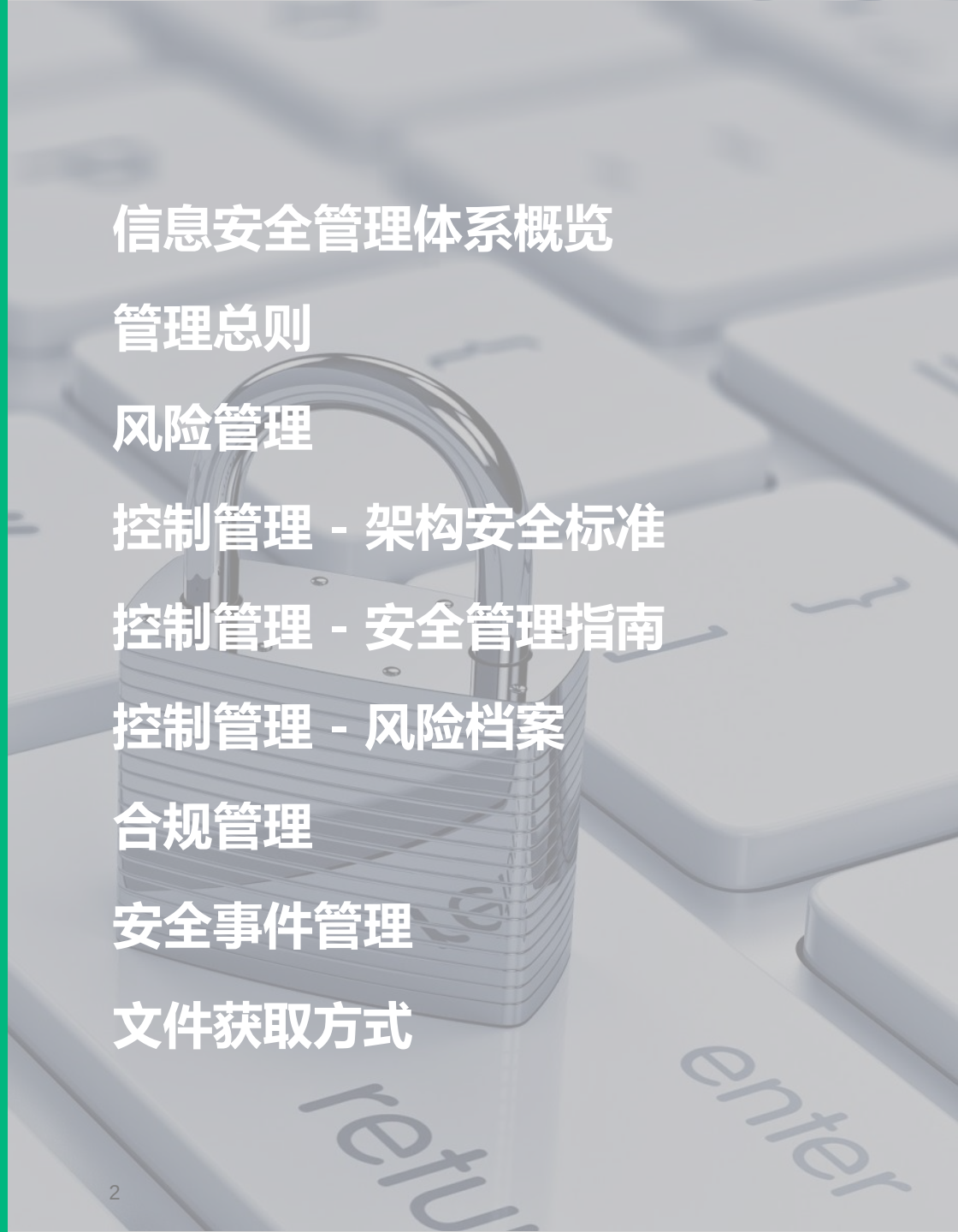
世界500强企业成熟

信息安全管理体系

- 文件架构及目录列表

目录



1

信息安全管理体系概览

信息安全管理体系框架

ISO 27001

管理流程

COBIT

ISO 27002 ~27048

法律法规

PCI-DSS

……

±340 ISMS 安全控制目标

架构安全标准

项目交付过程中设计阶段需遵从的标准（共12份文件）

安全管理指南

信息安全管理标准（共11份文件）

风险档案

基于控制域的风险分析（威胁和脆弱性）（共15份文件）

1. 管理总则

（共6份文件）

2. 风险管理

（共7份文件）

3. 控制管理

针对有价值的信息资产制定详细的控制流程和措施

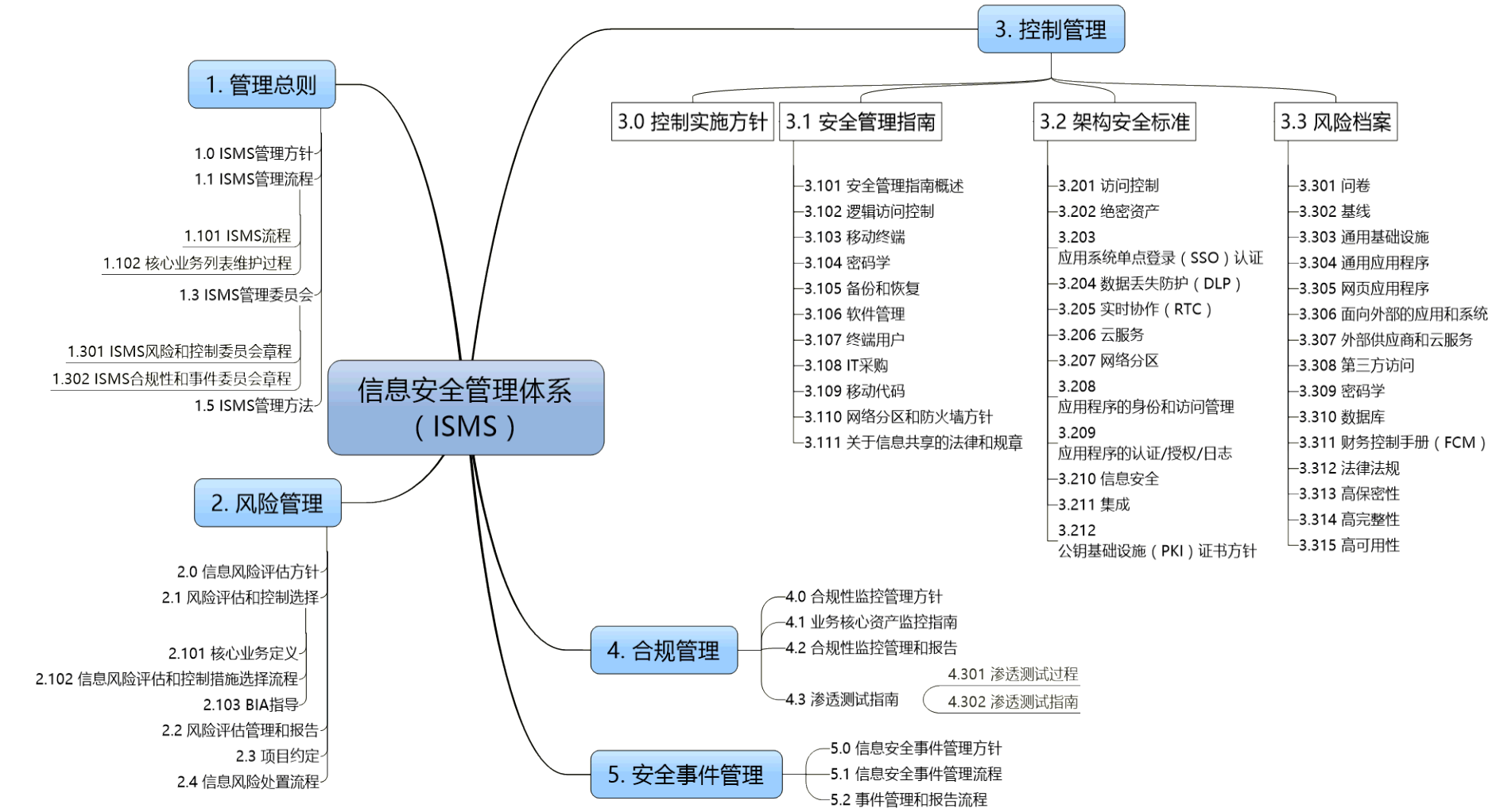
4. 合规性管理

（共5份文件）

5. 安全事件管理

（共3份文件）

信息安全管理体系文档地图



本文的价值

ISMS对企业的价值

内部IT团队收益	公司管理者收益	公司客户收益
• 帮助有效就信息安全事件进行沟通协作，提高事件应对能力 • 提升IT团队/人员安全意识和水平 • 改进IT团队绩效	• 有效降低IT风险及相关成本，提高IT投资回报率 • 向国际标杆靠齐，增强市场竞争力，提高公司声誉 • 符合来自各方不同的合规审核要求	• 信息服务可用性水平和信息安全水平得以保障，保证客户和投资者权益

本文对您的价值

已有ISMS体系的企业	计划建立ISMS的企业	个人
