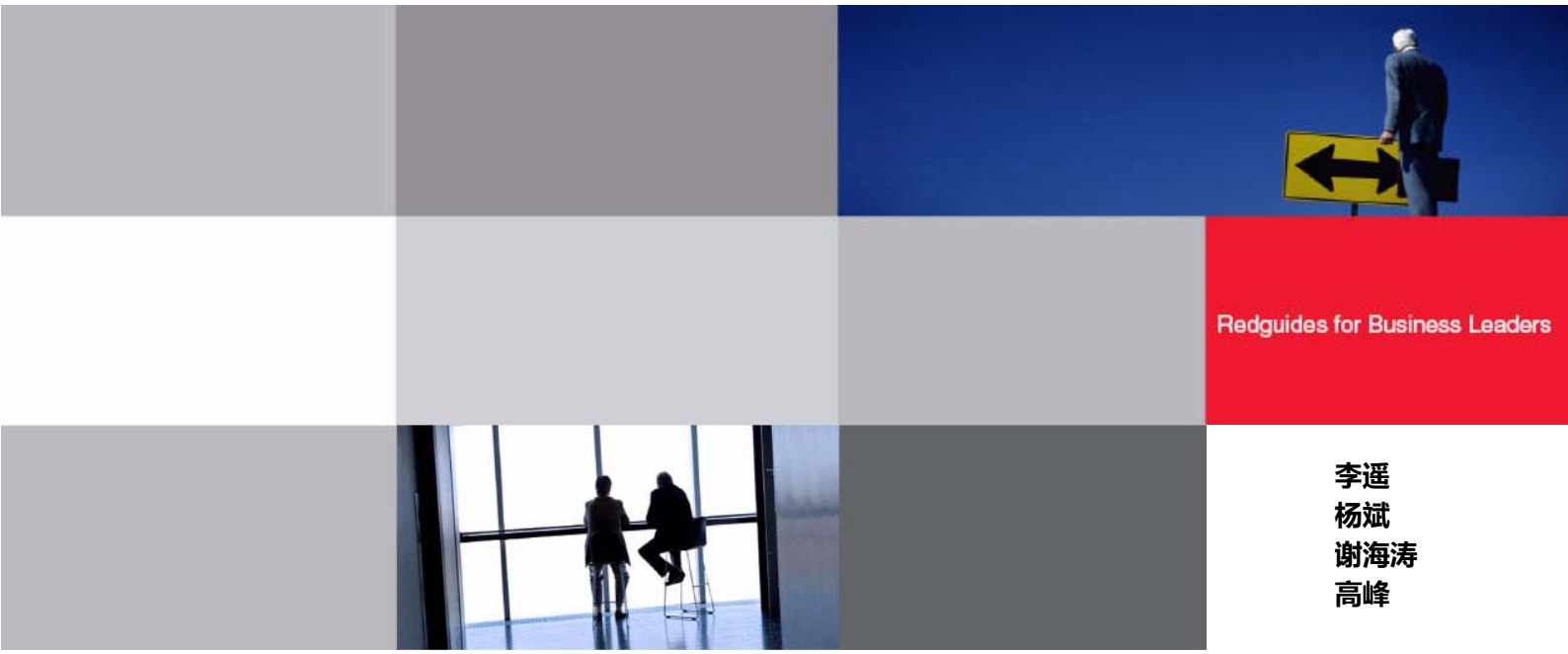
企业信息安全框架 V5.0 白皮书



Redguides for Business Leaders

李遥
杨斌
谢海涛
高峰

IBM Global Technology Services

Internet Security Systems

目录

序　言

IBM 提出“企业信息安全框架” ESF(Enterprise Security Framework v5.0)的核心目的是，在 IT 系统已经成为企业业务的运营平台之际，如何在企业无比复杂的信息环境中，对企业的信息安全进行整体的全面的把控。

“整体安全”的概念在安全业界已经不再是一个生疏的话题，IBM 的“企业信息安全框架”ESF(Enterprise Security Framework v5.0)的创新意义在于，首次从企业的业务本身出发， 结合安全最佳标准和业界相关标准的安全模型，形成一套行之有效的方法论，帮助企业定位安全建设的现状、了解安全建设的需求、组织未来安全建设的规划和实施。

众所周知，即便是在信息安全国际标准和相关最佳实践的指导下，企业按照标准的安全实践方法，设计和实施信息安全解决方案时，依然会遇到很多挑战。企业还必须考虑多平台，多组件架构集成的复杂性，实施安全解决方案的多样性等。

那么，企业信息安全框架 ESF 是如何能做到行之有效呢？ 企业信息安全框架 ESF 所提供的又是怎样的一个安全模型？

行之有效的最根本原因是，“企业信息安全框架 ESF”指导企业在信息安全建设之初，即根据企业业务发展的需要，确立合理的信息安全需求、确立企业信息安全架构，选择安全功能组件。

企业信息安全框架从上到下由三个主要层次组成：安全治理风险管理及合规层、安全运维层、基础安全服务和架构层。安全治理风险管理及合规层，是后两者的理论依据；安全运维层，则是对安全生命周期全过程的管理；基础安全服务和架构，是企业信息安全建设技术需求和功能的实现者。

- 安全治理、风险管理和合规：

它处于企业信息安全框架的最顶层，是业务驱动安全的出发点。主要包括企业战略和治理框架、风险管理框架、合规策略遵从。通过对企业业务和运营风险的评估，确定其战略和治理框架、风险管理框架，定义合规和策略遵从，确立信息安全文档管理体系。

- 安全运维：

安全运营是指在安全策略的指导下，安全组织利用安全技术来达成安全保护目标的过程。主要包括安全事件监控、安全事件响应、安全事件审计、安全策略管理、安全绩效管理、安全外包服务。安全运营与 IT 运营相辅相成、互为依托、共享资源与信息，它与安全组织紧密联系，融合在业务管理和 IT 管理体系中。

- 基础安全服务和架构

基础安全服务和架构定义了企业信息安全框架中的五个核心的基础技术架构和相关服务：物理安全、基础架构安全、身份/访问安全、数据安全和应用安全。基础安全服务和架构是安全运维和管理的对象，其功能有各自子系统提供保证。

总之，企业信息安全框架（ESF V5.0）给企业信息安全建设提供了一个集成的、标准的企业信息安全框架，帮助企业快速知晓企业信息安全现状和需求，能为企业信息安全平台的建设、设计、实施提供指导和参照 ，从而使业界提出多年的企业“整体安全”理论能够真正落地。

目前业界有很多关于信息安全建设的资料和书籍，但绝大多数都是针对安全建设具体技术的探讨。本书旨在帮助企业的高级管理层从风险管控的角度出发，以一个战略的高度，全方位的去考虑和实施安全的整体框架，实现一个风险可控的，优化的业务信息支撑体系。

余磊

总经理

IBM 信息安全服务部

第一章　企业与信息安全

1.1 企业风险与安全

我们赖以生存的地球就像有“智慧”的生命系统，由越来越多的人、越来越多的组织机构和自然系统相互连接而成。人类正在以前所未有的自由度来构建、汇集、整合和连接存在于任何地方的各类资源。随着网络的高度发达，人、数据和各种事物都将以不同方式联入网络。

对于企业来说，在进行商务活动的时候始终面临着各种风险，这些风险是固有的，其不但存在于企业与客户和合作伙伴的日常接触之中，也存在于企业内部。信息系统作为企业商务活动的重要组成系统，同样也无法避免各种风险的威胁。可以用水与船的关系来比喻企业对 IT 系统的依赖度与 IT 风险之间的关系，水涨船高，依赖度越强，IT 风险越大。

了解这些风险与相应的安全解决方案是降低这些风险的前提。企业通过提供产品与服务来创造价值，而在提供产品与服务的过程中不可避免的要跨越一些物理或逻辑上的边界。这些边界应该得到安全的保护，然而有效的保护这些边界并不是一件容易的事情。大多数企业并不是一张白纸，其人员、流程和资源已经形成了一套成熟、固定的体系。一个全面安全计划的实施可能会破坏当前企业的运作。因此绝大多数企业在这些年一直被**“如何实施安全解决方案以降低商业风险？”**的问题所困绕。与此同时，企业还面临如何降低管理运行成本和复杂性的挑战。

1.1.1 企业风险

安全不仅仅是产品，也不仅仅是服务。它是企业创造价值过程中的一个必要条件。安全包含了生产的安全：如财务、物流、市场等；物理的安全：如机房物理环境、计算机机房场地、操作室视频监控等；信息系统的安全：如信息系统基础架构安全、安全管理工具和安全管理服务。

安全不是绝对的，世界上不存在绝对的安全，企业始终面临着风险。有些风险可以避免，有些风险可以降低，而有些是可以接受的。一个企业如果了解了这些风险，并且处理好这些风险，那么它就是安全的。降低风险的成本与取得的回报总是相称的。因此企业需要平衡在安全上的投资与回报。

了解风险

商业风险是企业所设法避免的，通常这些商业风险的发生会对企业带来经济上的损失，如销售额下降或企业的声誉受损。那么企业会面临哪些商业风险呢？以及有哪些降低这些风险的手段呢？

资产风险：企业的有形资产或无形资产被损坏所带来的资产损失。

人员风险：人员身份冒用所带来的损失。

保管风险：不能有效保护第三方的资产和信息所带来的风险。

信息风险：信息资源没有得到有效的管理控制带来的风险。

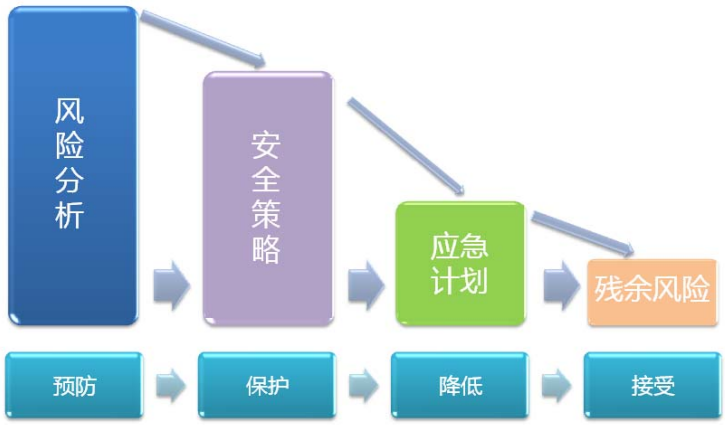
风险管理的手段

预防：企业可将风险转移给其他企业，如资产投保等。

保护：企业可通过一定的手段减轻风险发生的可能性或所导致的后果。

降低：通过技术手段和管理手段来避免风险的发生。

接受：某些风险所导致的后果属于企业可接受的范围。



图示 1：企业风险管理流程

1.1.2 企业信息安全

凯撒密码的传说

在人类历史上，保护信息的需求与信息本身一样历史久远。第一个用于加密和解密消息的文档化数学“密码”是凯撒密码，是由凯撒本人创造的。古希腊历史学家希罗多德于公元前 479 年记录道：

“当它在苏萨获悉薛西斯决定入侵希腊时，认为必须将这一消息传递给斯巴达。由于一旦被敌人发现，就会面临巨大的危险，所以只有一种方法可以用来传递消息：刮去一对木制折叠板的封蜡，在木板上写上薛西斯的企图，然后再用蜡封住木板。”

“按这种方式处理的木板，看上去相当光滑，不会引起路上哨兵的注意。当消息抵达目的地时，没有人能猜出这一秘密，只有 Cleomenes 的女儿 Gorgo（Leonidas 的妻子）发现了它并告诉给其他人……这样一来，人们得到了此消息并传递给其他希腊人。”

从这个故事可以透视出信息加密的历史和它的重要性。

当今企业所处信息环境

在信息系统介入企业商务运作的初期，企业的商务运作环境相对封闭，对信息数据的交互要求也不高，信息系统可以得到企业的完全控制。而如今的信息系统已经成为企业生产业务系统的一部分，企业商务运作中的大量重要信息交互必须依赖于开放的、互联的网络环境进行。

我们生活的地球已经进入了一个“智慧的地球”的新阶段，在“智慧的地球”上，各个领域的边界将会逐渐的溶解，各个领域之间交互的信息量激增，且必将建立在更加信任的基础上。与此同时，“智慧的地球”孕育而生的新的协作方式导致信息的流转变得更为复杂。这些都为企业在新的全球化环境中带来了新的风险和挑战。智慧的地球将商业企业、医疗机构、教育、政府部门、甚至个人联结到了一起，在带来丰富资源的同时，也带来了各种新的潜在的风险。这些风险涉及信息系统的多个领域。

调查显示，2008 年全球信息系统面临的主要风险包括以下几个主要方面。

安全漏洞-安全漏洞数量在 2008 年抵达顶峰，其中 53%的安全漏洞仍没有任何厂商提供补丁。在所有的安全漏洞中，54.9%是 Web 应用安全漏洞，在这 54.9%中，有 75%还不存在补丁。

恶意网站-仅 2008 年第四季度，全球新创建的恶意网站数量比 2007 年全年还多 50%。2008 年，中国首次超过美国，成为全球恶意网站数量最多的国家。

Web 应用-Web 应用成为公司的弱点及 IT 安全工作的薄弱环节。大量的端点利用攻击，不仅源自浏览器的安全漏洞，而且还源自大量的恶意电影和 Adobe PDF 文件等文档。

钓鱼和木马攻击-超过 90%的网络钓鱼针对金融行业，特洛伊木马占到全部恶意软件的 46%，主要目的是盗用信息。

自从网络和 Internet 万维网出现以来，新兴技术和数据信息量激增，虚拟

化和云计算增加基础架构复杂性,新兴技术的应用导致安全违规和安全攻击事件的大量增加，数据量每隔 18 个月翻一番，围绕着信息上下文的存储、安全和发现技术变得越来越重要。信息安全问题越来越凸现出来 使得企业规避信息安全风险的需求日趋紧迫。

信息安全事件不再危言耸听

Conficker 蠕虫感染 600 万台 PC 中国是重灾区

“Conficker”蠕虫是从 2008 年年底开始传播，以微软的 windows 操作系统为攻击目标的计算机蠕虫病毒。这个蠕虫利用的是一个已知的被用于 Windows 操作系统各平台的服务器服务漏洞。这种蠕虫为网络犯罪分子提供了实施拒绝服务攻击、窃取保密数据和发布垃圾邮件的手段。除此之外，Conficker 可通过移动存储进行传播，如 U 盘，移动硬盘等；在局域网中，该蠕虫还会通过猜测用户名和密码，以网络共享的方式进行传播。

全球各地已经有 500 至 600 万台电脑已经被“Conficker”蠕虫感染。被“Conficker”蠕虫感染的电脑数量最多的国家是中国，有大约 270 万台电脑被感染。其次是巴西和俄罗斯，被感染的电脑熟练分别是 100 万和 80 万台。菲律宾排名第十九位，已证实有 126，594 台电脑被这种蠕虫感染。

僵尸网络

如果是几年前，2009 年发生的 Twitter 的网络攻击事件难度很高，黑客需要是个计算机狂，能够同时操控数千台计算机；不然就要很有钱，支付白花花的银子让专家来做这件事。那么现在呢？据《Business Week》报道，现在网络攻击变得相当简单，那些攻击如 Twitter 网站的工具已经变得便宜且易于使用，让更多人可以制造网络灾难。网络信息安全公司 Damballa 副总 Gunter Ollman 表示：“门槛的降低，使得几乎所有人都可以进行网络攻击。”

信息安全专家表示，僵尸网络的爆炸性成长，使得地下供货商们面临削价

竞争的压力。 Ollman 指出，以往大概只有半打僵尸网络，受挟持的计算机约百万台，但现在僵尸网络成倍数成长，使得租借 1 万台计算机（一个足以瘫痪 Twitter 的量）的价格，从每天 2000-5000 美元，降到只剩 200 美元。这也造成了网络攻击事件的上升，8 月 10 日时，约有 1300 个分布式阻断攻击，但两年前时的同一天，只有约 700 个。

网络钓鱼

近年来，不法分子利用“钓鱼”网站等手段，大肆盗取用户网络银行账户。据统计，目前有 10%-15%的中国网民在使用浏览器、即时通讯、游戏等软件时，都曾接触过欺诈信息，网络诈骗形势严峻!

