆弱性或降低安全事件发生可能性为目标的，因此残余安全风险的等级，是根据换算系数、新脆弱性等级、新的安全事件发生率重新计算。 Conduct re-evaluation for the unacceptable security risks which have been improved by appropriate security risk control measures, to assess if they are acceptable after these. Generally, the objective of the security mgt. measures is to decrease vulnerability value and likelihood value of incident, so residual risk level should be calculated based on conversion ratio, new vulnerability value, and new likelihood value of incident.

9.1.1. 换算系数 Conversion Ratio

换算系数是基于计划实施的，控制行动的预期效果和覆盖面评估，通常为 0.3 / 0.6 / 1.

It is based on the desired effectiveness and coverage evaluation of the control measures will be implemented, it is 0.3, 0.6 or 1 as usual.

换算系数 Conversion Ratio	举例 Description
0.3	安全意识培训；保密标签/标识等 Security awareness training, confidentiality identifier etc.
0.6	处理文档等 Process document revision
1	信息安全系统审计；对供应商进行安全审核；异地存储关键数据库；病毒库更新等 Info system audit; security audit to supplier; offsite backup of key database; virus base updating.

9.1.2. 残余安全风险等级的计算 Calculation of Residual Security Risk Value

残余安全风险评估 Residual Security Risk Value	计算依据 Calculation Basis	计算公式 Calculation Formula
新脆弱性等级 New value of vulnerability	脆弱性等级、换算系数 Value of vulnerability,Conversion Ratio	最初脆弱性等级×（1-换算系数） Initial value of vulnerability×(1-Conversion Ratio)
新安全事件发生率 New likelihood value of incident	威胁可能性、新脆弱性等级 Value of likelihood of threat , New value of vulnerability	威胁可能性估值+新脆弱性等级估值-1 Value of likelihood of threat + New value of vulnerability-1
新保密性安全风险损失 New security risk damage	信息资产保密性、新安全事件发生率 Value of info asset confidentiality and New	保密性估值×新安全事件发生率估值 Value of info asset confidentiality × New

level of confidentiality	likelihood value of incident	likelihood value of incident
新完整性安全风险损失 New security risk damage level of integrity	信息资产完整性、新安全事件发生率 Value of info asset integrity and New likelihood value of incident	完整性估值×新安全事件发生率估值 Value of info asset integrity × New likelihood value of incident
新可用性安全风险损失 New security risk damage level of availability	信息资产可用性、新安全事件发生率 Value of info asset availability and New likelihood value of incident	可用性估值×新安全事件发生率估值 Value of info asset availability × New likelihood value of incident
残余安全风险等级 Residual Security Risk Value	新保密性安全风险损失、新完整性安全风险损失、新可用性安全风险损失 New security risk damage level of confidentiality, integrity and availability	Max（新保密性安全风险损失、新完整性安全风险损失、新可用性安全风险损失） Max one (New security risk damage level of confidentiality, integrity and availability)

9.1.2.1. 批准 Approval

- 批准申请：向管理者代表提交安全风险管理过程中的输出文档《安全风险评估总结与管理计划》，申请批准。

Application approval: submit <security risk evaluation summary and management plan> in the process of security risk management to the management representative and apply for approval.

- 批准处理：管理者代表依据安全要求和批准原则，与相关人员进行讨论和沟通后判断是否满足安全需求，依此做出批准决定。批准决定包括批准的范围、对象、意见、结论和有效期。如果通过批准，则进入持续监督阶段；否则，将需启动新一轮循环进行改进。

Handling approval: the management representative should to judge and make decisions after discussion and communication with related personnel based on the security requirements and approval principles. The approval decision shall include scope, object, opinion, conclusion and validity of the approval. If approved

安全策略部需每年组织各部门进行一次例行的全面的安全风险评估。即通常有效期为一

年。

9.2. 持续监督 Continuous supervision

- 检查是否过期：如果批准有效期到期，则启动新一轮的风险评估和风险处理。
- 检查有无变化：检查公司的发展情况、变更的情况、内部安全审核、外部安全审核、所发生的安全异常的情况。如果变化因素可能引入新的安全隐患并影响安全保障级别，依据《安全事故报告及处置管理标准》进行上报，并结束本次安全风险管理的循环，启动新一轮循环进行风险评估和风险处理。

10. 相关文件 Relevant Documents

- 信息资产安全管理标准 Info. Asset Security Mgt. Standard
- 安全手册 Safety Manual
- 安全事故报告及处置管理标准 Security Accident Report and Management Standard

11. 相关记录 Relevant Records

- 安全风险评估计划 Security Risk Assessment Plan
- 安全风险评估管理报告 Security Risk Assessment Management Report
- 安全风险评估总结与管理计划 Security Risk Assessment Summary and Mgt. Plan

12. 引用相关记录 Relevant Records Quoted

- 信息资产识别与评价表 Information Asset Identification and Evaluation Form