• 引入信息安全流程化管理理念，帮助企业切实落地； • 帮助ISMS管理者优化现有管理体系； • 本文作为检查表对现有体系文件进行补充	• 了解信息安全管理体系的全貌； • 为ISMS的建立提供参考，依照本文建立可全覆盖ISO27001认证需求。	• 通过本文可了解信息安全管理体系架构。

2

管理总则

目录

- ISMS管理方针
- ISMS管理流程
- ISMS管理委员会
- ISMS管理方法

管理总则

ISMS管理方针

摘要：

ISMS管理方针是基于企业控制框架，描述企业如何组织和管理的。本文档是专门为IT和业务领导撰写的。以使他们感谢ISMS的角色在确保那些对业务进行非常重要的信息资产会受到有效的控制和满足保密性、完整性、可用性和法规要求。 ISMS人员会发现这篇文档在阐明有关他们在企业的角色和职责上是有用的。

目录：

管理总则

ISMS管理流程

ISMS管理流程

摘要：

本文档定义了信息安全管理流程，以信息安全管理的方针为基础。它描述了在信息安全的治理、信息识别、风险评估和成本有效控制上的职责，以支持业务目标并满足法律法规要求。

信息安全管理流程的目标是提供一个标准的、实用的流程，以便业务理解以下内容：

- 信息资产的价值
- 信息质量对业务的价值
- 对信息资产的威胁和漏洞
- 如何选择合适的IT控制
- 如何监控IT控制的正确操作

目录：

核心业务列表维护过程

摘要：

核心业务列表是由底层基础设施/资产（如数据、硬件、软件、系统文档和存储介质）支持的应用和IT服务的统一清单，它可能通过以下一个或多个必要性影响企业（例如运营，资产或个人方面严重或灾难性的后果）：