网络钓鱼（Phishing，又名钓鱼法或钓鱼式攻击）是通过发送大量的声称来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人提供敏感信息（如用户名、口令、账号 ID、ATM PIN 码或信用卡详细信息）的一种攻击方式。最典型的网络钓鱼攻击将收信人引诱到一个通过精心设计与攻击目标的网站非常相似的钓鱼网站上，诱导并获取收信人在此网站上输入的个人敏感信息，通常这个攻击过程不会让受害者警觉。它是“社会工程学”的一种形式。

网络钓鱼攻击的趋势是攻击者集中攻击目标，金融机构成为网络钓鱼攻击的主要目标。网络钓鱼占到垃圾邮件总量的 5%，网络钓鱼攻击者的目标越来越集中。2007 年，在主题行提供大众化内容的网络钓鱼电子邮件，占到网络钓鱼邮件总量的 40%以上。2008 年，这个比例大幅度跌至 6.23%。2008 年的趋势是鼓动用户采取行动，网络钓鱼攻击人不再频繁使用“安全警报”等大众化的主题，而是鼓动用户采取行动，如修复可疑账户或更新账户信息等。超过 90%的网络钓鱼攻击针对金融行业，其他目标包括在线拍卖网站和商店等，只占一小部分（4.6%），在以金融机构为目标的网络钓鱼攻击中，99%以上发生在北美洲或欧洲。

安全业的“魔道”之争—全球黑客大聚会

2009 年 7 月，Black Hat（黑帽）大会在美国拉斯维加斯的凯撒皇宫酒店举行。

黑帽大会目前已经是全球最重要的 IT 安全系列会议。思科、RSA、微软、Qualys、IOActive 等众多的安全厂商以及独立安全研究人员都在会上发表了自己最新的研究成果。“黑帽”安全技术大会是一个具有很强技术性的信息安全会议，会议将引领安全思想和技术的走向，参会人员包括各个企业和政府的研究人员，甚至还有一些民间团队。为了保证会议能够着眼于实际并且能够最快最好的提出方案、问题的解决方法和一些操作技巧，会议环境保持了中立和客观。黑帽安全技术大会是世界上最好的能够了解未来安全趋势的信息峰会。15 年来，越来越复杂的网络环境和黑客技术的不断创新，安全形势越来越严峻，这些都促使黑帽需要更好的在第一时间触及安全问题。

随后举办的姊妹会议——DefCon 黑客大会，也是网络安全业界备受关注的事件。因为在会上所展示的关于网络技术的各种漏洞以及对操作系统和网络设备的全新攻击方式，对于安全业界和设备厂商来说既是严峻的挑战，也是一次绝好的学习和修补产品缺陷的机会。今年的黑帽大会已经是第 12 届，参会人数(4500 人)比去年增加了 12.5%，网络安全业界“黑白两道”的焦点人物几乎悉数到场。

网络战

随着网络技术的迅速发展，网络空间成为继陆、海、空及太空空间后新的争夺空间。如今网络正在成为联结个人和社会，现在和未来的纽带，各式各样的计算机网络都将成为一个国家的战略资源和战略命脉，一旦重要的网络系统陷入瘫痪，整个国家安全就面临着崩溃的危险，使“制网络权”的争夺与对抗不可避免。同时，随着信息技术在军事领域的广泛应用，军队对计算机网络的依赖越来越大，网络与作战的联系也愈来愈紧密，网络成为新的战场空间。

信息战是指以数字化部队为基本力量，以争夺、控制和使用信息为主要内容，信息战不同于信息作战和信息化战争。网络战是为干扰、破坏和威胁敌方网络信息系统，并保证己方网络信息系统的正常运行而采取的一系列网络攻防行动。网络战分为两大类：一类是战略网络战；另一类是战场网络战。

网络战正在成为高技术战争的一种日益重要的作战样式，它可以兵不血刃

地破坏敌方的指挥控制、情报信息和防空等军用网络系统，甚至可以悄无声息地破坏、瘫痪、控制敌方的商务、政务等民用网络系统，不战而屈人之兵。在网络空间的争夺中，网络既是己方的薄弱环节，又是对方攻击的重要目标，网络空间的对抗与争夺同电磁空间的对抗与争夺一样，成为没有“硝烟”的特殊战场。信息战、网络战，在近些年几场局部战争中已彰显出强大威力，也成为当前广为探讨的话题。

1.2 信息安全的重要性及价值分析

在全球信息化的今天，信息资产已经成为任何企业、组织发展壮大的至关重要的因素，必须得到最有效的保护。另一方面，这些资产也暴露在越来越多的威胁中。毫无疑问，保护信息的私密性、完整性、真实性和可靠性的需求已经成为企业和消费者的最优先的需求之一。

由于入侵、破坏企业信息系统的事件每天都在发生，加上人们对 Internet 危险性的认知不断加强，人们对信息安全的需求前所未有地高涨起来。对于大多数高级企业主管而言，他们已经认识到安全问题已不再遥不可及。安全风险会大大降低公司的市场价值，甚至威胁企业的生存。即使很小的风险也能将公司的名誉、客户的隐私信息和知识产权等置于危险之中。

通过以上讨论可以看出，在当前的商业和信息环境下，企业正面临着各种各样的信息安全问题，而解决这些安全问题对企业而言是至关重要的。从一定程度上说，安全的信息系统是现代企业赖以生存的基础，是企业发展驱动力的来源之一，而不仅仅是企业业务的支撑平台。

在这样的环境中，企业如何才能有效地解决这些问题呢？值得高兴的是，我们已经找到了一些有效的方法帮助企业建立安全灵活的基础设施，保护极其复杂的应用程序和资源，并通过系统的安全管理策略，计划规程，实施及监督程序等来保护企业的核心业务。

1.2.1 企业安全之痛

随着国内企业信息化程度的提升，企业的信息资产与业务运营所面临的安全威胁也在日益加剧。虽然企业对于安全防护的投入逐年递增，但在面对愈来愈频繁和复杂的病毒破坏与黑客攻击等安全问题时，仍停留在兵来将挡的被动应付阶段。

安全需求来自于业务本身，而非 IT 技术驱动，安全问题贯穿于整个企业的运作。如：

- 保护企业员工和客户的私有信息。
- 保护关键商务信息交换的安全性。
- 企业级的统一身份管理。
- 确保越来越复杂的系统环境的一致性、完整性。
- 完善安全管理策略，降低企业风险。

下面我们来看，企业信息安全的重大意义主要包括哪些方面。

1.2.2 保护企业客户信息和内部员工信息

如果没有明确的被保护对象和范围，信息安全是没有价值的。企业的内部组织信息，员工信息，以及企业的客户信息，商务伙伴的资料与数据等，是企业赖以生存的基础，都是需要保护的重要资产。

1.2.3 商业机密信息的安全交换

电子商务是当今世界商务活动运作发展的主流方向。在信息化的过程中，越来越多的企业在大规模的运用电子商务来取代传统的商务活动方式，以达到全面提高其市场竞争力的目的。然而，电子商务目前主要是以电子数据交换和 Internet 方式来实现的。企业必须防止电子商务中的欺诈行为，合同争议和信息泄露或篡改的现象发生。在网上进行商务活动会涉及许多企业的商业秘密与个人隐私，这需要保护；另一方面，任何商务活动都是建立在交易双方相互信任的基础上，如何确定交易对象的身份，并防止抵赖情况发生是保证电子商务顺利进行

的关键，企业开展电子商务活动必须建立在安全交易的基础上。

1.2.4 保障业务持续运转

“天有不测风云，人有旦夕祸福”。像地震，火灾，爆炸，洪水等自然灾害，系统软件与硬件故障，网络病毒，人员欺诈与恶意行为等威胁，都会造成企业商务活动的中断，甚至企业的破产，例如，如果通信网络因为故障造成用户数据丢失且没有用户数据备份，短时间内无法恢复，这将给通信运营商造成很大的经济与信誉损失。如美国的“9.11”恐怖事件的发生，因为企业数据的毁灭，造成很多公司业务长时间的中断，甚至使公司承受灭顶之灾。为了防止企业经营或商务活动的中断，保护关键商务过程免受重大故障或灾难的影响，建立和管理安全强壮的信息系统必不可少。

1.2.5 信息安全是企业持续发展的需要

现代企业的正常运作离不开信息资源的支持，这包括组织的知识产权，各种重要数据，信息处理设施，关键人员等。企业的商业秘密的泄露会使企业丧失竞争优势，失去市场；系统故障会造成正常业务的运作中断。因此，企业要保持可持续性发展，信息安全是基本的保证之一。

1.2.6 降低风险，简化复杂性

企业在商业活动中面临着各种各样的风险，这些风险是企业内部运作，与客户和业务伙伴合作中与生俱来的，不可避免的。正确识别、理解风险和安全解决方案的关系是降低企业风险的基本要求。企业需要根据商业安全规范建立有力的方法论，将信息安全植入到企业创造商业价值的流程和风险管理过程中，并且使企业的安全投资回报最大化，使企业能够有效利用安全资源来管理商业风险。

安全管理通用五步法：

风险分析：研究潜在的安全漏洞，决定可接受的安全控制，实施成本，以及不能被顾及的，可接受的风险因素。其主要活动包括：确定安全漏洞或风险，例

如自然灾害，外部黑客攻击，员工错误等；识别有商业价值的数据资产，例如客户数据库，研究信息，新产品计划，财务数据等；量化损失风险，资产价值及其控制成本；

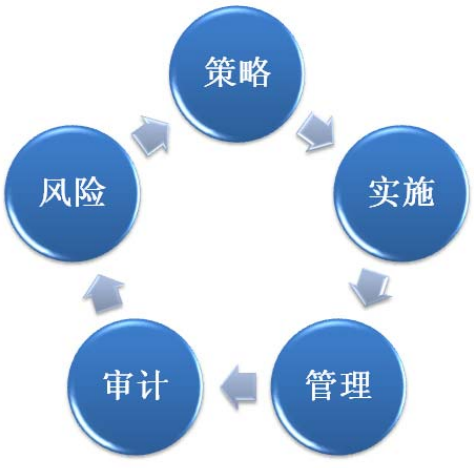
制定安全策略：制定资产分类计划；应用安全支持；信息服务供应商安全支持计划；高级别的管理目标承诺和责任；安全违规处理程序；用户培训和安全告知程序。

实施执行：安装适当的安全产品和安全控制系统，主要包括：为满足特定的安全策略选择适当的安全机制 ;安装安全软硬件产品 ;定义系统安全的控制方法；定义用户和资源分组，以便于管理。

管理：安全策略的应用和实践，例如：用户身份和口令管理；特殊系统和用户特权管理；数据库，应用程序，交易和设备的资源管理；安全日志管理。

审计：安全审计是指对安全控制和安全事件的审查、评估。审计的结果应定期的报告给管理层，并以此来更新和完善安全策略和执行程序。

为了实现有效的安全策略，构建企业安全平台，企业必须建立一个基于风险分析，策略定义，方案实施，管理和审计的循环往复的流程周期。安全审计主要包括：内部测试；渗透测试；合规性检查；外部认证等。



图示2：安全管理策略五步法

第二章　信息安全基础及发展趋势

2.1 洞察信息安全

2.1.1 信息安全概述

随着电子信息技术的迅速发展，人类已进入网络经济时代。世界经济网络化的发展速度使习惯于正常工作和生活的人们始料不及。据统计，目前全球信息产业正以 10%以上的年增长率高速发展。如今，互联网上网用户数达 15 亿，中国互联网用户数达到 3.5 亿。其他类型网络应用和新兴技术也如雨后春笋般的在世界各地诞生。

计算机网络化对经济、社会以及人们的生活带来了很多便利。但同时由于技术本身的原故，人们所依赖的信息化系统存在较大的脆弱性，极易受到电脑“黑客”的入侵。计算机网络的安全受到极大的威胁。

计算机网络运行所依赖的 TCP/IP 协议在设计时，安全并不是主要的考虑点。随着攻击技术的不断发展，各种各样利用网络底层协议本身的安全脆弱性进行攻击的手段层出不穷，而且其中很多是无法从根本上避免的。由于所有的应用协议都架设在 TCP/IP 协议之上，TCP/IP 协议本身的安全问题，将极大地影响上层应用的安全。

网络的普及和应用，还是近十年的事情，而操作系统的产生要远早于此。在互联网络广泛应用之前的操作系统，主要面向个人用户或者是同一个组织里的用户，这与互联网络广泛应用之后的情况是完全不同的。如：很多操作系统缺省安装时存在大量的后台服务进程和缺省用户帐号，这些都有可能带来潜在的安全隐患。

另外，企业日臻完善的安全体系结构也会因设计和实现时的细小瑕疵而存在安全隐患的可能，比如一个小的编程缺陷，亦可能导致系统被入侵。另外，如果应用系统中的各种构件之间缺乏紧密的通信和合作，将可能导致整个系统被逐个

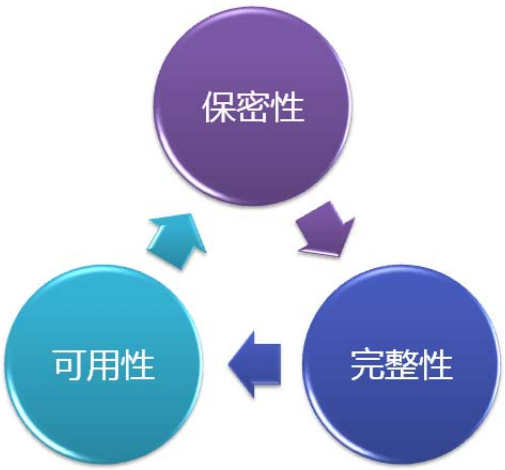
击破。

提高信息系统安全性的目的主要是为了满足保护信息资产的需要，这里的信息资产包括数据信息资产和物理设备资产(例如计算机本身)。在这里我们着重讨论的是数据信息资产的安全性。

广义上说，信息系统的安全就是通过各种方法和工具保护静态信息和动态信息。静态信息就是在电脑上存储的信息；动态信息就是在网络上传输的信息。换句话说，安全就是一个保密的过程，让不该看到信息的人不能读取信息，同时要让该看到信息的人读取到正确的信息。作为一个新兴的研究领域，网络安全正孕育着无限的机遇和挑战。相信在未来十年中 ,网络安全技术一定会取得长足发展。

2.1.2 信息安全基本目标

信息安全目标就是实现信息系统的基本安全特性（即信息安全基本属性），并达到所需的保障级别。信息安全的基本目标，包括保密性、完整性和可用性。CIA 概念的阐述源自信息技术安全评估标准(InformationTechnology Security Evaluation Criteria，ITSEC)，是信息安全的基本要素和安全建设所应遵循的基本原则。如下图所示：



图示 3：信息安全基本属性

- 保密性（Confidentiality）：确保信息在存储、使用、传输过程中不会被泄漏给非授权用户或实体。
- 完整性（Integrity）：确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性。
- 可用性（Availability）：确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时的访问信息及资源。

除了 CIA，信息安全还有其它的一些基本属性，包括：

- 可追究性：指从一个实体的行为能够唯一追溯到该实体的特性，可以支持故障隔离、攻击阻断和事后恢复等。
- 抗抵赖性：指一个实体不能够否认其行为的特性，可以支持责任追究、威慑作用和法律行动等。

2.2 信息系统安全发展历程

信息系统的安全在其发展过程中经历了三个阶段：

2.2.1 通信安全阶段

在早期，通信技术还不发达，电脑只是零散的位于不同的地点，信息系统的安全仅限于保证电脑的物理安全以及通过密码（主要是序列密码）解决通信安全保密问题。把电脑安置在相对安全的地点，不容许非授权用户接近，就基本可以保证数据的安全性了。但是，信息是必须要交流的。如果一台电脑上的数据需要让别人读取，而需要数据的人却在异地，怎么办？只有将数据拷贝在介质上，派专人秘密的送到目的地，拷贝进电脑再读取出数据。即使是这样，也不是完美无缺了，谁来保证信息传递员的安全？因此这个阶段人们强调的信息系统安全性是指信息的保密性，对安全理论和技术的研究也仅限于密码学。这一阶段的信息安全可以简单称为**通信安全**。它侧重于保证数据在从一地传送到另外一地时的安全性。1949 年 Shannon 发表的《保密通信的信息理论》将密码学的研究纳入了

科学的轨道，移位寄存器的物理舞台给数学家基于代数编码理论提供了运用智慧的空间。

2.2.2 信息安全阶段

进入上世纪 60 年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段，数据的传输已经可以通过电脑网络来完成了。这时候的信息已经分成了静态信息和动态信息了。人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的**信息安全阶段**，主要保证动态信息在传输过程中不被窃取，即使窃取了也不能读出正确的信息；还要保证数据在传输过程中不被篡改，让读取信息的人能够看到正确无误的信息。

1977 年美国国家标准局（NBS）公布的国家数据加密标准（DES）和 1983 美国国防部公布的可信计算机系统评价准则（TCSEC —Trusted Computer System Evaluation Criteria (俗称橘皮书)1985 年再版）标志着解决计算机信息系统保密性问题的研究和应用迈上了历史的新台阶。这一时期，国际上把相应的信息安全工作称之为数据保护。

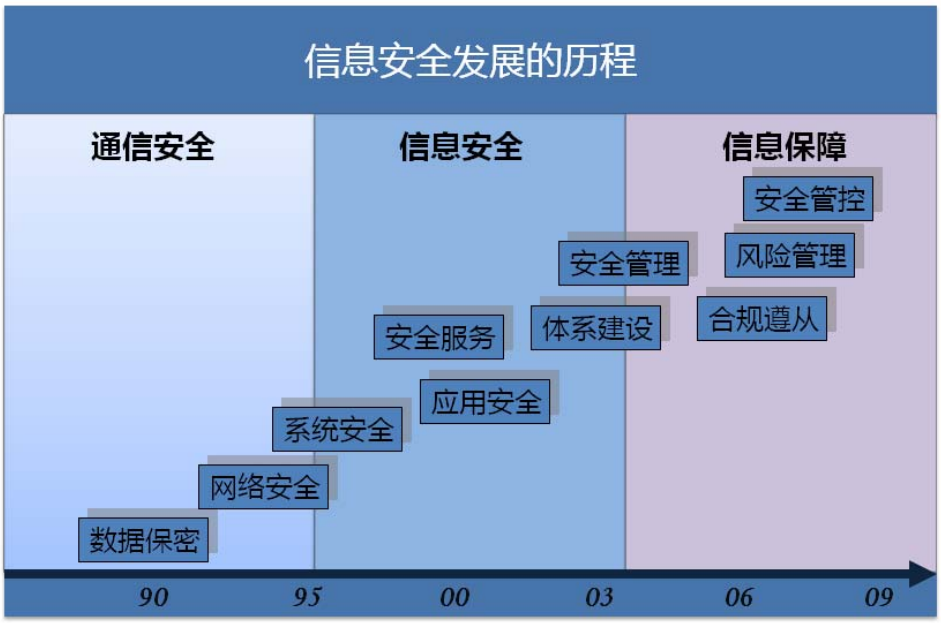
2.2.3 信息保障阶段

到了上世纪 90 年代开始，由于互联网技术的飞速发展，信息无论是对于企业内部还是外部都得到了极大的开放，而由此产生的信息安全问题跨越了时间和空间，信息安全的焦点已经从传统的保密性、完整性和可用性三个原则衍生为诸如可控性、抗抵赖性、真实性等其他的原则和目标。信息安全也转化为从整体角度考虑其体系建设的**信息保障阶段。**

如果说对信息的保护，主要还是从传统安全理念到信息化安全理念的转变过程中，那么面对业务的安全，就完全是从信息化的角度考虑信息的安全。体系性的安全保障理念，不仅是关注系统的漏洞，同时从业务的生命周期着手，对业务流程进行分析，找出流程中的关键控制点，从安全事件出现的前、中、后三个阶

段进行安全保障。面向业务的安全保障不只是建立防护屏障，而是建立一个“深度防御体系”，通过更多的技术手段把安全管理与技术防护联系起来，不再是被动地保护自己，而是主动的防御攻击，也就是说：面向业务的安全防护已经从被动走向主动，安全保障理念从风险承受模式走向安全保障模式。

随着网络上业务系统越来越多，各个业务系统的边界逐渐模糊，系统间需要相互融合，数据需要互通交换，多个业务系统的开发与运营统一到了一个管理平台上来，这些平台成为面向服务的架构的基础。因此，对单个业务的安全保障需求演变为对多个业务交叉系统的综合安全需求，信息系统基础设施与业务之间的耦合程度逐渐降低，安全也分解为若干单元，安全不再面对业务本身，而是面对使用业务的客户，具体地说就是用户在使用信息系统平台承载业务的时候，涉及该业务安全保障，由此，安全保障也从面向业务发展到面向服务。



图示 4：信息安全发展的历程

2.3 信息安全国际标准

伴随着信息安全的发展，在各个阶段不同的组织制定了相应的信息安全标准。

2.3.1 信息安全管理标准

2.3.1.1 信息和通信技术安全管理（ISO/IEC TR 13335）

ISO/IEC TR 13335，被称作“IT 安全管理指南”（Guidelines for the Management of IT Security，GMITS），新版称作“信息和通信技术安全管理”（Management of Information and Communications Technology Security，MICTS），是 ISO/IEC JTC1 制定的技术报告，是一个信息安全管理方面的指导性标准，其目的是要给出如何有效地实施 IT 安全管理的建议和指南。用户完全可以参照这个完整的标准制订出自己的安全管理计划和实施步骤。

该标准目前分为 5 个部分：

- IT 安全的概念和模型（Concepts and Models for IT Security），该部分包括了对 IT 安全和安全管理的一些基本概念和模型的介绍；
- IT 安全的管理和计划（Managing and Planning IT Security），这个部分建议性地描述了 IT 安全管理和计划的方式、要点；
- IT 安全的技术管理（Techniques for the Management of IT Security），覆盖了风险管理技术、IT 安全计划的开发以及实施和测试，还包括一些后续的制度审查、事件分析、IT 安全教育程序等；
- 防护的选择（Selection of safeguards），它是最新发布的一个部分，主要探讨如何针对一个组织的特定环境和安全需求来选择防护措施，这些措施不仅仅包括技术措施；
- 网络安全管理指南（Management guidance on network security），这部分提供了关于网络和通信安全管理的指导性内容。该指南为识别和分析建立网络安全需求时需要考虑的通信相关因素提供支持，也包括对

可能的安全措施方面的简要介绍。

2.3.1.2 澳新风险管理标准（AS/NZS 4360）

AS/NZS 4360:1999 Risk Management是澳大利亚和新西兰颁布的一个关于风险管理的标准，在国际上具有一定的影响力。在涉及风险评估与风险管理的具体方法和过程方面，AS/NZS 4360可以为促进组织ISMS的BS7799符合性提供帮助。

AS/NZS 4360定义了风险管理过程的5个步骤：

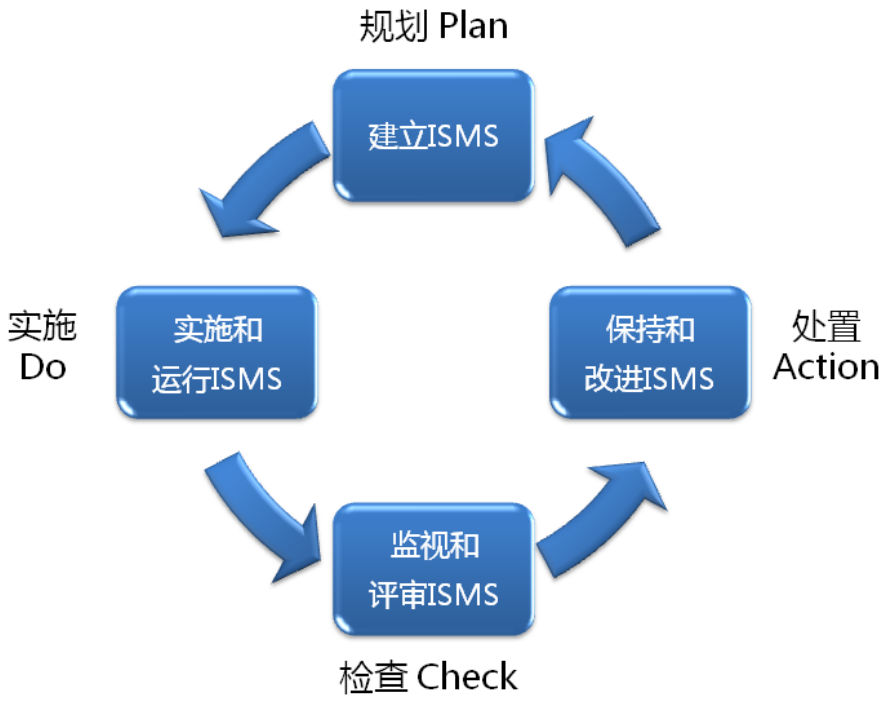
- 环境建立（Contexts established）—— 建立在风险管理过程中会用到的策略、组织和背景。
- 风险识别（Risks identified）—— 识别会出现的风险和出现的原因，为进一步分析打好基础。
- 风险分析（Risks analyzed）—— 识别在现有控制作用下的风险后果和可能性，进一步估计风险程度。
- 风险评价（Risks evaluated）—— 将估计的风险等级与预先建立的标准进行比较，得到按等级排列的风险，以便识别管理的优先顺序。
- 风险处理（Risks treated）—— 接受并监控低优先级的风险，而对其他风险，应该建立并实施特定的管理计划，包括对所需资金的考虑。

2.3.1.3 信息安全管理体系（ISO/IEC 27001）

ISO/IEC 27001标准用于为建立、实施、运行、监视、评审、保持和改进信息安全管理体系（Information Security Management System，简称ISMS）提供模型。采用ISMS应当是一个组织的一项战略性决策。一个组织的ISMS的设计和实施受其需要和目标、安全要求、所采用的过程以及组织的规模和结构的影响，上述因素及其支持系统会不断发生变化。按照组织的需要实施ISMS，是本标准所期望的，例如，简单的情况可采用简单的ISMS解决方案。

在建设信息安全管理体系的方法上，ISO 27001标准为我们提供了指导性建议，即基于PDCA（Plan、Do、Check和Act，即戴明环）的持续改进的管理模式。PDCA是管理学惯用的一个过程模型，在很多管理体系中都有体现，比如质量管理体系（ISO 9000）和环境管理体系（ISO 14000）。

PDCA如下图所示：



图示 5：ISMS PDCA 建设过程

2.3.1.4 信息安全管理实施细则（ISO/IEC 27002）

国际标准化组织 ISO 发布公告，该标准将取代 ISO/IEC 17799：2005，直接由 ISO/IEC 17799：2005 更改标准编号为 ISO/IEC 27002：2005，于 2007 年 7 月实施。

ISO 27002 是一个被国际社会广泛认可的信息安全管理标准。其目的是将信息系统用于工业和商业用途时为确定实施控制措施的范围提供一个参考依据，并且能够让各种规模的组织所采用。其前身 ISO 17799 于 2005 年进行了修订，新版本增加了最新的信息处理技术应用、网络和通讯技术。并更加强调了信息安

全所涉及的商业问题和责任问题。它主要涵盖了 11 个控制域，其中包含 39 个控制目标以及 133 个控制措施。ISO 27002:2005 中的 11 个主题分别是：

- 安全策略（Security policy）
- 信息安全组织（Organization of information security）
- 资产管理（Asset management）
- 人力资源安全 （Human resource security）
- 物理和环境安全（Physical and environmental security）
- 通信和操作管理（Communication and operation management）
- 访问控制（Access control）
- 信息系统获取、开发和维护（Information systems acquisition, development and maintenance）
- 信息安全事件管理（Information security incident management）
- 业务连续性管理（Business continuity management）
- 符合性（Compliance）

其结构如下图：

图示 6：ISMS 架构

ISO 27002 是一个完整的信息安全控制模型，它可以为企业带来如下好处：

- 一个受业界广泛认同的方法论；
- 按业界最佳实践方针去开展信息安全评估、实施、维护和管理；
- 为定义策略、标准、流程和指南提供框架。

2.3.2 信息安全产品标准

2.3.2.1 美国可信计算机安全评价标准（TCSEC）

TCSEC 标准是计算机系统安全评估的第一个正式标准，具有划时代的意义。该准则于 1970 年由美国国防科学委员会提出，并于 1985 年 12 月由美国国防部公布。TCSEC 最初只是军用标准，后来延至民用领域。TCSEC 将计算机系统的安全划分为 4 个等级、8 个级别。

D 类安全等级：D 类安全等级只包括 D1 一个级别。D1 的安全等级最低。D1 系统最普通的形式是本地操作系统，或者是一个完全没有保护的网络。

C 类安全等级：该类安全等级能够提供审慎的保护，并为用户的行动和责任

提供审计能力。C 类安全等级可划分为 C1 和 C2 两类。C2 系统具有 C1 系统中所有的安全性特征。

B 类安全等级：B 类安全等级可分为 B1、B2 和 B3 三类。B 类系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。B2 系统必须满足 B1 系统的所有要求，而 B3 系统必须符合 B2 系统的所有安全需求。

A 类安全等级：A 系统的安全级别最高。目前，A 类安全等级只包含 A1 一个安全类别。A1 类与 B3 类相似，对系统的结构和策略不作特别要求。A1 系统的显著特征是，系统的设计者必须按照一个正式的设计规范来分析系统。

这信息安全保障阶段，欧洲四国（英、法、德、荷）提出了评价满足保密性、完整性、可用性要求的信息技术安全评价准则（ITSEC）后，美国又联合以上诸国和加拿大，并会同国际标准化组织（OSI）共同提出信息技术安全评价的通用准则（CC for ITSEC），CC 已经被五个技术发达的国家承认为代替 TCSEC 的评价安全信息系统的标准，且将发展成为国际标准。

2.3.2.2 国际通用准则（CC）

CC 是国际标准化组织统一现有多种准则的结果，是目前最全面的评价准则。1996 年 6 月，CC 第一版发布；1998 年 5 月，CC 第二版发布；1999 年 10 月 CC V2.1 版发布，并且成为 ISO 标准。CC 的主要思想和框架都取自 ITSEC 和 FC，并充分突出了“保护轮廓”概念。CC 将评估过程划分为功能和保证两部分，评估等级分为 EAL1、EAL2、EAL3、EAL4、EAL5、EAL6 和 EAL7 共七个等级。每一级均需评估 7 个功能类，分别是配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试和脆弱性评估。

回顾 CC 全标准发展的过程：第一个有关信息技术安全评价的标准诞生于八十年代的美国，就是著名的“可信计算机系统评价准则”（TCSEC，又称橘皮书）。该准则对计算机操作系统的安全性规定了不同的等级。从九十年代开始，一些国

家和国际组织相继提出了新的安全评价准则。1991 年，欧共体发布了“信息技术安全评价准则”（ITSEC）。1993 年，加拿大发布了“加拿大可信计算机产品评价准则”（CTCPEC），CTCPEC 综合了 TCSEC 和 ITSEC 两个准则的优点。同年，美国在对 TCSEC 进行修改补充并吸收 ITSEC 优点的基础上，发布了“信息技术安全评价联邦准则”（FC）。1993 年 6 月，上述国家共同起草了一份通用准则（CC），并将 CC 推广为国际标准。CC 发布的目的是建立一个各国都能接受的通用的安全评价准则，国家与国家之间可以通过签订互认协议来决定相互接受的认可级别，这样能使基础性安全产品在通过 CC 准则评价并得到许可进入国际市场时，不需要再作评价。此外，国际标准化组织和国际电工委也已经制订了上百项安全标准，其中包括专门针对银行业务制订的信息安全标准。国际电信联盟和欧洲计算机制造商协会也推出了许多安全标准。

实际上，CC、ISO/IEC 15408、GB/T 18336 是同一个标准，只不过 CC 是最早的称谓，15408 是正式的 ISO 标准，18336 则是我国等同采用 15408 之后的国标。

国际标准 ISO/IEC 15408 是由联合技术委员会 ISO/IEC JTC1、信息技术与通用准则执行委员会、通用准则方案发起组织的成员组成的一个实体合作而准备的。ISO/IEC 15408 的同样的文章作为通用准则发表，被认定为信息技术安全性评估通用准则 2.0 版。通用准则附加信息和与它的发起组织的联系信息由第 1 部分的附加部分提供。ISO/IEC 15408 在“信息技术安全性评估准则”由以下几部分组成：

第 1 部分：简介和一般模型

第 2 部分：安全功能要求

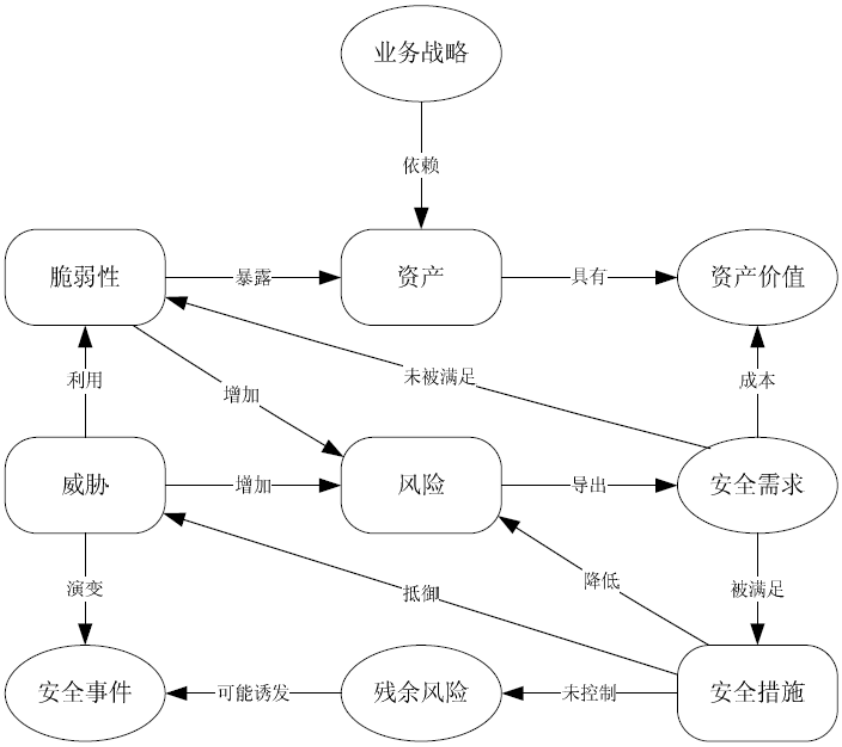
第 3 部分：安全保证要求

2.4 中国信息安全标准

2.4.1 中国国家信息安全标准

2.4.1.1 信息安全风险评估规范（GB/T20984-2007）

GB / T 20984—2007《信息安全技术 信息安全风险评估规范》提出了风险评估的基本概念、要素关系、分析原理、实施流程和评估方法，以及风险评估在信息系统生命周期不同阶段的实施要点和工作形式。这个标准适用于规范组织开展的风险评估工作。风险要素关系图说明了构成风险的各要素间的紧密性和关联性。



图示 7：风险要素关系图

2.4.1.2 信息系统安全等级保护

为了进一步提高信息安全的保障能力和防护水平，维护国家安全、公共利益和社会稳定，保障和促进信息化建设的健康发展，1994 年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》规定，“计算机信息系统实行安全等

级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。2003 年中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）明确指出，“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。

信息安全等级保护是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

根据信息和信息系统在国家安全、经济建设、社会生活中的重要程度；遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度；针对信息的保密性、完整性和可用性要求及信息系统必须要达到的基本的安全保护水平等因素，信息和信息系统的安全保护等级共分五级：

1. 第一级为自主保护级，适用于一般的信息和信息系统，其受到破坏后，会对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益。

2. 第二级为指导保护级，适用于一定程度上涉及国家安全、社会秩序、经济建设和公共利益的一般信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成一定损害。

3. 第三级为监督保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成较大损害。

4. 第四级为强制保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成严重损害。

5. 第五级为专控保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统的核心子系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成特别严重损害。

2.4.2 中国行业信息安全标准

2.4.2.1 商业银行信息科技风险管理指引

为进一步加强商业银行信息科技风险管理，银监会发布《商业银行信息科技风险管理指引》，原《银行业金融机构信息系统风险管理指引》（银监发［2006］63 号）同时废止。

新《指引》具有以下几个特点：一是全面涵盖商业银行的信息科技活动，进一步明确信息科技与银行业务的关系，对于认识和防范风险具有更加积极的作用；二是适用范围由银行业金融机构变为法人商业银行，其他银行业金融机构参照执行；三是信息科技治理作为首要内容提出，充实并细化了对商业银行在治理层面的具体要求；四是重点阐述了信息科技风险管理和内外部审计要求，特别是要求审计贯穿信息科技活动的整个过程之中；五是参照国际国内的标准和成功实践，对商业银行信息科技整个生命周期内的信息安全、业务连续性管理和外包等方面提出高标准、高要求，使操作性更强；六是加强了对客户信息保护的要求。

新《指引》共十一章七十六条，分为总则，信息科技治理，信息科技风险管理，信息安全，信息系统开发、测试和维护，信息科技运行，业务连续性管理，外包，内部审计，外部审计和附则等十一个部分。新《指引》的发布，将进一步推动中国银行业信息科技风险管理向更高水平迈进。

2.5 安全技术发展趋势

随着“电子化”社会越来越快的发展，信息安全产业也处在一个飞速的演进过程中。各种新技术、新思路层出不穷。这个产业正面临巨大的变化。

2.5.1 新概念新技术

云计算、虚拟化、3G 网络、无线局域网(WLAN)和无线应用协议(WAP)及其无线安全技术也日渐成为业界关注的焦点。

新概念安全产品的出现。安全产业正在从原有的防火墙、应急响应系统、风险评估系统等各种产品离散建立的情况中走出，各种产品之间相互融合，取长补短，成为一个完整的信息安全体系，这种兼有两种或者几种功能的产品正在逐渐走向成熟。

人工智能、行为学、对策理论在信息安全领域的应用。传统的网络安全研究侧重于防护，但是随着入侵网络和系统的技术和手段的复杂化，直接面向入侵者的攻防对战不可避免。目前的入侵检测产品，绝大多数基于现有的规则或入侵模式，而应急响应，更是主要有人工来进行分析，未来新学科在这些领域的应用，将改变网络防护的目前这种耗时耗力的被动局面。

2.5.2 信息安全行业转型

企业转向安全整体解决方案。企业对信息安全的投入持续增加，企业正从部署单一的网络安全产品向寻求信息安全整体解决方案转型。信息安全解决方案市场的出现和发展，既是中国信息化建设需求带动的结果，也是信息安全领域向全方位、纵深化、专业化方向发展的客观要求。

信息安全服务崭露头角。信息安全服务已成为信息安全整体解决方案的重要组成部分。近年来，有相当数量的专业信息安全服务解决方案提供商在市场上出现。信息安全服务从一开始就贯穿在整个的安全体系中，从售前的安全咨询、安全风险评估，到安全平台搭建项目实施，一直延续到售后的安全培训、技术支持、系统维护、安全平台升级等项目周期的全过程。