- 可用的
- 可恢复的
- 保密
- 未修改/或通过正式的变更控制流程进行修改

目录：

管理总则

ISMS管理委员会

ISMS风险和控制委员会章程

摘要：

信息风险管理是一个不断发展的领域。随着持续和快速变化的威胁环境，风险和控制需要确保新的IT与业务发展的保护与风险偏好和遗留环境的安全相一致。我们在未来几年关注的重点是：

- 对我们服务的企业从信息风险角度知识的增长；
- 对项目在潜在风险上提供意见；
- 通过（根本）原因的分析和持续的风险评估来为常见的风险缓解成果评定优先级；
- 对来自不同机构的和决定业务风险变更的信息进行风险评估；
- 推动可以自动监控的简化和标准化的控制；
- 支持/促进与业务/利益相关者的IT风险讨论。

目录：

- 策略
- 目的
- 目标
- 参与者
- 频率、参与人数和委托
- 范围和活动
- 结构
- 输入
- 决策制定流程
- 输出

ISMS合规性和事件委员会章程

摘要：

IT部门的信息风险管理领域把重点放在确保以下要求的信息上：机密性、完整性、可用性、合规性。未来这可能会扩展到信息的效率、有效性和可靠性。合规性和事件委员会的目标是提供：

- 一个强大的合规性和事件管理流程，包括ISIM，BCIs和跨业务IT/ ITS的技术事件；
- ISMS合规性和事故管理流程和范围的治理；
- 合规性活动的计划和优先级排序；
- 审查事件和调查的根本原因和交流成果；
- 输入年度、季度和月度合规性和事故处理和报告；
- 处理高影响度问题的升级点；
- IT控制框架的持续改进。

目录：

- 目标
- 活动
- 范围
- 交付物
- 指导原则
- 工作方式
- 成员和治理

管理总则

ISMS管理方法

摘要：

本文档提出了ISMS干预的方法。过去几年在整个企业内的审计和合规性审查表明，我们需要改变我们对信息风险管理的表现。我们需要更持续的评估我们的风险，更严格的实施控制来减轻这些风险。需要系统地、持续地改变ISS管理方法，来提高对风险的理解和合规性水平。

目录：

3

风险管理

目录

- 信息风险评估方针
- 风险评估管理和报告
- 风险评估和控制选择
- 项目约定
- 信息风险处置流程

风险管理

信息风险评估方针

摘要：

本文档规定了企业内部信息风险评估的方针。方针介绍了企业信息风险评估实践的规定处理，并解释了业务人员、IT人员（IT交付人员）和信息风险管理人员的角色。方针决定了信息风险评估工作的背景，并明确重点区域、关键活动、岗位职责和权限。

目录：

风险评估管理和报告

摘要：

本文档解释了风险评估管理和报告如何支持从风险评估或合规流程中确定的风险的管理。本文描述了ISM和风险管理和控制委员会的角色，也分别描述了在风险接受步骤中的角色。

风险评估管理和报告为企业IT管理提供了：

- 对ISM特定风险生成风险可视化的手段；
- 对信息风险的理解，以促进ISM中修复和改进活动的优先次序。

目录：

风险管理

风险评估和控制选择

信息风险评估和控制措施选择流程

摘要：

本文介绍如何基于识别出的风险从IT控制框架中选择相关的控制。这个流程的目的是确保选择和实施适当的控制来缓解对企业信息资产已识别的风险。

风险评估和控制选择流程适用于企业业务流程所使用的信息资产。这可以由企业通过企业IT部门提供，也可以由第三方通过他们的基础设施提供。这意味着，风险评估和控制选择也适用于第三方（应用服务提供商，云计算）托管的信息资产，如网站和应用程序。以下的风险要素需要被考虑到：机密性、完整性、可用性和法规合规性。

目录：

核心业务定义

摘要：

本文档定义了核心业务信息资产。

核心业务定义的目的是为了识别企业必要资产，并确保它们得到适当的保护和管理。这些资产应当由核心业务列表来维护，并受到更严格的管制和合规性监视活动。

目录：

BIA指导

摘要：

业务影响评估（BIA）是理解任何涉及信息资产的安全事件的发生（泄密、数据损坏、信息不可用等）对业务的影响的ISM的过程。这个评估假定保护有关的信息资产上没有ISM控制。

目录：

风险管理

项目约定

摘要：

本文档有助于项目经理、服务提供商和ISM专家在IT解决方案的开发上实现ISMS要求的规划和整合。本文档中描述的步骤与项目交付框架（PDF）是一致的，并且定义了：

- 项目交付生命周期所需的最少的ISM活动；
- ISM门径管理签署所需的最少的交付物。

目录：

信息风险处置流程

摘要：

此过程说明了风险管理过程需要如何由业务ISM团队来实施，以积极管理从风险评估或合规流程中识别出的风险。当涉及到风险接受请求的审查时，业务ISM和风险管理及控制委员会的角色会出现在风险接受的过程中。