2.5.3 “云安全”

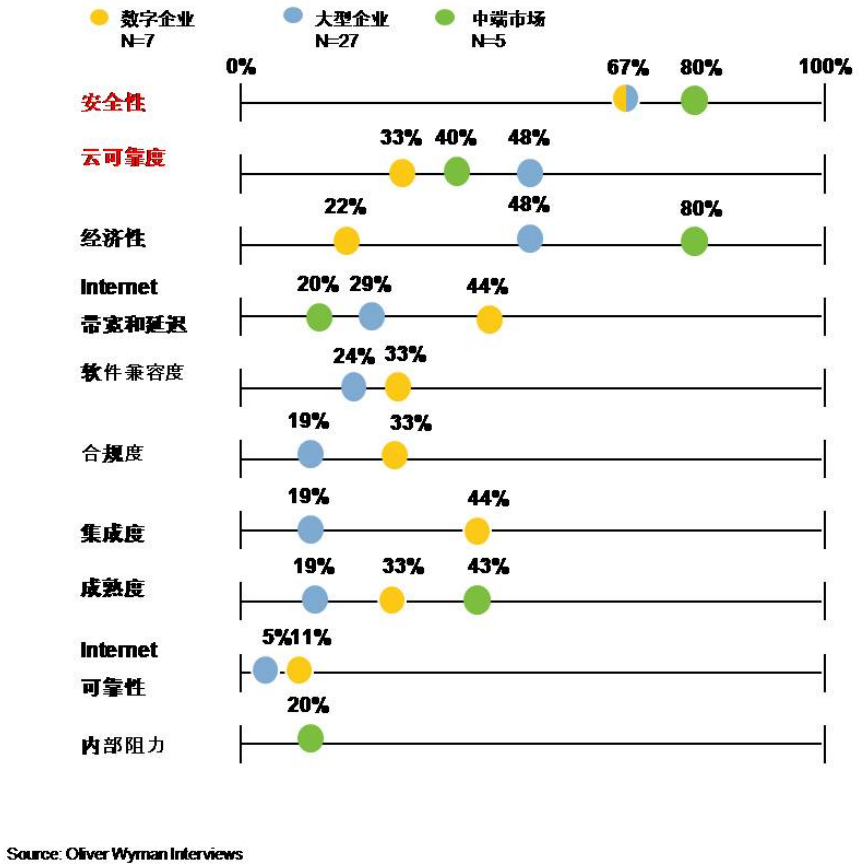
云计算的演变从1990年左右开始，经历了网格计算、效用计算、软件即服务（SaaS）几个阶段。伴随着云计算概念的提出以及各种关于云概念的推广，

“云安全”的关注度也与日俱增。无论是云计算服务提供商还是使用云计算相关服务的企业，他们在信息安全领域的建设都正面临着新的挑战。

目前云计算相关的安全关注点主要是：

- **可靠性:** 高可靠性将成为主要的担心，特别是关键业务应用，足够的可靠性保障将成为这些业务迁移到云计算平台的前提。
- **数据安全:** 迁移应用到一个共享的网络和计算平台增加了潜在的数据暴露给非授权用户访问的风险，身份认证和访问技术变得日益重要。
- **合规:** SOX,HIPPA 等法规的要求将限制某些应用在云计算平台上使用，更全面的审计功能将成为必备的能力。
- **安全管理:** 云计算供应商必须提供易用、直观的防火墙和相关安全配置的管理方式，以保护云中的应用及其运行环境。
- **缺乏控制：** 由于云计算模式降低了企业和组织对资源的控制，供应商必须提供足够的安全透明度，以打消他们的顾虑。

安全性，可靠性和经济性是“云”最大的关注点。安全通常是新的IT解决方案中首要关注的问题，在云计算环境中，用户将主要关注云计算的安全性和可靠性。同时，大型企业普遍认为“云”可以为企业提供满意的安全解决方案。客户对“云安全”风险点的关注度如下一页图所示。



图示 8： “云安全”风险点

2.5.4 “SOA 安全”

面向服务的体系结构(service-oriented architecture. SOA)是一个组件模型。它将应用程序的不同功能单元(称为服务)通过这些服务之间定义良好的接口和契约联系起来。接口是采用中立的方式进行定义的。它应该独立于实现服务的硬件平台、操作系统和编程语言。这使得构建在各种这样的系统中的服务可以以一种统一、通用的方式进行交互。

安全访问信息是任何业务的前提和基础。所以安全性是SOA中的一个焦点问题，根据SOA的设计和实施原则，安全已经成为SOA实施过程中非常关键的架构基础。安全总体原则适用于任何环境，不论是SOA还是云计算，都是相同的：身份，身份验证，授权，机密性，完整性，审计和遵守，策略管理和可靠性。安全管理的概念渗透于面向服务的生命周期的每一个环节。

SOA安全主要关注点如下：

- 安全不仅仅是技术需求，而成为业务需求；
- 基于 SOA 的企业架构关注身份识别及相关安全挑战；
- SOA 环境下的安全挑战包括如下：

  - 跨组织用户和服务的身份识别。
  - 许多基本事务需要不同组织间实时的、无缝的连接。
  - 确保整合应用有足够的安全控制措施。
  - 对建立在新、旧技术平台上，混合而成的系统和服务进行身份和安全管理。
  - 不仅需要保护数据在传输过程中的安全，还要保护数据在整个生命周期中的安全。
  - 政府、行业、企业本身在合规方面的安全要求。

SOA安全需要包括整个生命周期的发展，通过建模，组装，部署和管理SOA应用程序来获得实现。

2.6 企业信息安全架构

企业信息安全架构是企业根据自身对信息安全的需求，制定的一个切实可行的安全体系。它涵盖了企业信息系统的基础安全服务和架构、安全运维、安全治理、风险管理和合规等几个子系统。

由于企业信息安全建设需求的不同，各企业的信息安全架构存在着较大的差异，因而直接照搬其它企业信息安全架构的方法并不可行。另外，信息安全架构涉及企业的业务流程和组织架构以及安全合规等问题，不是简单的安全产品的堆砌。可以说，企业信息安全架构的设计和建设是一个极其复杂的系统工程，不是单一产品和技术平台可以解决的。

在企业信息安全架构的设计和建设中，企业还应该认识到，信息系统中信息的交互和安全风险是并生共存的。企业信息安全架构的设计和建设并不能实现绝

对的信息安全，除非切断所有的信息流动和共享，然而这将导致信息系统失去其存在的意义。

实际上，设计和建设企业信息安全架构的意义在于，通过科学的安全机制和方法，将信息系统的安全维持在一个可接受的安全水平线上。好的安全机制可以减小风险所带来的损失，比如赋予某合法用户访问权的时候，限定其数据访问区域，不允许该用户访问其它区域的数据。这样，即使攻击者通过某些手段获得了该用户的访问权限，也只能访问部分数据，从而达到将损失限制在一定范围的目的。

在企业信息安全架构的设计和实现中，还有一个需要关注的内容：安全措施应有一个合适的平衡点，不应该影响企业业务的正常运营以及用户的工作习惯。举个例子：一般的安全认证措施都会通过密码验证，管理员为加强安全性会要求用户定期更改密码；如果片面追求更改密码的频率，将会给用户带来使用上的困扰，有可能迫使某些用户将密码写在变笺纸并贴在电脑上，这样安全性反而降低了。

2.6.1 企业信息系统安全威胁

知己知彼，百战不殆！我们有必要先对企业信息系统所面临的威胁做一定的了解，这将有助于我们更好的理解企业信息安全架构所需要考虑的需求。传统概念中，企业信息系统安全威胁似乎就是黑客入侵等导致信息资产损坏的行为。事实上，在企业信息安全体系中，信息安全及其关联的信息资产有着更为广泛和科学的范围。

造成企业威胁的因素可分为人为因素和环境因素。根据威胁的动机，人为因素又可分为恶意和非恶意两种。环境因素包括自然界不可抗的因素和其它物理因素。威胁作用形式可以是对信息系统直接或间接的攻击，在保密性、完整性和可用性等方面造成损害；也可能是偶发的或蓄意的事件。

企业信息安全考虑威胁的来源包括：

来源		描　述
环境因素		断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、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、数据、通讯线路等方面的故障。
人为因素	恶意人员	不满的或有预谋的内部人员对信息系统进行恶意破坏；采用自主或内外勾结的方式盗窃机密信息或进行篡改，获取利益。 外部人员利用信息系统的脆弱性，对网络或系统的保密性、完整性和可用性进行破坏，以获取利益或炫耀能力。
	非恶意人员	内部人员由于缺乏责任心，或者由于不关心或不专注，或者没有遵循规章制度和操作流程而导致故障或信息损坏；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。

我们可以根据以上威胁的表现形式，对这些威胁进行进一步的分类和分析：

种类	描述	威胁子类
软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷等问题。	设备硬件故障、传输设备故障、存储媒体故障、系统软件故障、应用软件故障、数据库软件故障、开发环境故障等。
物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害。	断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等。
无作为或操作失误	应该执行而没有执行相应的操作，或无意执行了错误的操作。	维护错误、操作失误等。
管理不到位	安全管理无法落实或不到位，	管理制度和策略不完善、管

	从而破坏信息系统正常有序运行。	理规程缺失、职责不明确、监督控管机制不健全等。
恶意代码	故意在计算机系统上执行恶意任务的程序代码。	病毒、特洛伊木马、蠕虫、陷门、间谍软件、窃听软件等。
越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的权限，做出破坏信息系统的行为。	非授权访问网络资源、非授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等。
网络攻击	利用工具和技术通过网络对信息系统进行攻击和入侵。	网络探测和信息采集、漏洞探测、嗅探（帐号、口令、权限等）、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏等。
物理攻击	通过物理的接触造成对软件、硬件、数据的破坏。	物理接触、物理破坏、盗窃等。
泄密	信息泄露给不应了解的他人。	内部信息泄露、外部信息泄露等。
篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用。	篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息等。
抵赖	不承认收到的信息和所作的操作和交易。	原发抵赖、接收抵赖、第三方抵赖等。

2.6.2 企业信息安全子系统

随着协作业务模式、高明的犯罪攻击以及越来越复杂的 IT 基础设施的出现，现有的从战术上独立实施的安全技术已经不足以应对新的风险。企业的应对方式应跨跃多个信息安全技术领域，从战略的高度端到端的管理风险：

人员和身份识别：保障合法用户在允许的时间访问合适的资源

人员和身份识别子系统是整个信息安全系统的基础，它一方面提供了有效的访问控制能力，另一方面实现了基于人员和身份的管理。获得授权的用户可以访问基础设施，数据，信息和服务。同时，其访问范围受到了其身份和权限的控制。人员和身份的识别可以采取多种方式进行，包括物理身份证或逻辑令牌或用户标识符等。

数据和信息：保障数据在传输及整个生命周期中的安全

数据和信息子系统主要负责对分布在企业各个信息系统中的数据和信息进行安全防护。数据和信息是企业的核心资产，信息系统中的数据和信息在存储、转移、使用、传输、交换等过程中，都有可能受到安全威胁。数据和信息子系统通过对资产进行分类统计、分配属性、设定强制访问策略、审计、加密等措施实现对数据和信息的保护。

应用和流程：保障应用和业务服务的安全

应用和流程子系统负责对企业业务应用的整个生命周期进行安全防护，它涵盖了从应用的设计开发、实施到使用的整个过程，使应用在其整个生命周期中获得有效的控制和安全的保护。另外企业的应用和业务安全还需要考虑行业或地区法律法规的遵从等内容。

网络、服务器和终端：保障信息系统基础架构的安全

网络、服务器和终端子系统主要面向企业信息系统的基础架构，它通过对存在于基础架构中安全隐患的主动监控和控制，避免或减少技术设施带来的风险，确保上层应用系统的安全和稳定。该子系统一般会通过部署相应的安全防护产

品，结合安全监控、安全管理、应急响应预案等安全措施，来达到预期安全防护的目的。

物理基础架构：保障信息系统有关物理设施和环境的安全

物理基础架构子系统负责保护企业信息系统的物理基础设施和环境。物理基础设施和环境的损坏将极大的影响企业信息系统及其业务的连续性。该子系统涉及到的内容可能包括物理访问控制设施和环境被破坏，关键物理设施的损坏或丢失等。物理基础架构安全子系统通常需要通过一个有效、集中的监控系统，实现对有关资源的集中管理和监控，包括：物理设施、员工、客户、公用场所甚至天气情况等。

在信息安全的理论体系中，这五个层面不是孤立的，它们是相辅相成的。企业在设计信息安全系统时必须全面考虑信息安全体系的各个层次，并结合自身具体情况进行有所侧重的规划和设计。只有通过对以上安全子系统的深入分析，才能建立起一个强大的安全矩阵，有效的应对各种安全风险和威胁。

2.6.3 完整的企业信息安全架构

今天，企业的管理决策层需要去关注威胁企业的各种风险，如 CFO 管理财务领域的风险。对于信息系统而言，企业面临的安全风险和潜在影响同样需要得到企业管理决策层的关注。企业信息系统同样需要考虑管理以及安全运维的风险，并实现对法律法规的遵从。

企业信息安全系统需要和企业的生产系统有效关联，通过对信息系统、业务系统的整体管理和优化，达到安全生产、生产安全的最终目标。

作为一个企业，要加强业务流程的安全，需要从业务驱动的角度出发来指导信息安全系统的设计和建设，以确保所有不同安全领域的工作能以全面合作和协同的方式进行，从而实现总体的业务安全目标。否则，企业会因为缺乏信息系统策略的合理性而导致企业面临信息安全风险，削弱信息系统对企业生产业务支撑

的可靠性。

然而，基于标准的方法实现企业业务系统和信息安全系统之间的关联映射，对于企业来说往往是是一件非常困难的事情，并难以在企业信息系统建设的初期得以考虑。

一方面是企业构建信息安全架构的重要性和必要性，一方面是信息安全架构构建的复杂性和不确定性。为解决这一困扰信息系统建设的难题，企业需要一个全面的、完整的企业信息系统安全框架。企业在该框架的指导和建议下，可以全面的，有条理的完成企业信息系统的规划和建设，并确保在企业信息安全架构中对一切必要的信息安全领域进行有效的管理。

第三章 企业信息安全框架概述

3.1 企业信息安全实践的挑战

企业信息安全需要从全方位的视角去管理，而不是通过单一系统或程序来实现。企业战略，安全标准，作业流程，安全组织，规范制度，甚至安全工具与实施手段等都是环环相扣的，都是企业实现信息安全建设目标的必要因素。

在企业越来越复杂的信息环境中，使用传统的系统方法开发信息安全解决方案时往往会遇到很多挑战，例如：系统安全平台需求开发的困难性；多平台，多组件架构的安全功能平台整合的复杂性，以及安全解决方案实施的多样性。这些都会使企业在实际的安全实践中陷入困境。

尽管业界的安全标准和相关最佳实践使得开发一个可扩展的信息安全架构的困难减少了很多，但在具体过程中仍然存在着很多障碍。

本章将主要介绍一个更为全面和周详的企业安全架构建设的范本——企业信息安全框架（ESF　Enterprise Security Framework v5.0)。企业信息安全框架（ESF　v5.0）可以帮助我们全面理解和解决企业 IT 基础架构中与安全有关的各种问题。通过这个全面的 ,基于安全最佳实践和业界相关开放标准的安全模型，可以帮助企业定位安全建设的现状、了解安全建设的需求、组织未来安全建设的规划和实施。

3.2 企业信息安全框架（ESF v5.0）的定义

在各种风险日趋复杂化的今天，企业的决策层希望能够获得有效的手段来管理和控制其责任范围内的各种风险。他们需要了解安全风险对信息系统以及相关业务所产生的潜在影响 ;需要获得应对这些风险的快速有效的措施来保障相关业务的可用性和稳定性。与此同时，他们还需要通过加强合规管理、业务流程优化来提高企业安全风险管控。

企业信息安全系统中的各个安全组件或要素只有整合成为一个整体协同作

用时，才能有效保证企业整体安全管控的目标得以实现。然而，对于大多数企业或组织来说，在信息安全建设之初，如何根据企业业务发展的需要，确立合理的信息安全需求、确立企业信息安全架构，选择安全功能组件往往是一件非常困难的事情。

企业信息安全框架（ESF v5.0）旨在为企业提供一个全面的，基于信息安全建设最佳实践的，以及结合了业界相关开放标准的安全模型。为企业提供一个自上向下的，整体的信息安全建设视图，参见下图所示。

图示 9：ESF v5.0 企业信息安全框架

企业信息安全框架（ESF v5.0）从上到下由安全治理、风险管理及合规层，安全运维层和基础安全服务和架构层三个层次构成。安全治理、风险和合规作为 ESF 架构顶层的核心内容，是第二层安全运维的服务对象，同时，它们也是企业信息安全策略制定的基础和依据，此外，这一层也为最下层，基础安全服务和架构层中的各个子系统提供选择和建设的依据。

基础安全服务和架构层是企业信息安全建设技术需求和功能的实现者。是企

业信息安全建设的重要支柱。

中间的安全运维层则通过对信息安全基础服务所提供的功能，结合安全运维管理的流程，来实现安全治理、风险管理和合规的要求，从而保障业务系统的安全风险管理需求。

- 安全治理、风险管理和合规

  安全治理和风险管理及合规的内容主要包含企业信息安全建设的战略和治理框架、风险管理框架以及合规和策略遵从。安全治理、风险管理合规是企业信息安全框架的最顶层，是业务驱动安全的出发点。通过对企业业务和运营风险的评估，确定其战略和治理框架、风险管理框架，定义合规和策略遵从，确立信息安全文档管理体系。

- 安全运维

  安全运维是指在安全策略的指导下，安全组织利用安全技术来达成安全保护目标的过程。安全运维与 IT 运维相辅相成、互为依托、共享信息与资源。

  安全运维与安全组织联系紧密，融合在业务管理和 IT 管理体系中。安全运维包含威胁分析与预警，安全状态和事件的监控，安全事件或事故的响应，以及基于安全目标的操作行为和日志审计，这些安全运维的任务主要可通过安全事件监控、响应、审计和相应的安全策略体系共同完成。

- 基础安全服务和架构

  基础安全服务和架构定义了企业信息安全框架中的五个核心的基础技术架构和相关服务：物理安全、基础架构安全、身份/访问安全、数据安全和应用安全。基础安全服务和架构是安全运维和管理的对象，其功能由各自的子系统提供保证。

  企业信息安全框架（ESF v5.0）完整地覆盖了企业信息安全建设的全部内容，

并详细说明在今后的实际工作中如何利用这一架构来指导安全工作。

企业信息安全架构（ESF v5.0）描述了企业每一个关键安全组件的设计，通过开发与应用适当的安全技术来保护信息资产，并结合质量流程把风险降低到可接受的水平。

企业信息安全架构（ESF v5.0）为企业提供了必要的安全理念来保护业务流程，从而使企业的信息资产免受来自内部和外部的威胁，

企业信息安全架构（ESF v5.0）同时也为帮助企业开展信息安全方案设计，实现安全建设的目标提供了架构指南。

3.3 企业信息安全框架建设的意义

企业信息安全框架（ESF v5.0）旨在给企业信息安全建设提供一个集成的、标准的企业信息安全框架，帮助企业快速知晓企业信息安全现状和需求，为企业信息安全平台的建设、设计、实施提供指导和参照。包括：

- 帮助企业了解企业信息安全建设的整体状况；
- 帮助企业找出现有安全系统可能存在的差距 ；
- 帮助企业识别业务风险 ，系统了解风险状况；
- 帮助企业在完全建设中合理定义安全需求和建设方向；
- 全面分析评估企业信息安全政策、标准和指南及其日常执行情况，衡量其是否能够有效保障公司的信息安全；
- 帮助企业制定核心信息安全管理流程，初步建立有效的信息安全体系；
- 完善企业的信息安全架构蓝图及路线图。

第四章 企业信息安全框架

企业信息安全框架为企业提供了一个整合的、标准化的企业级信息安全建设的范本。企业可以基于这一框架迅速的定位目前企业安全能力的现状， 并以这一框架为指导，对企业未来信息安全的各个平台进行设计和实施。

本章将进一步阐述企业信息安全框架的详细内容。

4.1 安全治理、风险管理和合规

4.1.1 战略和治理框架

4.1.1.1 企业安全治理的挑战和需求分析

信息安全并不是企业单一部门的使命，而是全体员工的共同责任。企业对信息系统的依赖意味着更易受到安全威胁的破坏，面对公共和私人网络的互联、信息资源的共享以及信息系统本身的设计漏洞，技术手段有时也无能为力。信息安全管理不能脱离日常业务流程，企业需要建立全体员工共同遵守的信息安全管理制度。

企业信息安全架构规划涉及到管理和技术两方面的内容，而不是单一系统或工具能实现的。如果想凭借企业内部管理人员的经验、技术人员的执行力来完成架构规划，不仅需要大量的时间，更需要精力去不断地磨合与调整。

4.1.1.2 企业安全治理概述

信息安全治理不同于信息安全管理。从工作内容看，安全管理一般是从具体的操作层面出发，针对信息系统具体安全目标的实现所采取的行动。而安全治理则是在宏观层面的战略角度上，对信息安全战略上的过程、结构和联系进行梳理和监控，以确保组织信息系统的安全运营管理能够始终沿着正确的方向演进。

从执行主体看，安全管理是由专业的信息系统安全管理人员执行，而安全治理则是组织高层领导机构的工作。从技术深度看，进行安全管理涉及到很多具体

的信息安全技术，要求具有充分的安全专业知识；安全治理则更多地运用管理学相关知识，从组织整体战略和目标角度描述和控制信息系统安全状态，而很少使用具体的信息安全技术。

因此可以说，安全治理为组织的信息安全运作定义了一个战略性的框架，指明了具体安全管理工作的目标和权责范围，使信息系统安全专业人员能够准确地按照组织高层领导的要求开展工作。

4.1.1.3 企业安全治理的工作及应用

安全战略体现了企业高层经理对企业安全架构的需求，体现了业务对安全的要求，反映了信息安全的价值。另一方面，信息安全要求主要来源于国家相关法律法规、监管机构要求及国家行业标准。安全原则对企业未来安全建设方向的抉择提供了依据。

通常业界通用的安全原则如下，企业需要根据通用安全原则和本企业的业务需求明确企业自身的安全原则。

- 最少准入特权（Least Privilege）
- 深入防御（Defense in Depth）
- 狭窄进入通道（Choke Point）
- 最弱点原则（Weakest Link）
- 故障无碍位置（Fail-Safe Stance）
- 全面参与安全控制（Universal Participation）
- 防御手段多样化（Diversity of Defense）
- 防御机制简单化（Simplicity）
- 安全机制区域划分（Compartmentalization）
- 内外安全防御能力（Protect against insider as well as outsider threats）

安全治理的成功因素

观念转变：在最高管理层（董事会）树立和维护信息安全战略地位的思想认识，建立 IT 战略与信息安全战略的互动观念，清晰阐明信息安全应担当的角色，从业务的视角创造信息技术指导原则。

业务驱动：从组织的业务战略出发而不是从系统的需求出发，可以避免脱离目标而进行建设的困境。从业务的变革出发而不是从技术的变革出发，有利于充分利用组织的现有资源来满足关键需求，从而避免建立的信息安全系统无法有效地支持组织的决策。

信息安全管理体系是信息安全保障体系的一个重要组成部分。信息安全管理体系框架是从企业管理的层面出发，按照多层防护的思想，为实现信息安全战略而搭建的。

信息安全管理体系由几下几部分组成：

- 安全政策，标准——管理规定

信息安全政策与标准是信息安全管理、运作、技术体系标准化、制度化后形成的一整套对信息安全的管理规定，是安全意识培养的内容来源，是组织管理控制和审计的依据，是技术方案必须遵从的基础要求。

- 安全组织——管理控制

通过完善的组织架构，明确不同安全组织、不同安全角色的定位和职责以及相互关系，对信息安全风险进行控制管理。这里包含了“管理”和“监控”两方面的含义，特别是对专职的信息安全管理部门而言，“监控”是极其重要的职责。

管理控制的落实需要通过标准、安全意识培养和审计工作进行保障和监督，同时它又是信息安全标准、安全意识培养和审计工作开展的重要对象。

- 安全意识培养——宣传教育

员工在信息安全方面的自我约束、自我控制，是信息安全管理体系的一个重

要层次。安全意识培养是信息安全管理控制的基础，实际工作中大部分的信息安全控制需要依靠员工的主观能动性。

安全管理的最终目标是建成一体化的、规范的，具有国际水平，符合中国国情，体现企业特色的信息安全管理和运营机制，为企业安全运行和可持续运营提供有力的保障。

4.1.2 信息安全风险管理

4.1.2.1 信息安全风险管理的挑战和需求分析

一个机构要利用其拥有的资产来完成其使命。在信息时代，信息成为第一战略资源，更是起着至关重要的作用。因此，信息资产的安全是关系到该机构能否完成其使命的大事。资产与风险是天生的一对矛盾，资产价值越高，面临的风险就越大。信息资产有着与传统资产不同的特性，面临着新型风险。信息安全风险管理的目的就是要缓解和平衡这一对矛盾，将风险处理到可接受的程度，保护信息及其相关资产，最终保证机构能够完成其使命。

信息安全风险管理是信息安全保障工作中的一项基础性工作，主要表现在以下几方面：

信息安全风险管理体现在信息安全保障体系的技术、组织和管理等方面。在信息安全保障体系中，技术是工具，组织是运作，管理是指导，它们紧密配合，共同实现信息安全保障的目标。信息安全保障体系的技术、组织和管理等方面都存在着相关风险，需要采用信息安全风险管理的方法加以控制。

信息安全风险管理贯穿信息系统生命周期的全部过程。信息系统生命周期包括规划、设计、实施、运维和废弃五个阶段。每个阶段都存在着相关风险，同样需要采用信息安全风险管理的方法加以控制。

企业运营永远存在各类风险因素，成功的企业能够预知风险所在，进而通过管理风险或是转移风险来提升自身的竞争力。面对不断推陈出新的信息科技，如

何能以最有效的资源及时掌握，并控制新的信息风险因素，已经成为企业主管的重要挑战。

- 关注企业安全，希望了解其安全漏洞
- 需要维护安全控制，以在可控成本内，有效的确定其业务需求
- 将攻击的可能性降至最低，同时建立快速的业务增长方案
- 需要对企业整体安全具有大局观，从而实施解决方案，以确定问题根源，将其解决
- 如何理解政府和/或行业规定
- 如何运用政策和标准，以保证其一致性

4.1.2.2 信息安全风险管理概述

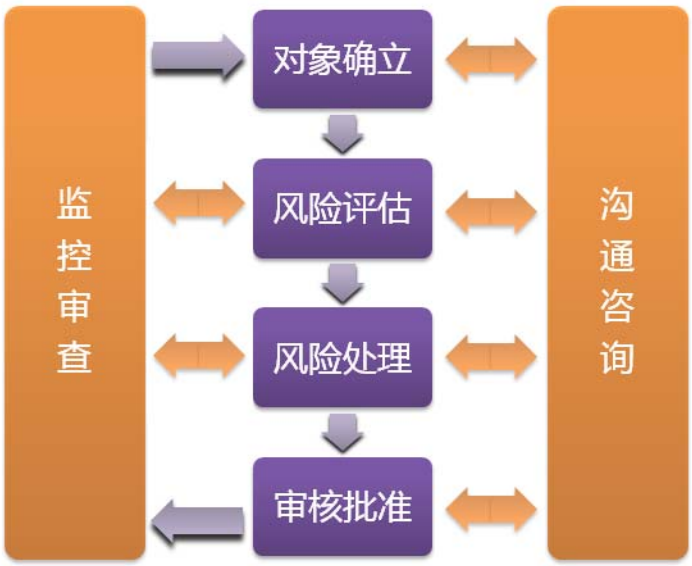
风险管理的目的在于控制企业内安全风险在可以接受的范围内，避免因为信息安全而造成企业的严重损失。风险管理的方法是一个系统化的过程，通过事先建立之评定标准及方法，确定企业重要信息资产或体系，分析及评估企业面临的风险（如威胁、弱点，业务面、法规及信息安全要求）；然后通过制定适当的风险处理计划，采取适当的处理措施（如避免、移转、降低风险等），将企业安全风险控制在能够接受的范围内。

信息安全风险管理是基于风险的信息安全管理，也就是，始终以风险为主线进行信息安全的管理。

从概念上讲，信息安全风险管理涉及到信息安全上述三个方面（即信息、信息载体和信息环境）中包含的所有相关对象。对于一个具体的信息系统，信息安全风险管理主要涉及到该信息系统的关键和敏感部分。因此，根据实际信息系统的不同，信息安全风险管理的侧重点，即重点选择的风险管理范围和对象有所不同。

4.1.2.3 信息安全风险管理的工作及应用

信息安全风险管理包括对象确立、风险评估、风险处理、审核批准、监控与审查和沟通与咨询六个方面的内容。对象确立、风险评估、风险处理和审核批准是信息安全风险管理的四个基本步骤，监控与审查和沟通与咨询则贯穿于这四个基本步骤中，如图所示：



图示 10：信息安全风险管理的内容和流程

第一步骤是对象确立，根据要保护系统的业务目标和特性，确定风险管理对象。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。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。第四步骤是审核批准，包括审核和批准两部分：审核是指通过审查、测试、评审等手段，检验风险评估和风险处理的结果是否满足信息系统的安全要求；批准是指机构的决策层依据审核的结果，做出是否认可的决定。当受保护系统的业务目标和特性发生变化或面临新的风险时，需要再次进入上述四个步骤，形成新的一次循环。因此，对象确立、风险评估、风险处理和审核批准构成了一个螺旋式上升的循环，使得受保护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。

信息安全风险管理与信息系统生命周期的关系

信息系统生命周期是某一信息系统从无到有，再到扬弃的整个过程，包括规划、设计、实施、运维和废弃个基本阶段。

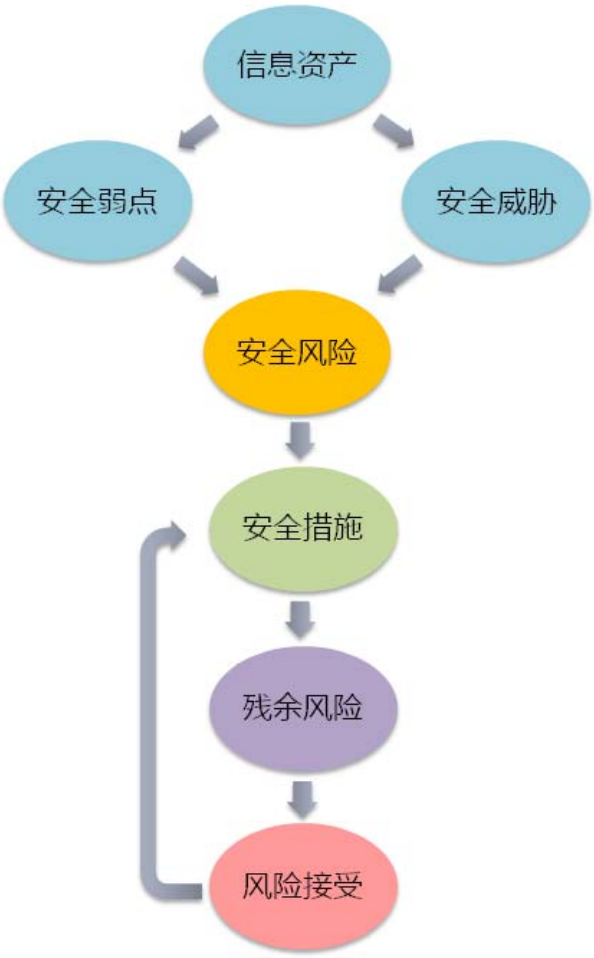
在规划阶段，确定信息系统的目的、范围和需求，分析和论证可行性，提出总体方案。在设计阶段，依据总体方案，设计信息系统的实现结构（包括功能划分、接口协议和性能指标等）和实施方案（包括实现技术、设备选型和系统集成等）。在实施阶段，按照实施方案，购买和检测设备，开发定制功能，集成、部署、配置和测试系统，培训人员等。在运维阶段，运行和维护系统，保证信息系统在自身和所处环境的变化中始终能够正常工作和不断升级。在废弃阶段，对信息系统的过时或无用部分进行报废处理。当信息系统的业务目标和需求或技术和管理环境发生变化时，需要再次进入上述五个阶段，形成新的一次循环。因此，规划、设计、实施、运维和废弃构成了一个螺旋式上升的循环，使得信息系统不断适应自身和环境的变化。

信息安全风险评估概述

风险评估是一个企业实现信息系统安全的必要的步骤，可以协助企业的 IT 决策者们对其业务信息系统的安全建设或安全改造思路有充分的理论依据和更深刻的认识。

通过风险评估，可以帮助企业的 IT 决策者们清楚业务信息系统包含的重要资产、面临的主要威胁、本身的脆弱性；哪些威胁出现的可能性较大，哪些脆弱性问题很严重，可能造成的影响较大；为安全防护措施的选择、制定系统安全策略、构架安全体系提供了充分的依据；更进一步，还可以分析出信息系统的风险是如何随时间变化的，将来应如何面对这些风险。

下图描述了风险评估方法中，威胁和风险评估的基本架构，有助于表述风险和信息安全的关系。



图示 11：风险评估基本架构

以下为威胁和风险评估的方法论简要描述：

- 定义信息资产
- 确定这些资产的弱点和面临的威胁
- 确定这些资产的风险和风险等级
- 确定保护这些资产的安全措施
- 确定残留的风险
- 确定是否接受残留风险。 如果残留风险不能接受，就需要选择额外的安全措施

在选择安全措施时应综合分析安全弱点、风险、威胁以及它们之间的关系，

力求构建最合理的整体安全保护体系。另外，在选择安全措施时，还应考虑到组织、资金、环境、人员、时间、法律、技术和社会文化等多方面的可能限制因素。

4.1.3 合规和策略遵从

4.1.3.1 合规和策略遵从的挑战和需求分析

合规管理的总体发展过程是与外部监管和企业业发展相适应、相磨合的动态过程。例如在市场经济环境下，银行业经营的高风险及其与社会经济的高度关联性，导致银行业的外部监管不断加强。正是源于银行外部监管的相关法律、法规和要求，银行业合规管理得以产生、发展并成为银行专门的管理职能。

在金融行业的合规，可以追溯到上世纪初。美国银行业在十九世纪三、四十年代就已经建立了合规管理的大部分法规，在世界上最早实施银行合规管理。此后，银行业界和外部监管者对合规管理的要求不断发展。英国是世界上建立银行体系最早、最先进的国家，外部合规性监管和商业银行的合规管理一直都比较完备。“金融服务权力机构”（FINANCIAL SERVICES AUTHORITY,简称 FSA）是英国对银行实施合规性监管的政府权威部门。与国际银行业的发展变化相适应，巴塞尔银行监管委员会（” 巴塞尔委员会”）先后在一系列文件中对银行合规问题给予了相应指导，如 1998 年 9 月《银行机构的内部控制制度框架》、1999 年 9 月《健全银行公司制治理》、2001 年 8 月《银行的内部审计以及监管者与审计师的关系》、2001 年 10 月《消费者对银行应有的关注》。2005 年 4 月出台了《银行的合规与合规管理部门》指导性文件。随着经济环境的变化和银行业的发展，近 20 年来监管机构的监管理念和目标发生了很大变化。监管理念从主要考虑宏观经济中金融体系的稳定，保护消费者利益，即消费者主权论，逐渐发展到更多考虑银行作为商业性盈利主体的利益 ,而且更加强调银行安全稳健运行的市场制约理念和在银行内部建立全面有效的风险管理体系以及跨国监管。

另外，合规管理是企业对各项法规、行业规定以及资本市场对上市公司信息披露和内部控制要求等的遵从工作的管理。例如萨班斯法案掀开了在美上市公司完善企业合规管理的变革序幕。由于萨班斯法案对在美上市公司的苛刻要求使得

所有在美上市公司不得不开展了以萨班斯法案遵从为主的合规管理工作。

合规性能确保利用所有适用于企业的法律法规对信息进行处理，并且确保需要时能够按要求进行证明。要实现信息合规性，企业必须定义和实施策略、过程和解决方案，确保信息准确、可靠、完整、可跟踪且可在需要时由授权的用户进行检索。虽然这些需求似乎带来极大压力，但是信息合规性使企业能够最大程度地降低其风险、提高生产力并显著降低法律和运营成本。

4.1.3.2 合规和策略遵从概述

合规，是指使企业的经营活动与法律、规则和准则相一致。法律、规则和准则，是指适用于企业业经营活动的法律、行政法规、部门规章及其他规范性文件、经营规则、自律性组织的行业准则、行为守则和职业操守。合规管理应当遵循独立性、系统性、全员参与、强制性、管理地位与职责明确和科学管理原则。