目录：

4

控制管理 - 架构安全标准

目录

架构安全标准

访问控制

摘要：

本文从IRM的角度讨论了对访问解决方案和从任何设备访问的结构要求。本文将分别介绍每一个访问模型。访问模型包括:

- 企业内部客户端：通过企业提供的台式机或笔记本登录企业网络
- 企业外部受信客户端： 通过一台不属于企业但是属于用户个人的受信设备上登录企业网络
- 企业外部非受信客户端：通过一台不属于企业也不属于用户的非受信设备上登录企业网络

目录：

架构安全标准

绝密资产

摘要：

本文从安全角度讨论了使客户端处理绝密（MC）数据的技术要求。本文不涉及其他为了处理绝密数据可以使用的技术（例如服务器，客户端等）要求。

目录：

架构安全标准

应用系统单点登录（SSO）认证

摘要：

企业规定用户登录到公司网络之后不会提示需要提供凭据登录任何其他企业应用程序或已经购买的程序。这就要求单点登录（SSO）功能可用于应用程序访问。本文介绍了要求，提供了解决方案的建议，并为未来的要求（1-3年）提供了路线图。此外，本文还讨论了需要双因子验证（2FA）的应用。

目录：

架构安全标准

数据丢失防护（DLP）

摘要：

该文档作为DLP的安全参考架构，给出满足企业安全标准的DLP技术类型的建议。本文档的主要读者是负责创建DLP实施的具体结构设计的解决方案架构师。这份文档把DLP看作产品和潜在的服务来实施。它不包括当下存在的帮助防止数据丢失的工具（如全盘加密）。

数据丢失预防（DLP）是一个计算机安全术语，它指的是通过深度内容检测和用集中管理框架来识别、监视、保护数据的系统。该系统的设计来检测和防止可能意外或恶意地发生的“敏感信息”（SI）的未授权使用和传输。

目录：

实时协作（RTC）

摘要：

本文从安全角度讨论了实时协作（RTC）的技术需求。RTC主机方面的技术（服务器、客户端等）不再讨论范围之内。

以下列出的条目在RTC的范围之内：语音（电脑到电话）、音频（电脑到电脑）、视频、即时信息、语音会议、语音信箱、网络会议、桌面共享、移动蜂窝集成、网络电话、群组聊天。

目录：

架构安全标准

云服务

摘要：

本文讨论了IT架构中的云安全。云安全对内部IT来讲包括相同的考虑因素（参考其他SRA文件，例如，信息安全和应用程序的认证/授权/记录），而且还引入了其他因素，如基于互联网的访问、对供应商的信任和法律/合规性问题。本文主要针对特定的云方面的考虑，同时也指出了对云场景的通用安全指导的重要实例。

目录：

架构安全标准

网络分区

摘要：

本文讨论了IT架构中服务器端内网的安全分区。网络区域划分的目的是改变内网模型，从任何主机都可以访问任何其他主机，变为每个访问都要服从定义的策略。这减轻了攻击和传播的机会和风险。一个区域由具有共同安全需求的一组资源（服务器）或一组用户（客户机）组成。企业内网通过使用安全网关（内部防火墙）来分区，以划分资源区域，并在网关上定义特定资源和/或特定用户的访问策略。

目录：

架构安全标准

应用程序的身份和访问管理

摘要：

本文从安全结构的角度讨论了应用程序的身份和访问管理（I&AM）。虽然重点是在应用程序方面，但总体企业级环境的I＆AM结构也会在本文中讨论。本文的重点是身份和访问的管理，即资料库、基础设施和生命周期的管理。

目录：

架构安全标准

应用程序的认证/授权/日志

摘要：

本文讨论了应用程序的认证、授权和日志记录。由于所有这些应用方面都涉及到身份资源库和生命周期，所以这篇文章和《应用程序的身份和访问管理》是密切相关的，并且应当相结合着来查看。本文的指导会特定在应用程序的分类等级上。一个应用程序的分类等级是由它处理的信息的最高等级- CIA维度的高/中/低，来决定的。

本文件的重点是应用程序。因此，基础设施级的认证/授权/记录的细节不在讨论范围内。例如Windows登录技术、Windows组架构、防火墙/ IDS日志记录、企业SIEM等。

目录：

架构安全标准

信息安全

摘要：

本文讨论了IT架构内的信息安全和相应的管理，没有讨论架构里的应用和基础设施元素。信息安全包括它的分类、库存、传输保护、密码学的使用和各种信息管理和存储的安全性。本文将从规则、结构和能力三个方面提供指导。本文对解决方案架构中的安全信息和信息相关的安全服务和基础设施实施/配置提供了标准，指南和建议。本文主要是一篇关于安全技术结构和关注安全技术的文档，而不是通用的安全指导。

目录：

集成

摘要：

本文讨论了IT架构中应用集成的安全性。集成的安全包括通信实体的认证/授权，和信息传输的保护。因此它存在于其他文档中，例如应用系统信息的安全性和认证/授权/日志。本文将从规则、结构两个方面提供指导。本文对解决方案架构中的安全信息和信息相关的安全服务和基础设施实施/配置提供了标准，指南和建议。本文主要是一篇关于安全技术结构和关注安全技术的文档，而不是通用的安全指导。