合规管理与相关部门的关系：

- 一是合规工作与合规管理部门的关系
- 二是合规管理与内部审计的关系
- 三是合规管理部门与业务发展部门的关系
- 四是合规管理与风险管理部门（不仅指资产风险管理部门）的关系
- 五是合规管理与法律事务部门联系

一方面，商业风险与 IT 流程及控制之间的关系，已经成为企业实现合规和策略遵从的基础。企业应该更加明确各种风险，以更好地体现审计的必要性，通过重要风险指标对新风险加以识别和控制。

另一方面，管理的变革已经是影响企业合规和策略遵从的关键。在 IT 环境下，对变革进行有效且有力的管理，包括应用软件与基础设施建设，是企业关注的重要领域。通过结合战略，流程和技术，企业的的合规和策略遵从举措，不但创造了有效且成熟的管理实施流程，还将能够高效且持久的保持合规和策略的遵从

性。

4.1.3.3 合规和策略遵从的工作及应用

合规和策略遵从管理应从以下几个方面考虑：首先需要企业加强对规范策略的认识，了解需要合乎规范和策略的条款和要求，它的范围及对于信息系统的要求；其次，针对企业的信息系统现状和环境进行合规性评估、分析和风险管理，识别战略目标，并划分其优先次序，确立企业需要合规的具体内容和实现方式；然后进行合规性的建设，使用内部控制实施安全遵从性策略，监控并报告法规遵从性，从管理和技术层面落实规范和策略的要求；企业最后还应该建立合规性审计（compliance audit）的流程和机制，对企业是否遵从了监管方针提供综合性评述。

安全遵从包括行业标准和政府法规，如 PCI、FISMA、Basel II、SOX、HIPAA 和 ISO 27001 等。举例而言，SOX（萨班斯法案）是一部由美国颁布，涉及会计职业监管、公司治理、证券市场监管等方面改革的重要法律，包括在美国注册上市公司和在外国注册而于美国上市的公司，都必须遵守该法案。保存或传送如个人健康信息这样的电子医疗记录的医疗服务提供商必须遵守美国医治保险携带和责任法案（HIPAA）。传送信用卡数据的金融服务公司必须遵守 PCI DSS 标准。独立核算、安全或 IT 顾问需对合规准备的优点及全面性做出评价。无论在哪种情况下，被审计的组织都必须通过提供审计跟踪记录（审计跟踪记录通过由事件日志记录管理软件的数据生成）表明自己符合相关规定。

为遵从 SOX 方案，保证会计账务、财务报告、流程、财务应用和底层信息技术基础架构的完整性、可用性和准确性，要求企业的 IT 信息系统从优化财务流程、建立内部控制体系并引入内控管理信息系统及加强 IT 控制等方面有所准备。特别是在业务流程高度依赖 IT 系统支撑的电信与金融行业，重视信息技术控制、完善信息技术控制对满足监管机构要求和企业自身发展都至关重要。

企业通过在一个解决方案中集成安全风险管理和策略遵从性管理两种功能，可以使企业降低风险，并可以对实现策略遵从性的过程进行管理。安全管理人员

可以利用实现策略遵从性的功能，对企业是否符合企业内部安全策略以及企业外部法规的情况进行审核和记录，并可以通过强制手段使企业符合这些策略和法规。

4.2 信息安全运维

随着企业各项业务对信息系统依赖程度逐渐提高，信息系统的复杂度急剧增加。与此同时，信息系统在运维过程中的安全问题变得更加突出。因此业务系统对信息系统提出了越来越高的安全运维要求；另一方面，复杂的业务系统和异构的 IT 环境，也增加了系统安全运维的难度。传统的单一、孤立的安全运维管理已越来越不适应企业系统安全运维管理的需求。所以，安全运维在企业信息安全框架中被作为独立的一层，在企业信息安全规划中加以考虑。其主要包括：安全事件的监控，安全事件或事故的响应，基于安全目标的操作行为日志审计，安全策略和安全绩效评估等。

4.2.1 安全事件监控

4.2.1.1 安全事件监控的挑战和需求分析

随着 IT 安全建设的逐步完善与深入，运维人员就要管理越来越庞大的 IT 系统。仅仅在安全保障方面，公司已经部署相当多的安全设施，但众多的安全技术与安全设备的应用在相当程度上加重了系统与 IT 管理人员的负担。 而在另一方面，安全设备的应用越来越多，安全文件也越来越厚，而安全问题仍时有发生，如下这些就是经常摆在 IT 管理人员面前的问题：

- 在安全方面已经投入很多，基本的安全手段都已具备，为什么安全问题还时有出现？
- 安全项目已经做了很多，安全制度、文件和流程等不下几十个，但面对众多的文档，如何真正的落地？
- 如何才能建立起一套将事前预警、事中监控、事后追溯和应急的处理能力一体化的系统来提升日常运维管理工作中安全机制的效果和效率？

- 如何才能提高安全管理能力，促进安全工作的可视化和可量化，实现可管理的安全服务体系？

过去，企业部署的防病毒、防火墙/VPN、IDS 等安全系统往往仅供技术人员了解某方面的安全防护状况，管理管理层和业务等非技术人员很少能说清楚一个企业的安全到底怎么样了。

安全运维中心实现一个安全可管理、运维的平台。实现类似网管系统的运维人员对网络设备的管理、运维与故障响应一样，使管理层、业务人员、技术人员都可以在安全运营中心系统里找到自己关心的安全信息。

4.2.1.2 安全事件监控概述

安全事件监控的重要功能需求主要包括安全事件的收集、安全事件的归并和过滤、安全事件标准化、安全事件显示和报表。

在企业的信息系统中，存在大量的 IT 资源，这些资源在实际运行中每时每刻都在产生各种类型的事件信息，在这些事件信息中，安全事件是需要安全运维人员重点关注的内容。通过安全事件监控，可以帮助企业积极监控整个组织内的 IT 资源，过滤并关联事件，迅速定位安全威胁，并为安全事件响应提供支持。

但是，企业信息系统中的安全事件类型复杂、数量较大，如何快速的识别和过滤出有效地安全威胁信息，是企业安全运维人员需要重点考虑的问题。

在具体的信息安全系统中，安全事件监控的内容主要包括安全事件的收集、安全事件的归并和过滤、安全事件标准化、安全事件显示和报表等。安全事件监控大多通过单一安全控制台，集中地管理安全事故和漏洞，为企业用户提供安全架构的总体视图，使企业用户能够深入研究网络拓扑，了解受影响的资源的位置并判断问题的真正根源。

4.2.1.3 安全监控的工作及应用

安全事件收集

通常安全事件管理首要功能是安全事件收集，包括支持数据的数据捕获，支持海量安全事件数据处理，支持的安全事件格式包括 SYSLOG，LEA, SYSLOG-NG，W3C 和文件型安全事件在内的多种形式的安全事件格式，可以读取防火墙的配置策略。支持 SYSLOG、SYSLOG-NG、SNMP TRAP、JDBC 数据库连接等实时或定时采集协议。

下表为某电信运营商在安全事件日志收集表：

安全数据源类型	安全资料来源	一般需要收集日志类型	日志收集内容
安全产品	防火墙	Syslog OPSEC	规则变更 连接失败 重要安全事件
	入侵侦测系统	数据库	DOS 攻击 入侵事件（例如端口扫描等） DDOS 攻击
网络设备	交换机、路由器	syslog	网络配置变更 登入信息
主机	Unix 日志	Syslog/sulog	登入信息 SU 等安全事件信息
	W2k 日志	Event log	登陆信息 用户权限使用失败（例如试图关闭系统等） 安全策略更改

安全事件的归并和过滤

安全事件归并和过滤是可选用的功能，过滤用于丢弃从设备提取的原始安全事件信息中监控人员认为不重要的信息，从而减少轻微告警安全事件的干扰；归并是一种组合技术，将基于选定的时间值或安全事件数量，合并具有匹配字段值的多条安全事件。

在安全事件收集引擎和关联分析引擎上都具备安全事件归并和过滤能力。

通过在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，以最大程度地减少发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间地占用。

在关联分析引擎上设置过滤条件，可以过滤掉该类型的安全事件的实时显示，而该安全事件仍然保存到安全事件数据库中。这样既给管理员的实时监控提供了方便，又可以在以后需要的时候察看分析这些安全事件数据。

具有归并技术的安全事件收集代理会在一段时间内比较收到的安全事件，如果安全事件相同，则只发送一条安全事件，该安全事件应包括安全事件详情及该安全事件发生的次数，这样可以减少安全事件通信量。例如，对于每隔 500 毫秒重复一次的安全事件来说，假如归并规则时间阈值设为十秒，这样就会得到 20:1 的安全事件压缩率。从而降低传至关联分析引擎的安全事件流量和数据库的存储空间要求。

对单位时间内发生的大量安全事件，建议按照维护要求和管理部门的考评要求及实际管理情况，对指定安全设备进行告警安全事件归并，也可以通过安全事件严重程度级别、安全事件类别、安全事件标题等安全事件属性进行归并。

安全事件标准化

各种安全事件源在其返回安全事件信息时并非都使用相同的命名约定，为了解决这种“语言不通”的情况，通常可能需要分析人员编写重复的规则并修改每个案例中的安全事件名，以检测相同安全事件的不同返回名称。这样的做法将导

致灵活性和可用性都特别差。

分类法通过广泛和灵活的安全事件映射，对安全事件做标准化处理，它将每条安全事件分配到相应的类别中，这消除了需要学习来自不同厂商的同类产品例如防火墙或 IDS 的信息差别的过程。新的分类法不仅仅提供一系列能满足报告、过滤器和关联的更丰富的资讯，而且还能够精确定义某安全事件资源的种类，即使该设备是一个诸如入侵防护设备的集多种功能集合体，它的安全事件资源也能被精确定义。这样，即使客户日后扩容选用了新的系统，它的安全事件也很容易纳入到整个系统中来，无需更改相应关联规则、过滤器等。

例如，若要分析攻击某服务中漏洞的所有尝试，您可以组合这些安全事件类别：/Host/Application、/Service、/Communicate 和 /Exploit/Vulnerability。这样，您可以使用通用的类别说明，而不是可能随系统变化的安全事件名，来建立规则。分类还可以简化环境中新系统的集成。

安全事件关联分析

安全事件管理中心收集到的安全事件种类多，数量大，为了更有效地对这些海量的安全事件进行分析和处理，确保能在第一时间对各种存在的安全问题采取措施，安全事件管理中心必须具有强大的安全事件处理和分析功能。目前对实践进行处理和分析最有效的方法就是安全事件的关联。

安全事件管理最重要的一个任务就是消除安全基础设施产生的过多误报信息，让安全事件管理人员将注意力集中在真正的威胁和攻击上，避免分析麻痹，所以关联能力是非常重要的。

安全事件显示

事件的可视化显示

安全事件管理系统能够提供列表形式的日志活动频道，操作人员可以在控制台上监视到设备或应用系统产生的实时日志，对相关事故进行告警确认、清除等

操作，或启动相关日志历史信息查询浏览功能。

日志可视化显示应具备如下特点：

- 采用列表的形式显示收集到的日志。
- 可以通过图形化界面实时显示收集到的各种日志，包括原始日志和经过关联后产生的新日志。
- 不同严重程度级别的日志通过不同的颜色显示。
- 各种日志能够查看详细信息，关联性日志必须可以查看它的原始触发日志。
- 为了方便用户查看，分析某一段时间内的日志，实时监视功能可以考虑实现快照功能，获取某一时刻的静态断面。
- 提供通过日志信息中的设备标示，直接启动访问对应设备的仿真终端程序功能。
- 能够提供多种三维形式的动态图表，实时显示某一时刻以来，满足特定条件的不同严重级别日志数量的变化情况。
- 实时显示的内容可以根据不同的用户进行定制，确保不同的用户只看到自己关系的内容。
- 对日志信息提供多窗口显示功能，多个显示窗口应可以分别设置显示过滤条件
- 维护人员可以对每条日志监视窗口设置告警显示过滤条件，只有满足条件的日志信息才报告到监视窗口。日志显示条件可根据日志的级别、类别、日志的标题等条件以及他们的组合来设定。
- 管理维护人员可以制定自己专用的显示过滤条件，也可以存储日志显示过滤条件，和其他操作维护人员共享。

事件监控的报表功能

安全管理平台可以对所有事件、案例、通知、资产和数据库中存储的其他资源创建报表。安全管理系统通常可以提供多种预定义的报告模板，并且集成了报

告编辑器，客户可使用预定义的报告模板生成报告，也可创建新的报告，比如针对客户操作和管理人员的报告。

报告可以立刻生成也可以在指定日期时间生成。

报告可用 PDF、HTML、Excel、CSV 或 RTF 等格式存档。

安全事件管理的报表功能需求通常包括：

- 适合各种类型用户的需求，不同的用户都可以查阅到相关的报表，如适合管理员的运行报表，反映系统各个侧面地分析报表，以及高层管理人员查阅的统计报表。
- 可以通过事先定义好的报表模版库，查看各种格式报表；能够根据用户的不断变化和增加实际要求，定义新的报表模版，并加入到现有的模版库中。
- 报表模板包含数据的内容列表，格式的描述等信息，报表的内容列表可以由安全中心管理人员通过对安全事件数据库中数据的描述生成，也可以由报表模板中已有的字段通过简单的函数生成，可以设置默认的过滤方式、显示格式、排序条目等信息，可以在报表模板中设置由指定列生成的图形〈直方图、曲线图、饼图等〉。
- 可以产生日报表，周报表，月报表，季度报表和年报表，也可以按照选定的一段时间生成报表；
- 生成的报表可以按照标准的，通用的报表格式进行保存和打印，例如 Microsoft Excel，Word 以及 Adobe PDF 格式；
- 报表功能要求支持图文混排格式，方便分析和查看；
- 报表功能能够在多台工作站上浏览和查阅，方便不同人员在不同的地方查看关心的内容。为了减少配置的复杂性，满足该项要求，建议报表功能支持 WEB 浏览器方式。

安全事件监控是安全运维中基础和重要的工作，也是安全运维平台建设首要考虑的建设和内容。

4.2.2 安全事件响应

4.2.2.1 安全事件响应的挑战和需求分析

对于信息系统的安全而言，我们追求的是防患于未然而不是亡羊补牢，只要有可能，我们就应该尽可能的去主动防止安全事件的发生。然而，我们不可能预防所有的安全事件。一旦安全事件发生，我们首先要做的，就是及时响应，将安全事件的影响最小化。对于这一点，仅仅依靠安全防护产品的自动化的防御是不够的。比如：安全防护产品无法防止由于人为错误导致的安全事件。

由于信息系统及相关系统的复杂性和互相关联，为了实现有效的安全事件响应，必须考虑以下方面的工作，包括：制订安全事件响应计划、组建安全事件响应小组、确定团队人员角色等。另外，安全事件响应本身还有着突发性强，对处理人员的综合技术和专业能力要求高等特点，这些都对企业信息系统的管理者提出了不小的挑战。

4.2.2.2 安全事件响应概述

安全事件是指在企业信息系统中出现的影响业务正常运行的任何异常事件，以及安全咨询，病毒库升级，产品升级等事件。例如：破坏系统的完整性、系统资源拒绝服务、通过渗透或者入侵的方式来对系统进行非法访问，系统资源的滥用以及任何可能对系统造成损害的行为等。

安全事件响应需要企业安全人员提供工具、工作流以及报告，可减少攻击识别和补救之间的时间。风险处置流程分为自动响应和工单管理两大部分。

企业针对常见的网络安全问题可以预定义大量规则、活动列表和仪表板视图，通过仪表板用户可以可视化地观察目前网络的关键日志事件（例如：当机、死机、应用、程序死机、重启、非法删除、蠕虫传播、DDOS 攻击、暴力破解等）；通过活动列表（动态更新）可以看到当前出现问题的设备和应用，以及敌意或危险访问的源地址、用户列表等；可以根据需要定义规则的动作，当规则被

触发时采用多种方式向用户发出告警（控制台告警、发邮件、短信通知）或执行预定义的脚本操作、向网管系统发送事件信息（SNMP Trap）。

比如：运行自定义脚本或商业应用程序，发送一个 TCP Reset 到攻击者和受害人以阻止攻击或更改防火墙或路由器上的访问控制列表，等等。

自动响应机制包括：

- 发送一个事件到控制台。
- 设置事件的严重程度。
- 将攻击者和/或受害人添加到查看列表中。
- 执行一个命令（运行用户自定义或商业程序）。
- 发送一个通告或报警。
- 发送一个事件到网管系统。
- 发送一个事件到外部的工单处理系统，比如 Remedy。
- 电子邮件、寻呼、SNMP、短信等。

4.2.2.3 安全事件响应的工作

安全事件响应工作包括以下步骤：

记录日志：当发生安全事件时，企业首先需要对环境现场进行记录，对事件的影响进行详细的描述。安全事件日志对于安全事件的识别、处理和调查非常重要，安全事件可能在其刚刚发生时就暴露，也可能在发生的过程中或发生以后才被发现，因此所有安全事件都应该有一份书面的经过调查证明足够客观的日志，而且应该把日志妥善保存以免被修改。另一方面，在线日志很容易被修改和删除，手工记录是很有必要的。

分析确认：企业根据记录的安全事件描述，结合前期进行过的安全检查、安全监控与审计、以及网络状况，进行分析和判断。也可以通过工具直接进行测试，结合当前扫描、探测、实时监控和审计的结果进行分析，可以更容易定位出问题

所在。

事件处理：事件响应最主要的任务之一就是维持或恢复组织的运作。因此，一旦发生意外事件，如何防止攻击或损害事件的扩大是其主要的目标，相关人员在现场或者远程依照不同事件类型进行事件处理。事件处理过程中，要对每个处理的动作进行详细的记录。

系统恢复：在处理了事件以后，就要对系统进行恢复，使企业业务重新运转。如果系统在故障点有备份，被攻击的系统就用备份来恢复；应该从系统中彻底删除诸如受到感染的文件；如果调整了网络或安全产品，要把所有安全上的变更作记录。

事后分析与跟踪：在安全事件处理完毕，所有系统恢复正常以后，应该针对事件进行分析。集中企业所有相关人员来讨论所发生的安全事件以及得到的经验教训，对现有的一些流程进行重新评审，并对不适宜的环节进行修改。在安全事件处理后的一段事件内，企业应该密切关注系统恢复以后的安全状况，特别是曾经出问题的地方。

4.2.3 安全事件审计

4.2.3.1 安全事件审计的挑战和需求分析

企业的 IT 环境中通常已经部署了防火墙、防病毒、入侵检测等安全措施，但是对于内部人员、第三方支持人员等的访问和操作需要有监控和审计的措施。

根据美国欺诈稽核师协会 ACFE (Association ofCertified Fraud Examiners) 2008 调查显示：

- 欺诈带来的损失，平均占企业年收入的 7%
- 60%的欺诈案件和内部员工有关
- 65%的欺诈案件是由于意外事故而检测出来

另外内部威胁研究机构发现 :超过 75%的内部欺诈犯罪事件是来源于授权用户，而且是使用简单，合法的用户命令引起的。

4.2.3.2 安全事件审计概述

在企业里，用户操作、后台维护所带来的安全风险包括：

- 误操作导致关键应用服务器异常甚至宕机
- 违规操作导致敏感信息泄露（如客户信息，账户数据等）
- 恶意操作导致系统敏感数据信息被篡改和破坏

当企业关注用户操作所带来的安全风险时，往往会发现企业无法有效地监控内部人员的日常操作，很多内部欺诈事件都是授权用户使用简单、合法的用户命令实现的，要发现这样的问题就象大海捞针，很难审计的到；缺乏从业务操作层面和运维操作层面监控用户行为的措施，现有手段可能只是数据库或网络层面的日志跟踪；而且不能提供回放功能，无法真实还原违规行为的操作过程。另外一个大的问题是缺乏对特权用户（如 root）的有效审计。

通过实施日志集中管理和审计框架，可以达到对用户操作行为重点审计的目的。实现日志的集中采集与存储，将各专业系统的系统日志、应用日志、操作访问日志汇聚到一起，进行分类、压缩存储。 实现日志的集中分析，通过定义规则，对日志进行横向和纵向的关联，进行自动化的分析，找出潜在的安全问题。实现日志的集中审计，通过将操作、访问日志关联到用户，分析用户的操作行为，以便于责任认定。实现审计结果的自动响应机制，以便更快、更早地发现问题，尽可能地将损失降低到最低限度。通过集中化的日志集中管理与审计系统，实现对日志的自动采集、分析、审计和响应，提高日志审计的效率，做到问题早发现早处理，将风险控制在可以接受的程度。

4.2.3.3 信息安全审计的工作

目前企业对于日志审计的工作汇总如下：

- 全面的日志采集工作：根据企业业务系统各资源主机、网络设备、应用系统的类型和网络分布，采取本地型日志采集方式和网络型日志采集方式，对全网的设备、应用以及网络操作进行全面的日志采集。
- 审计记录的规范化工作：由于企业的网络中设备种类繁多，每种设备由于业务不同，日志上报的格式和内容项都有所不同。因此日志审计产品必须对采集到的各种设备日志格式进行统一，同时尽可能保留审计记录来源信息，为后续的审计分析提供依据。
- 基于策略的日志过滤、归并：企业的业务网络中，各个设备运行繁忙，日志信息量非常大，日志集中管理与审计系统可根据相关策略对原始日志进行过滤和归并，以减轻日志数据在网络中的传输压力和数据中心的存储压力。
- 本地型日志审计与网络型日志审计相结合的审计体系。本地型日志记录本地操作，通过多种采集机制汇总到日志集中管理与审计系统；网络型日志则通过网络旁路抓包的方式获取网络操作，两者结合可构成综合的审计体系。
- 多维关联分析工作：对于来自各个资源的日志信息，提供多维的关联分析功能，站在用户角度，将一个用户在多个设备上的操作进行横向关联分析，形成针对用户为主题的操作行为审计；站在事件角度，对于发生在多个设备上的事件进行关联分析，形成一个完整的事件流操作过程审计；站在设备角度，对于多个用户对本设备的操作，形成本设备被访问的安全审计报告等。
- 符合 Sox 法案的内控报表工作：根据 Sox 法案对企业内控的要求，按通行的内控框架（如 BS7799 或 COBIT）提供符合 Sox 法案要求的各种内控报表。

4.2.4 安全策略管理

4.2.4.1 信息安全策略的挑战和需求分析

很多企业在信息安全建设中，已经部署了一些相关技术措施和产品，同时也

建立了很多安全管理制度，甚至通过了信息安全管理体系的认证，投入了很多财力人力，但整体信息安全管理水平并没有明显提升。在信息安全方面，技术只是帮助实现管理的手段。对于企业信息安全管理，比如物理安全、人力资源安全、业务连续性管理这些都无法纯粹依靠技术来实现，更多的是要靠策略和管理来实现。

企业信息化系统安全政策需要在高层面上为企业安全提出方向和要求，体现管理层对安全的支持和对安全的期望。安全政策不针对具体的安全技术给出实现方法，该部分内容会体现在第二层安全标准和指导方针中。所以安全政策这一层只有一个纲领性文件作为指导。

安全政策是一个高层次的，全面的，企业范围内的信息安全要求和规则。除安全政策外，企业还需要建立相应的安全标准和指导方针来配合安全政策的实施，安全标准和指导方针是一系列有系统和技术特性的、具体的安全文件。否则企业用户和管理人员没有可以遵守的安全策略文件，就无法满足企业范围安全政策的要求。这部分安全策略文件需要包括两类，一类为管理类的制度和办法，另一类为技术类的安全标准和规范。

企业信息安全策略体系还需要包括信息安全流程和步骤，目的是为了保证安全标准和指导方针的有效实施而制定的实施流程、指南与细则。安全流程和步骤是对企业信息安全标准与规范的解释与明细。举例来说，电子邮件系统在开发和维护阶段需遵从企业应用开发与维护相关标准和管理规范，具体的实施时需依照相关标准和管理规范编制实施指南和细则，例如用户手册等。

4.2.4.2 信息安全策略概述

安全策略以及相应的规范、规定、标准和流程应有明确的信息资产保护对象或保护对象类。相同信息资产或信息资产类不同方面的安全策略应不能产生冲突。

在用户的日常运营中，信息系统已成为支撑业务的基本需求，信息系统与业

务有着不可分割的联系。要确保信息系统的安全运行，安全管理和安全意识必须贯穿到业务人员及日常业务中。根据对计算机信息系统现状的风险分析结果，确定安全策略的起点；制定安全体系；向用户相关部门和人员宣传安全方针和意图；进行安全策略、标准和制度培训；推行安全体系的执行和安全措施的实施；有计划、分阶段的逐步完成安全体系的建立。

安全策略以及相应的规范、规定、标准和流程应有明确的人员管辖。相同人员不同方面的安全政策应不能产生冲突。安全策略以及相应的规范、规定、标准和流程将遵循一个多阶段的生存期管理模型。

4.2.4.3 信息安全策略的工作

安全策略管理中用户计算机信息系统安全体系的安全策略文件包括：

- **主策略**
- **技术标准和规范**
- **管理规定和办法**
- **操作流程**
- **用户协议**
- **培训资料和用户手册。**

❒ 主策略

主策略，纲领性的安全策略主文档，等同于安全指导方针，陈述本策略的目的、适用范围、信息安全的管理意图、支持目标以及指导原则，以及各个方面所应遵守的原则方法和指导性策略。所有其它部分都从主策略引申出来，并遵照主策略，不与之发生违背和抵触。

❒ 技术标准和规范

技术标准和规范，包括各个网络设备、主机操作系统和主要应用程序的应遵守的安全配置和管理的技术标准和规范，各业务系统采用的技术标准和规范。技

术标准和规范将作为各个网络设备、主机操作系统和应用程序的安装、配置、采购、项目评审、日常安全管理和维护时必须遵照的标准，不允许发生违背和冲突。向上遵照主策略，向下延伸到安全操作流程，作为安全操作流程的依据。

- **组织机构和人员职责**

安全管理组织机构和人员的安全职责，包括安全管理机构组织形式和运作方式，机构和人员的一般责任和具体责任。作为机构和员工具体工作时的具体职责依照，此部分必须具有可操作性，而且必须得到有效的推行和实施。从安全策略中延伸出来，其具体执行和实施由管理规定、技术标准规范、操作流程、培训资料和用户手册来落实。

- **安全操作流程**

操作流程，详细规定主要业务应用和事件处理的流程、步骤及相关注意事项。作为具体工作时的具体依照，此部分必须具有可操作性，而且必须得到有效的推行和实施。向上遵照技术标准和规范、主策略。

- **管理规定和办法**

各类管理规定、管理办法和暂行规定。从安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是必须具有可操作性，而且必须得到有效的推行和实施。此部分文档应该必较多，覆盖到安全工作的各个方面。

- **用户协议**

用户签署的文档和协议。包括安全管理人员、网络和系统管理员的安全责任书、保密协议、安全使用承诺等等。作为员工或用户对日常工作中的遵守安全规定的承诺，也作为安全违背时处罚的依据。向上遵照管理规定和办法、主策略。

4.2.5 安全绩效管理

4.2.5.1 信息安全绩效的挑战和需求分析

企业信息安全建设是一个不断走向成熟的过程。从风险管理和流程管理角度，我们可以把信息安全建设分为建立、优化和完善三个阶段。在企业信息安全建设的不断演进过程中，人、流程和技术始终是一个整体。要不断提高信息安全管理和控制水平，为了使企业信息安全从改进阶段、制度化阶段、可控阶段、可审阶段、可信阶段不断演进，建立合理的信息安全绩效管理体制是信息安全建设的重要内容。但安全绩效管理的体系如何建立、如何考评、如何建立相应的指标评价体系、如何与企业绩效管理、人力资源相关管理制度结合都是一个较大的挑战。

4.2.5.2 信息安全绩效概述

所谓安全绩效管理是指企业安全管理目标与各级人员之间在目标与如何实现目标上所达成共识的过程，以及增强员工成功地达到企业安全管理目标的管理方法以及促进员工取得信息安全管相关理工作优异绩效的管理过程。在企业信息安全框架中的安全绩效管理的目标定位在信息安全管理和运维层面。目的在于提高信息安全管理系统的运行和维护的的能力和素质，提高企业员工信息系统管理和使用方面的能力及相关素养，遵从信息系统安全的相关制度和流程。做好安全绩效考核，才能完整清楚地反映安全运维的主要活动，明确部门和职责、部门与绩效的关系;才能将业务目标、外部竞争环境和处于后台支持的安全运维员工个人工作表现连接起来，提供激励的依据和评判标准，从而提升员工工作成就感，开发员工潜能;才可以发现安全运营管理潜在问题，提出预警，并通过及时的纠正改进，避免故障的发生以及可能带来的负面影响。

4.2.5.3 信息安全绩效的工作

安全绩效管理的范围

本文中定义的安全绩效指标覆盖整个企业信息安全工作的安全治理层面和日常安全运维层面。涵盖了目前的信息安全控制关注点，如：

- 安全事件管理
- 变更管理
- 业务连续性管理
- 物理和环境安全管理
- IT 终端管理
- 病毒管理
- 帐户权限管理规范性
- 安全日志审计规范性

安全绩效考核计划

信息安全绩效管理计划是绩效管理体系的第一个关键步骤，也是信息安全实施绩效管理系统的主要平台和关键手段,通过它可以建立起一种科学合理的管理机制，能有机地将各部门人员的利益，其价值已经被越来越多的企业接受。

考核计划的有效性

一个成功的信息安全有效性测量考核计划，应当具备以下 4 个组成部分。

- 高层领导的重视和支持。
- 一套可实施的安全策略和流程。
- 量化的评估指标。
- 面向结果的指标分析。

安全绩效考核方法

KPI 的定义和类型。

KPI（关键绩效指标）是 Key Performance Indicators 的英文简写，是管理中“计划—执行—评价”中“评价”不可分割的一部分，反映个体/组织关键业绩贡献的评价依据和指标。KPI 是指标，不是目标，但是能够借此确定目标或行为标准：是绩效指标，不是能力或态度指标；是关键绩效指标，不

是一般所指的绩效指标。依据关注的角度不同，信息安全管理有效性测量指标大致可以分为 3 类：

- 实施类考核指标：用于度量安全策略的实施情况，主要考核事前安全工作。
- 效能类考核指标：用于度量安全服务的工作效力和效率，主要考核事中安全工作。
- 影响类考核指标：用于度量安全事件对业务的影响，主要考核事后安全工作。

人员角色

与信息安全管理有效性测量指标相关的人员角色，应当包括：

- 管理层：为信息安全考核计划提供高层支持和监督。
- 部门各级经理：为信息安全考核计划提供支持，协调有关工作。
- 系统/信息的所有者：为安全指标的制定和数据采集提供支持。
- 审核员：负责信息安全日常工作，收集数据和计算安全指标。

成熟度

信息安全指标，主要是用于评价安全策略的执行和改进工作。根据安全策略的管理方法，信息安全指标计划可以分为 5 个能力阶段，进行成熟度评估。

第 1 级：定义了安全策略。
第 2 级：定义了详细的安全流程和控制方法。
第 3 级：实施了安全流程和控制方法。
第 4 级：测试了安全流程和控制方法的有效性和符合性。
第 5 级：安全流程和控制方法被集成到日常工作中，不断对结果进行跟踪和分析。

在第 1-3 阶段，关注的是安全策略和流程的实施情况，采用的信息安全指标主要实施类指标。在第 4-5 阶段，关注的是安全策略和流程的效果和作用，采用的信息安全指标主要是效能类指标和影响类指标。

信息安全绩效考核示例

通过信息安全相关员工职位的 KPI（员工的业绩衡量指标）的设定，评定职位的输出业绩，对关键的业绩进行考核，综合工作能力，策略符合执行情况等并将它们与其它考核体系相结合。

考核对象	内容及权重	
	信息安全管理关键绩效指标	工作目标完成情况
管理层		
各级部门经理		
系统/信息资产所有者		
审核人员		
信息系统使用人员		

4.2.6 安全外包服务

4.2.6.1 安全外包的挑战和需求分析

迫于财力和人力，大部分的中小企业都无法组建包含相应专家和专业技术人员的安全团队。随着中小企业的关键业务越来越依赖于 IT 系统，他们对 IT 的安全性也会越来越看重，和大企业之间的安全需求差距也越来越小；而对于一些大型企业来说，建立这样专业的技术团队同样面临着挑战。于是，安全外包服务就浮出了水面。

然而，安全外包的发展和推广本身在现阶段还面临一些挑战和制约因素。安全外包服务模式客观上要求完善的行业标准的建立；此外，安全外包服务提供商

在提供相关安全外包服务时，可能会接触到企业的敏感信息，这是众多企业对选用这一服务模式所不得不考虑的问题。

随着信息安全技术的不断发展，不是所有的企业都可以投入更多的人力、资金和技术去管理自己的信息安全运维体系。安全外包服务已经开始进入企业信息安全建设相关决策者的视野。

4.2.6.2 安全外包概述

安全外包是将自身的安全运维工作外包给外部专业的安全管理服务商，依赖外部的专业力量来协助组织自身的安全运维工作，实现安全托管。安全托管服务常见的内容：

- 入侵检测/防护系统的事件监控与设备管理• Intrusion Detection / Prevention Monitoring and Management
- 防火墙系统的事件监控• Firewall Monitoring
- 企业范围的弱点/漏洞管理• Enterprise Vulnerability Management
- 安全智能服务主要包括威胁预警与安全建议服务 Security Intelligence Services (Threat, Advisory Services)
- 漏洞扫描服务 Vulnerability Scanning
- 安全技术测试服务 Security Technical Testing
- 安全符合性管理• Security Compliance Management
- 病毒监控与管理（桌面与服务器）• Anti-Virus Monitoring and Management (both desktop and server support)
- 安全事件管理• Incident Management
- 安全通报服务• Information Security Advisor
- 其它定制开发的服务

4.2.6.3 安全外包的工作及应用

安全外包及托管服务能够帮助客户在短时间内提升安全服务水平，让客户更

关注自身的业务运作，真正可管理的安全服务具备以下能力：

- 针对客户网络环境提供安全防护设备；
- 提供安全防护设备的运行维护以及安全事件监控服务；
- 与此同时，帮助客户制定安全运营的策略及流程；
- 并在管理服务期间根据客户的环境改变进行更新以帮助客户成功规避演化的风险；
- 通过上述服务给客户提供综合的网络安全保护；
- 提供 7×24×365 的专业级监控，为用户的安全产品提供最好的管理，事件响应及技术支持；
- 实时响应非授权行为和安全事件并在必要时提升　响应级别；
- 为用户提供实时的访问接口，了解被管理设备的工单状态、事件响应及处理情况、报表生成、安全趋势分析等；
- 提供在线部署及紧急响应工作组；
- 利用先进的虚拟补丁技术为用户提供保护；
- 威胁分析服务帮助用户实时了解全球最新的安全趋势以及与用户环境相关的安全威胁。

4.3 基础安全服务和架构

4.3.1 身份和访问安全

4.3.1.1 身份和访问安全的挑战和需求分析

企业或组织随着业务发展，规模扩大，在用户的身份和访问管理方面将会面临很大的问题和挑战，其中有由于业务变革所带来的新的问题和挑战，也有一直以来遗留下来的管理问题和挑战。如在用户管理方面，以前都采用手工的方式由系统管理员进行管理，而当用户大量增加的时候，这种手工管理的方式就会影响到用户管理的效率和安全性，这些问题和挑战的出现是在企业发展必然的结果。

- 管理和运营成本升高

随着组织结构的扩大，人员增加，以目前的管理方式，必定会造成在用户管理方面的管理和运营成本升高的问题。因为目前的管理方式是由信息科技部门的系统管理员通过手工的方式来管理和实现用户的管理，没有使用任何工具来进行辅助，一旦人员增加导致IT系统用户增加，必然会大大增加用户管理工作的工作量，从而大大增加用户管理的成本，因此目前面临最大的问题和挑战就是管理和运营成本的升高，同时面临的挑战是通过什么样的方式来改善管理流程和方法，来降低管理和运营成本。

- 管理效率降低

在管理和运营成本升高的同时，另一个问题就是管理效率的降低，例如，以前当一个新员工加入公司后，管理员能够在三个工作日将该员工工作所需要的帐号和口令设置完成，而当员工从1000人快速增加到3000人之后，由于增加了很多的额外工作量以及增加的审批流程，预计完成这些工作的时间需要增加到至少五个工作日，因此将带来管理效率降低的问题，将会对整个Demo公司的内部管理流程产生很大的影响。