目录：

架构安全标准

公钥基础设施（PKI）证书方针

摘要：

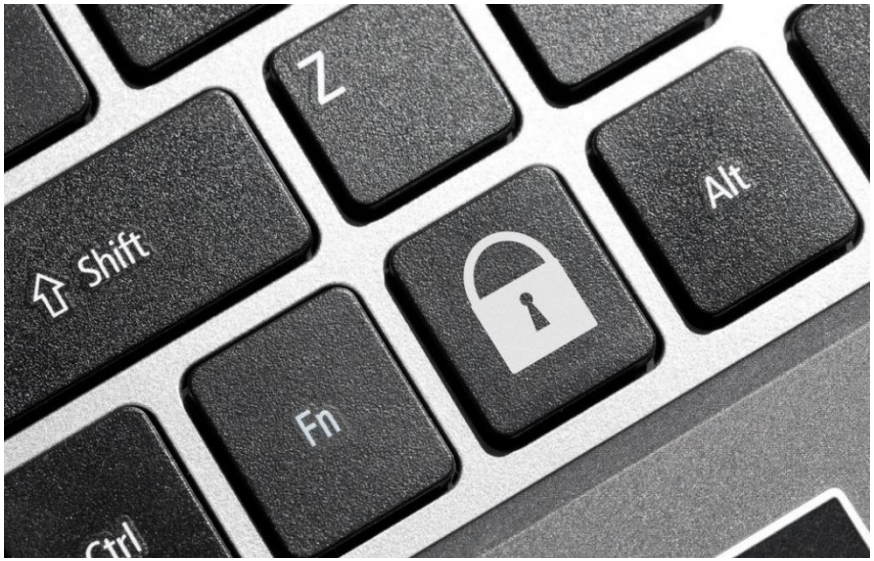
公钥基础设施（PKI）为公钥密码学提供和管理X.509证书。证书鉴别出证书中指定的实体，并将实体绑定到特定的公共/私有密钥对上。安全解决方案的公钥加密部分的可靠性是建立PKI的安全和可靠的运行的直接结果，包括设备、设施、人员和流程。这一方针的适用性声明应被视为最低要求;应用程序认证机构可能需要比在应用中的证书策略指定的更高水平的保证。此证书方针符合互联网工程任务组（IETF）RFC3647的证书策略与认证业务规则建设。

目录：

5

控制管理 - 安全管理指南

目录



安全管理指南

安全管理指南概述

摘要：

本文描述了安全管理指南在IT控制框架里的目的和结构。威胁结合新技术和商业模型的出现使信息风险管理更加复杂和具有挑战性。在这个变化的环境下，企业对如何处理信息风险需要保持清晰和一致的观点。

安全管理指南是IT控制框架的一部分。他们打算提出具体的议题，然后对关系到这个议题的IT控制目标如何实施提供具体、有力的指导。安全管理指南包含需求。这些需求应被看作是信息风险管理的建议水平，但是根据情形，其他措施可能是更适合的。安全管理指南的目标是对ISMS的充分执行和为企业总体设想和方向的一致性提供支持。

安全管理指南的目的包含两个方面：建立控制等级和提供清晰的思路。

目录：

逻辑访问控制

摘要：

安全管理指南对访问域控、信息资产和服务设立了信息风险管理需求。企业越来越依赖于信息流程来达成业务目标。访问控制是预防信息的误用和丢失的最重要的控制之一。为保护信息的访问控制关注于通过身份管理、用户和管理员认证、分配和撤销信息访问等来实现对信息系统、IT服务和应用的逻辑控制。

目录：

移动终端

摘要：

安全管理指南对被用作企业IT环境的一部分的移动终端设立了信息风险管理需求。移动设备的使用越来越广泛。移动设备的风险属性与传统的台式电脑是不同的。本文描述了保护移动设备的要求。移动设备访问公司网络、接收邮件和存储业务信息等都在讨论范围内。

目录：

密码学

摘要：

安全管理指南对被用作企业IT环境的一部分的密码学设立了信息风险管理需求。

通过加密手段确保真实性，机密性，完整性及合规性的控制都在讨论范围内。这类控制的实例包括：

- 使用（非）对称加密和解密来确保机密性
- 使用散列算法来确保发件人的真实性和数据的完整性
- 使用传输证明和来源证明来确保不可抵赖性
- 密码学的法律法规要求

目录：

备份和恢复

摘要：

安全管理指南对被用作企业IT环境的一部分的备份和恢复设立了信息风险管理需求。

包含信息的所有资产，也就是和企业运维、计划、或管理相关的数据元素的集合，都在范围之内。安全管理指南是适用于IT控制框架范围内的所有环境。这可能包括财务或战略信息系统，也包括系统配置信息或隐私相关的信息。例如应用软件、中间件、数据库、操作系统，还有网络组件如交换机、路由器等。外包给第三方的IT控制框架范围内的信息资产也包括在内。

目录：

软件管理

摘要：

安全管理指南对被用作企业IT环境的一部分的软件管理设立了信息风险管理需求。软件用于处理数据。该处理包括数据访问保护、数据存储和数据分析。如果软件无法按预期运行或有不恰当的访问控制，这可能导致机密性、完整性和可用性的问题。在安全管理指南中，软件生命周期中的ISMS方面包括以下主题：

- 软件开发生命周期;
- 软件操作。

软件管理需要保障软件的安全和法律/合规性要求，同时软件需要包含保障措施，以保护基础数据的机密性，完整性和可用性要求（如业务影响分析的定义）。

目录：

终端用户

摘要：

安全管理指南对被用作企业IT环境的一部分的终端用户设立了信息风险管理需求。本文描述了ISMS角度终端用户的责任。企业行为准则和商业交流规范考虑到最终用户的责任（不仅是ISMS）会更加全面。本书的范围包括通过用户的行为确保数据的真实性、保密性和完整性的所有控制。重点将放在有权限访问企业IT资源和处理电子数据的终端用户的要求上。安全管理指南提供了有关终端用户的通用类要求；注意业务部门可能对特定职能有附加要求（如服务台员工、开发人员、安全管理员等）。这些特定的要求不在本文档中详细介绍。

目录：

IT采购

摘要：

安全管理指南对被用作企业IT环境的一部分的IT采购设立了信息风险管理需求。IT采购可以定义为从外部供应商（提供商）处获取IT产品或服务。IT采购可以被分为三个子阶段：采购、运维、终止和转换。本文提供了与这些阶段相关的ISMS方面的内容，包括风险管理、合同、保证、服务级别管理、企业流程和程序的集合以及相应的角色和义务。讨论的范围包括从外部供应商采购的所有IT服务（例如软件、平台、基础设施等）。

目录：

移动代码

摘要：

安全管理指南对被用作企业IT环境的一部分的移动代码设立了信息风险管理需求。安全管理指南描述了关于移动代码执行和内外部服务提供商移动代码开发的IT控制框架要求。这些要求适用于所有企业资产。移动代码指从远程信息系统获得、通过网络传输并且在本地信息系统上执行的软件程序或一部分程序。例如Java、JavaScript、ActiveX、VBScript等。移动代码最常应用于互联网环境，经常在网页浏览器中执行。除了浏览器，宏（如微软Word、Excel、PPT中）和移动设备等可以执行移动代码的也要满足本文中定义的要求。

目录：

网络分区和防火墙方针

摘要：

安全管理指南对被用作企业IT环境的一部分的网络分段和防火墙方针设立了信息风险管理需求。

该方针描述了对网络分区的规范性要求，包括作为基础设施的一部分提供给企业的防火墙、代理服务器和反向代理服务器。它也解释了业务人员，IT人员（IT交付人员）和信息风险管理人员的角色。所有扮演了保护网络分区、相关资产和服务的连接性的资产都在讨论范围中。另外，该文件也旨在帮助组织理解防火墙技术与防火墙策略的功能。

目录：

关于信息共享的法律和规章

摘要：

设立了法律和规章对信息共享的信息风险管理要求，涉及所有的第三方，不只是IT供应商，还有所有合资企业。和相应的控制被用作壳牌IT控制框架的一部分管理L＆R信息共享风险。在授予合资企业或第三方供应商访问企业网络之前，必须对其进行风险评估。风险评估有三个输出：

- 合同要求；
- 授权管理；
- 访问规则。

目录：

6

控制管理 - 风险档案

目录

风险档案 - 结构

基线			基线			通用标准，包含环境控制
业务影响度(BIA)	通用基础设施	通用应用程序	高保密性	高完整性	高可用性	资产有C、I或A的中高级BIA评级
特定	外部供应商	密码学	网页应用			特定条件发生时适用
	第三方访问	数据库	面向外部的应用和程序	财务控制手册(FCM)	法律法规	

信息风险档案

法规档案

风险档案 - 实例

特权管理

3.303 通用基础设施

用户账户的访问仅限于相关人员，由指定的人员授予和维护。下面的步骤应考虑：

1. 访问特权与每个系统产品（例如操作系统、应用程序）相关联，应验证哪些程序应分配给用户；

2. 分配给用户的特权应基于“按需使用”的基础（对职能角色的最低需求）；

3. 应当维护一个授权流程和分配所有特权的记录。授权流程结束之前不应当授予特权;

4. IT资产所有者应确保在身份管理服务中注册一个有效和激活的身份，作为对所有用户允许和维护对IT资产的访问的先决条件。

3.304 通用应用程序

用户账户的访问仅限于相关人员，由指定的人员授予和维护。下面的步骤应考虑：

1. 访问特权与每个系统产品（例如操作系统、应用程序）相关联，应验证哪些程序应分配给用户；

2. 分配给用户的特权应基于“按需使用”的基础（对职能角色的最低需求）；

3. 应当维护一个授权流程和分配所有特权的记录。授权流程结束之前不应当授予特权;

4. IT资产所有者应确保在身份管理服务中注册一个有效和激活的身份，作为对所有用户允许和维护对IT资产的访问的先决条件。

实施指引

为了开通对应用程序的访问权限，每个用户都分配了一个个人账户，用来登录应用程序。基于访问管理流程设定的流程授予用户访问权限。特权账户只可用于以下身份：

基于额外认证账户的应用服务提供机构的员工；

接受了相关的职责和责任的其他业务批准的用户。

风险档案 - 实例

特权管理（续）

3.305 网页应用程序

OWASP（开放式Web应用程序安全项目）与OWASP开发指导了以下在实施期间应用的授权规则：

1.用户只能访问取得特定授权的受保护的功能;

2.用户只能访问取得特定授权的网址;

3.用户只能访问取得特定授权的数据文件;

4.直接对象引用是受保护的，只有被授权的对象对每个用户来讲是可以访问的;

5.除非特意申请，否则目录浏览是被禁用的;

6.用户只能访问为他们拥有特定的授权服务;

7.用户只能访问取得特定授权的受保护的数据;

8.访问控制安全地失效;

9.对表示层的相同的访问控制也在服务器端执行;

10. 除非特别授权，访问控制使用的所有用户和数据属性和政策信息不能由最终用户进行操作;

11.所有访问控制都在服务器端执行;

12.对各类受保护资源的访问保护有一个集中的机制;

13.企业对应用程序的在输入和访问上的限制（如每日交易限额或任务的顺序）不能被绕过。

3.306 面向外部的应用和系统

应用程序控制：

对于面向外部设备的应用程序，具有管理特权的用户必须控制在最小数量，并只有得到业务所有人（或正式委托人）的批准，在按需知密的基础上才能存在。

基础设施控制：

对于面向外部的设备，具有本地或域管理特权的用户必须控制在最小数量，并只有得到业务所有人的批准，在按需知密的基础上才能存在。有权访问面向外部设备的管理员必须具有与内部系统访问不同的账户和凭据来管理面向外部的系统。

风险档案 - 实例

特权管理（续）

3.307 外部供应商和云服务

1.在按需知密的基础上，在应用层限制相关人员对管理员账户和高特权账户的访问；由指定的人员授予和维护访问权限；使用基于角色访问时要保证职责分离;

2.当一个账户被授权访问核心业务应用时，这个账户即为高特权账户;

3.对每个服务维护一个高特权账户列表;

4.对每个服务的高特权账户列表，应与应用程序或系统的所有者或其委托人达成一致;

5.至少每月一次与应用程序所有者一起审查高特权账户的访问;

6.如果需要对信息系统的紧急访问或非例行访问，必须由管理层授权;

7.应保存一份使用紧急访问账户的记录;

8.在紧急活动完成之后，对应的任何紧急账户的密码应当被更改，账户应当被禁用;

9.应监控所有的行为，以确定是否出现任何不恰当行为。当发现不合规行为时应立即采取补救措施。

3.310 数据库

数据库专用操作系统账户：

DBMS流程或服务必须在定制的、专用的操作系统账户下运行。因此，为个人DBMS流程或服务创建和指派定制的用户账户来使用。此外，禁用对运维来说不需要的任何DBMS流程或服务账户。给自定义服务账户或流程的可执行文件分配需要的用户权利或特权。用文件记录在系统安全计划中的分配。

数据库专用目录：

DBMS的数据文件、事务日志和审计文件必须存储在和软件或其他应用程序文件分开的专用的目录或磁盘分区中。指定数据库的数据、事务和审计文件存储的专用目录。配置DBMS默认的文件存储路径，以使用由DBMS支持的专用目录。确保对每个目录的访问权限都是定制的，只允许被授权的用户和流程的访问。

数据库数据文件：

DBMS数据文件必须专用于支持单独的应用程序。重新定位应用程序数据库表到DBMS支持的特定的数据库数据文件上。

风险档案 - 实例

特权管理（续）

3.311 财务控制手册（FCM）/ 3.313 高保密 / 3.314 高完整

应用程序控制：

在按需知密的基础上对相关人员访问管理账户和高特权账户进行限制，由指定的人员授权和维护。

基础设施控制：

1.当一个账户被授权访问核心业务应用时，这个账户即为高特权账户;

2.对每个服务维护一个高特权账户列表;

3.对每个服务的高特权账户列表，应与应用程序或系统的所有者或其委托人达成一致;

4.对高特权账户的问责应保留在企业内部，即使访问流程已经外包给了服务提供商。在外包的情况下行使问责制，定期（至少每季度一次）的对账户和员工变更的详细流程审查必须由企业员工来进行。

风险档案 - 实例

信息安全的认知、教育和培训

3.301 基线

业务控制：

信息安全相关的培训会在各个业务领域适当的开展。信息安全认知沟通计划应提供给一些特殊的团队，像是那些机密性高的团队。

集中控制：

为信息安全团队、企业全体员工还有相关的合同工和第三方用户提供和维护一个安全认知培训课程。

提供关于信息安全认知、包含量化指标的沟通计划。

1.展示可测量的认知形式（如调查，访谈等）；

2.展示SLA中规定的KPI报告：

- 安全认知培训的完成情况;
- 未完成者数量及逾期时间。

基础设施控制：

基础设施支持应确保支持人员具备履行其为企业提供服务的角色所需的适当的技能。

在年度目标、绩效考核及个人发展计划会议之前，各部门经理还要考虑对IT控制或近期安全控制变更的培训。

风险档案 - 实例

信息安全的认知、教育和培训（续）

3.307 外部供应商和云服务

对有权访问机密或绝密级的企业数据的供应商的员工，应在合同中强制规定其必须周期性的参与：

1. 安全意识会议;

2. 关于执行信息安全相关控制的操作的培训。

3.313 高保密性 / 3.314 高完整性 / 3.315 高可用性

应用程序支持应确保支持人员具备履行其为企业提供服务的角色所需的适当的技能。

在年度目标、绩效考核及个人发展计划会议之前，各部门经理还要考虑对IT控制或近期安全控制变更的培训。

风险档案 - 矩阵

安全控制目标	次数	基线	高保密性	高完整性	高可用性	通用基础设施	通用应用程序	网页应用程序	面向外部的应用和系统	外部供应商和云服务	第三方访问	密码学	数据库	财务控制手册(FCM)	法律法规
数据管理的安全要求	5					1	1		1		1		1		
网络服务安全	3					1			1				1		
信息交换政策和程序	3					1			1		1				
交换协议	4					1	1		1		1				
审计记录	10		1	1		1	1	1	1	1	1		1		1
故障记录	2					1							1		
特权管理	9		1	1		1	1	1	1	1			1	1	
用户访问权限审查	7		1	1		1				1	1		1	1	
信息访问限制	4					1	1						1		1
敏感系统隔离	3					1	1						1		
安全登录程序	5		1	1		1	1			1					
密码管理系统	2					1							1		
连接时间限制	2					1							1		
网络服务使用政策	2					1							1		
网络隔离	2					1			1						
操作软件控制	1					1									
系统测试数据保护	1						1								
业务职能和技术需求的定义和维护	4		1	1	1	1									
测试环境	3					1	1		1						
输入数据验证	3						1	1					1		
消息完整性	1						1								
输出数据验证	3						1	1					1		
信息泄露	2					1					1				
技术漏洞的控制	9	1	1	1	1		1	1	1	1				1	
确定连续性要求	1					1									
确定选择	1					1									
知识产权	6	1	1	1	1		1			1					
信息安全的认知、教育和培训	5	1	1	1	1					1					

7

合规管理

目录

- 合规性监控管理方针
- 业务核心资产监控指南
- 合规性监控管理和报告
- 渗透测试指南

合规管理

合规性监控管理方针

摘要：

本方针文件规定了对IT控制的合规性及有效性监测和报告的规则。例如，IT控制是否符合目标，是否按照惯例框架规定的实施指导进行。

合规性监控流程对信息资产控制的有效性提供了详细的洞见，并帮助找到那些把企业暴露在高风险下，需要被修复的缺陷。合规性监控提供了需要的证明来保证内外部利益相关者支持核心业务流程和目标的信息资产的风险得到验证和有效的缓解。

目录：

合规管理

业务核心资产监控指南

摘要：

本文档为IT关键控制提供以下指导：

- 通过监控建立设计和运营有效性
- 状态的记录和报告

对设计有效性（DE）：

- 确保所记录的控制满足控制目标，指出需要减轻的和能够控制的风险

对运营有效性（OE）：

- 确保控制按照设计的来运营

目录：

合规性监控管理和报告

摘要：

每个业务负责选择、实施和维护控制，充分保护它们的资产，并确保在IT控制的目标能够达到。这应根据资产的重要性和风险评估。合规性监控将关注于确定的范围和年初同意的控制集合。

在这一年中，应由IT交付人员确定和报告，业务ISM人员协调，针对确定范围的合规性监控得到有效的设计和运行。

目录：

渗透测试指南

渗透测试过程

摘要：

对所有的业务核心应用，建议每年进行一次，或者在重大更新上线之前进行渗透测试。这将有助于确保软件的新版本或者重大功能更新不会对应用的CIA要求产生不利影响。

渗透测试的范围专注于以下领域：

- 业务核心应用；
- ITS基础设施；
- 业务要求的临时渗透测试。

目录：

渗透测试指南

摘要：

渗透测试实际上是由IT专业人员进行的对非法破译/黑客活动的模拟。与安全审计有指定的衡量标准不同，渗透测试没有单一的标准。进行的测试是寻找技术实施方面的差距、已知风险和漏洞，并会利用已知的黑客攻击方法。

渗透测试可以被看作是一种方法，用来确保对IT控制框架充分的执行，提高技术和程序上的IT控制，并建立可接受的剩余风险的意识。

目录：

8

安全事件管理

目录

- 信息风险事件管理方针
- 事件管理和报告流程
- 信息风险事件管理流程

安全事件管理

信息风险事件管理方针

摘要：

该方针制定了报告和调查对企业信息资产的信息风险事件的规则。

此策略的设置用来确保所有信息风险事件都由ISM专家调查。ISM专家应该能够就如何防止此类事件的再次发生提供建议。

目录：

事件管理和报告流程

摘要：

事件管理实施和报告文档描述了在信息风险事件管理流程以及相关的报告中使用的数据。这将通过确保所需数据提供给各参与方，来促进该流程的执行。

本文档的目的是为涉及信息风险事件管理流程的所有人员提供高层级的数据字典。

目录：

信息风险事件管理流程

摘要：

本文档介绍了信息风险事件管理流程中的流程和责任方。它建立在“信息风险事故管理方针”描述的目标、范围和高层级的流程和责任上。信息风险事件管理流程的目标是：

- 确保信息风险事件和信息系统有及时的沟通，以便有恰当的纠正措施；
- 通过及时采取纠正措施限制事件的影响；
- 提供信息安全事件的管理，包括监测、报告和响应流程；
- 收集证据，以应对起诉，纪律处分和对企业的指控
- 通过确定并执行从事件中的学习，改进信息风险，防止未来信息风险事件的发生。

目录：

9

文件获取方式

文件获取方式

- 本文仅为体系文件目录， 欲获取全部正文请联系：
  - 邮箱：sale@it17580.com
  - QQ：58801860
  - 微信：IT咨询我帮您

谢谢