- 安全问题增加

在人员大量增加的同时，由于没有一些自动化的工具或者技术帮助内部管理的实施，将会出现很多安全隐患。一个很突出的问题就是幽灵帐号的问题，这一问题实际上在人员较少时有时也会出现，但由于目前人员数量还不算太多，因此很多时候并未凸显出来，随着人员大量增加给内部管理带来巨大压力，这一问题将很快暴露出来，比如，当一个员工离开公司，那么他原来所拥有的帐号和权限应该在第一时间被从原来他有权限访问的系统中及时清除，而目前有时会出现并不是所有帐号都被及时清除的情况，相信在将来这一问题会更多，这就将会给公司的业务系统带来极大的安全隐患，甚至有可能给公司带来巨大的经济风险。

- 内部审计与外部审计要求

随着公司在证券市场上市，要求公司管理层对公司采取更为严格的符合法规

要求的管理措施，其中之一就是加强对公司管理行为的审计，主要是采取内部审计与外部审计结合的方式。目前，公司主要的业务系统都架构在IT系统之上，因此，如何从IT系统出发对业务行为和管理行为进行有效的审计是企业面临的问题之一。

从IT审计的角度来说，IT系统的用户访问以及管理是其中非常重要的内容，因此，必须对用户的管理以及对应用系统的访问和日常运维管理进行有效的审计，以满足内部审计和外部审计的要求，从而帮助公司整体符合法律法规的要求，实现合格的公司治理。

4.3.1.2 身份和访问安全概述

身份和访问安全通常定义为身份验证、访问管理和身份生命周期管理三部分。他有助于组织识别访问系统、应用和数据的用户身份，确保只有经过授权的用户才可以访问，从而保护这些资产的安全性，降低管理成本，增强用户体验，支持遵从性，帮助提高对人员身份的信任度。要想在物理和逻辑环境中有效的进行身份管理和访问管理，就必须在整个身份生命周期中管理用户身份和资源访问权限，包括：身份生命周期管理，包括用户自主维护、注册、验证、配置、重新验证和取消配置身份控制，包括访问和隐私控制、角色管理、单点登录（SSO）和审计访问授权.访问授权可在用户的整个生命周期内（跨多个环境和安全域）及时地提供访问。

4.3.1.2.1 身份验证概述

身份认证管理需要能够集中地自动实现用户帐号和审批工作流的创建，从整体角度设置IT和非IT资源，并通过自动化流程降低成本。借助集成化的单次登录以及个性化的门户自服务（包括密码重置），同时也提升了用户的生产效率。由于有了能够满足当前及未来企业需求的功能强大的身份鉴别和识别存储支持，身份识别管理范围可以含盖企业管理涉及到的身份识别的各个环节。从员工入职工作、合作伙伴签约或客户访问系统开始，它就能追踪、管理并自动实现需要的系

统访问变更，同时启动所有的工作流和批准过程。

身份认证管理提供集中的完全自动化的全用户管理，采用经济高效的解决方案，管理用户账户和工作流以及企业资源的设置。此外，还可以提供授权控制服务、基于Web的管理和自我服务功能，以便提升用户的生产效率和降低用户的管理成本。

身份认证管理通过提供一次登录，可自动实现安全地访问基于浏览器、客户机/服务器以及传统设备的应用程序，并且可消除当今IT安全领域最大的、造成高额成本支出的安全难题——持有多个ID的密码问题。

身份认证管理需要为管理身份识别和认证方法提供强大的存储库，通过接近实时的查找功能来管理成千上万的用户，能够从Netware、Lotus Notes、Active Directory、LDAP等来源整合用户信息，为身份认证管理提供基础。

身份认证管理要对所有的身份处理提供实时的证书验证、集中的客户管理、持续的隐私保证以及详细的审计跟踪。在此基础上，需要提供基于策略的处理以及分布式、负载平衡的吞吐量管理。另外，还需要无缝集成LDAP和X.500目录服务以及相关PKI要素。

4.3.1.2.2 访问管理概述

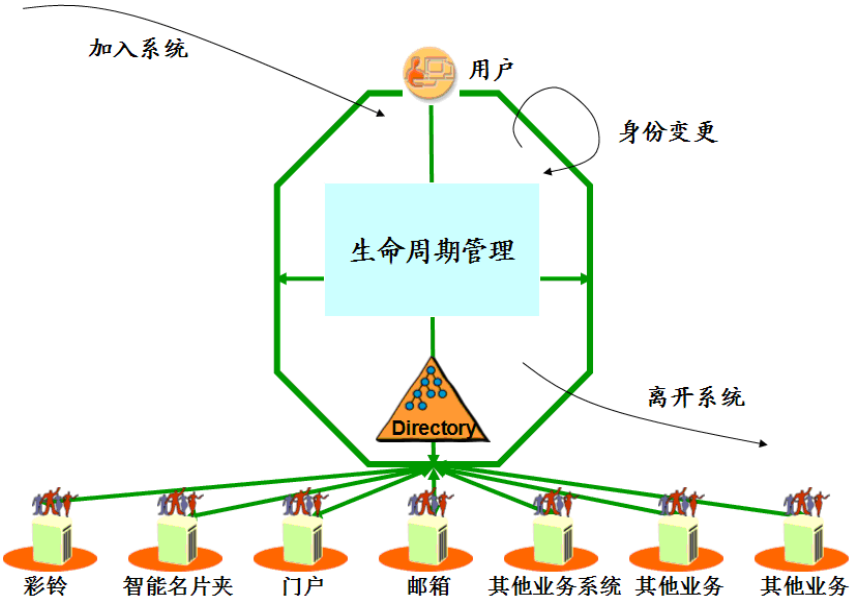
管理用户访问当前无数的企业资源是一项复杂工作。员工、企业合作伙伴及客户要求跨不同平台和操作系统，安全地访问关键型业务应用。许多分布式操作系统支持管理员访问所有信息，这也意味着诸如患者信息或者敏感商业计划等信息的私密性可能遭到破坏。管理访问也意味着对被认证的用户访问所有类型的资源进行控制，同时确保强大的安全策略始终如一地应用到所有职员。

访问管理解决方案通过集中和强化的端到端的安全性，保证业务关键型资产的安全，而无需受限于操作系统、平台、业务应用以及是否是Web资源。集中管理汇同提升生产效率的个性化以及统一的安全策略，可以确保降低成本。借助

主动的动态安全措施，这些解决方案能提供最强大的保护，因此能够在防止内部破坏和外部攻击的同时，全面监控IT和物理访问设备的违规使用。

4.3.1.2.3 用户生命周期管理概述

用户的生命周期管理是指IT系统用户的管理应和其在企业内部的人事流程相关，同时也是受其驱动的；通常内部用户的人事关系发生变动之后，其在统一用户管理系统中的用户状态能够作相应的调整。用户的生命周期管理能够根据其人事管理过程的演进而发生变化。如下图所示。



图示 12：用户生命周期管理

通常企业机构在考虑身份和访问管理时，已统一建设了一批信息系统，各信息系统都独自管理用户身份和认证，但缺乏统一规范的用户身份管理流程，存在口令简单、更新不及时等多方面问题，迫切需要从整体考虑信息系统的身份管理流程，制定相应的规范，加强身份管理与认证的安全性，从而保障系统的安全、可靠运行；作为信息安全体系技术架构的重要组成部分，身份管理与认证是建成企业机构信息安全保障体系的关键技术类项目；作为共享的重要信息安全基础设施，身份管理与认证为业务流程在系统中的实现提供安全的身份认证，并降低系统建设与集成的复杂性和成本，提高信息系统的安全防护能力；集中身份管理也

作为提高身份管理效率的措施，可以有效避免用户身份管理不一致、无法适应信息系统大规模应用、影响信息技术应用的情况，从而保证信息系统向用户提供服务的可用性；集中身份管理与统一认证授权服务能够解决应用系统用户帐号管理复杂、口令安全性不足等信息安全问题，是安全、有效地达到等级保护和内控合规性要求的重要措施。

4.3.1.3 身份和访问安全的工作及应用

建设身份和访问管理IAM系统通常包括以下目标：

- 建立身份和权限管理标准、流程、组织，实现；
- 统一身份信息源，统一身份管理，确保每一位员工在所有应用系统中有唯一的身份标识；
- 统一授权，所有应用系统的帐号和权限由统一的组织管理、统一的工作流程、统一的受理接口；
- 确保合理授权，使员工在所有应用系统中的权限与其工作岗位相适应；
- 帐号和权限可审计，具有统一界面的用户权限查询、用户权限日志查询；
- 建立统一的身份和访问管理平台，提高企业机构统一的信息安全基线和效率，降低运维成本；
- 与企业相关系统进行集成。

身份和访问管理的实现方式

根据发展趋势分析得出的建设及功能需求，身份管理与认证的功能范围主要包括身份管理与认证授权部分。如图所示，集中身份管理与统一认证授权服务具体包含以下三方面的主要功能：

- 集中身份管理——主要通过对现有分散式的用户身份目录服务以及应用系统中的身份数据进行管理，形成以用户身份为中心的统一身

份视图，实现对信息系统用户身份信息集中的创建、修改、删除等操作，同时形成并维护用户身份与具体应用系统帐号的对应关系；

- 统一身份存储——统一存储实现统一认证授权所需要的身份数据，提供身份信息的查询、验证等功能；
- 统一认证授权——主要通过与应用系统中的认证执行模块的集成，验证用户提交的身份及鉴别信息，并支持用户身份的强认证。

身份和访问管理的体系架构如下图所示：

图示 13：身份和访问管理体系架构

■ 集中用户管理

集中用户管理为企业用户提供统一的用户帐号管理服务，管理企业用户使用各种企业IT系统时的用户帐号有利于降低用户管理的成本，有利于强化用户帐号信息安全策略实施，主要功能包括：

- 组织管理，实现对企业组织结构的管理；
- 帐号管理，实现对用户自然人身份的主帐号的管理，以及主帐号与用户在目标IT系统的帐号的关联同步管理；

- 用户审批管理，实现对用户帐号建立、变动的审批管理；
- 用户验证方式管理，实现对用户帐号的验证方式的选择和管理；
- 角色管理，定义和管理在企业用户的工作岗位/角色，提高企业用户管理的效率和灵活性；
- 帐号策略检查，定义和管理帐号信息安全策略，并进行帐号合规性信息安全检查。

■ 用户目录

为企业提供统一的权威用户目录。通过目录整合将已有应用系统中分散的、非规范的用户目录进行整合，统一或者同步，以支持统一用户管理的实现，其主要功能包括：

- 企业用户目录：实现将所有用户信息存储在企业用户目录，企业用户目录设计需要反映出企业的组织结构；
- 信任凭证信息安全存储：实现所有用户的敏感的信任凭证信息的信息安全存储；
- 目录整合与数据同步：实现企业用户目录的良好整合功能，能够整合企业已有系统的非规范用户信息；
- 目录复制与恢复：实现企业用户目录的复制与恢复，有效保障用户目录信息的高可用性。

■ 信任凭证管理

管理企业用户信任凭证（Credential），提供信任凭证的建立、分发和撤销。常见的信任凭证有静态密码、一次性密码、生物特征等。主要功能如下：

- 信任凭证策略管理：根据企业的信息安全策略来统一设定相应的信任凭证策略；
- 信息凭证的自动生成：提供信任凭证的自动生成功能，信任凭证自动生成是基于定义的信任凭证策略；

- 信任凭证的信息安全发送：信任凭证生成后，以信息安全的方式发送给用户；
- 信任凭证的同步：根据密码策略，从集中用户管理服务向目标系统进行密码自动同步，同时支持收集并检查目标系统的密码策略符合性；
- 信任凭证撤销：根据企业信息安全策略，对用户的信任凭证实行撤销，例如对用户的密码撤销，密码撤消后将失效。

■ 集中访问认证

能够以统一的方式对企业用户对应用和平台的访问进行身份验证。

统一认证服务能够与现有企业应用和平台进行整合。通过统一集中认证服务提高应用身份验证的灵活性和强健性，不必增强每个企业应用的认证功能。主要功能如下：

- 功能组件能够以统一的方式对企业用户对应用和平台的访问进行身份验证；
- 统一认证服务能够与现有企业应用和平台进行整合；
- 通过统一集中认证服务提高应用身份验证的灵活性和强健性，不必增强每个企业应用的认证功能。

■ 单点登录

在分布计算环境中，用户每天要登录到很多不同的系统和应用中。每个系统都有自己的认证过程，要求用户输入不同的用户名、口令。用户需要进入的系统越多，用户出错的概率和安全问题出现的可能性就越多。单点登录（eTrust Single-Sign On）指使用户进行单一认证。一旦获得认证，用户可以立即访问所有被授权的系统，包括C/S系统和基于WEB的系统。系统或安全管理员可以实施安全控制，但不用改变或影响用户登录。

- 访问策略

以集中的方式对企业用户访问应用或平台的资源的权限策略进行管理。可以根据业务信息安全要求，对用户的访问策略进行设置，包括访问访问主体、对象资源、访问时间等。可实现将访问授权策略数据的存储和管理和实现统一管理企业的应用和平台系统的访问策略。

- 访问授权

可以以集中的方式对企业用户访问应用或平台的资源的权限进行检验。用户身份确认后，需要对用户访问资源的权限进行检验，以确定用户是否能够访问目标资源。目前大多数应用采用在应用本身实现细粒度的资源管理和访问授权控制；部分基于B/S架构的应用提供访问授权服务；标准系统平台（如开放平台操作系统）提供访问授权服务。

完善的身份识别和访问管理解决方案应该能够识别和提供有效的业务流程，并能够将业务流程集成为一个流畅的、可扩展的业务运作过程中。用户按需供给、工作流程与授权。企业需要的是实时的按需访问。当雇员加入公司时，需要立即赋予他相关资源的访问权限。因此，对于企业来说，身份和访问管理是一项需要迅速处理的关键任务。自动化的自助功能，包括密码重置、用户供给、业务工作流程的支持、自动化授权、基于角色和策略的访问权限分配、帐户撤销和安全报警报等都能够帮助企业节约时间以及实现其安全保障需求。

4.3.2 数据安全

研究表明，在一个依赖计算机应用系统的企业，丢失300M的数据对于市场营销部门就意味着13万元的人民币损失，对财务部门意味着16万元RMB的损失对工程部门来说损失可达80万元RMB，而企业丢失的关键数据如果15天内仍无法恢复，企业就有可能被淘汰出局。国内外发生的种种案例都证明了保证数据安全的重要性，随着信息系统应用的依赖程度提高，如何保护数据安全也成为我们迫切需要研究的一个课题。

4.3.2.1 数据安全的挑战和需求分析

关于数据生命周期：

面对迅猛增长的业务数据，存贮设备的投资越来越大，在数据的整个生命周期中，如何把合适的数据，在合适的时间，存储在合适的介质上？数据生命周期安全问题涉及数据整个数据生命周期的管理过程 :从创建到其失去商业价值或按规定要求被删除。虽然部分数据对于企业来说已经毫无意义，但在很多情况下，它对某些人来说并未失去价值。

就企业而言，所有的数据在其生命周期中都应当被有效地管理，通过必要控制手段清晰地界定，以使其避免内部非授权的访问。

如何指定完善的数据备份、恢复策略，保证数据的安全性？ 如何根据需要长久保存关键任务信息？ 如何制定自动化管理方案，然后根据企业制定的方案保存信息？ 如何在现有 IT 环境下满足访问和安全的要求，优化存储从而根据存储条件及未来发展制定恰当的计划？

数据泄露保护：

在当今的企业信息系统中，我们会通过在网络边界部署防火墙等安全系统，建立针对外部用户的安全登录和访问控制。但是在企业内部，我们最重要的各种信息数据却是开放的。这就像个很大的餐馆，您的数据就摆在菜单上。而且，与大多数餐馆一样，没人注意用户使用了哪些受特权保护的数据以及使用了多少。

在这种无人监视数据使用的情况下，我们能够相信有权限的用户会可靠地使用数据吗？不幸的是，这种乐观的想法是靠不住的。根据 Privacy Rights Clearinghouse（www.privacyrights.org）的调查，“从 2005 年 2 月以来，由于发生安全破坏，有超过 1.04 亿美国居民的数据记录泄露了。” 这个数字表示大约每三个美国人中就有一个人的信息泄露了。我们正在为过度追求开放性付出代价，现在应该为更严密的安全性而努力了。

具体到实际信息系统中，数据泄露保护面临的主要挑战如下。

终端设备上的数据不安全，面临丢失风险

- 如何控制来自网络内部的数据安全威胁？
- 是否会因为担心安全问题而限制合法用户接入数据和进行协作？
- 是否针对电子邮件传输使用了加密软件？
- 使用什么程序来处理丢失或被盗的设备？

无法在终端位置执行公司的安全策略并且跟踪循规情况

- 是否知道公司员工何时违反了公司安全策略？
- 用户能否打印、拷贝、删除或修改他们接入的数据？
- 针对公司安全策略，您是否对员工进行了培训？
- 是否采取了一定措施来阻止滥用或误用行为，即使违规者是合法用户也不例外？
- 能否确保用户不会将保密信息拷贝或发送给不当接收方？

由于终端设备的数量和类别都在不断增长，因此，难以保证它们的安全性

- 都支持哪些类型的固定和可移动的端点设备？
- 在处理端点设备上与安全相关的问题时，需要多少 IT 资源？
- 对于端点安全性，公司的 IT 机构采取主动还是被动的方法？
- 部署完整的端点保护解决方案的最大阻力是什么？

为了创造便利性和提高经营效率，企业将数据保存在种类繁多的端点上，为数据的安全保护提出了挑战，再加上可移动存储设备、笔记本电脑和手持智能设备的大量使用，更进一步地加剧了企业机密数据的防护问题。

由于企业机密数据的泄漏不仅会给企业带来经济和无形资产的损失，而且，如果这些泄漏的机密数据是一些与人们密切相关的隐私信息，例如银行帐号、身份证号码等信息，那么，还会带来一些社会性的问题。为此，一些行业甚至制订

了相关的数据保护法案,来强制企业必需使用相应的安全措施来保护机密数据的安全。

数据加密：

在解决以上问题的同时，企业需要同时考虑保护静止的、传输中的、使用中的业务数据，即使这些数据已经脱离了业网络。但是，又不能因为数据加密措施的采用而增加 IT 系统的复杂性。

数据归档：

调查显示，目前行业用户的一级存储设备中，高达 80%的数据在最近 90 天没有被访问，而这些未被访问的数据中又有 60%数据将在未来几乎不再被访问。一方面，这些未频繁访问的数据占据了绝大多数的高端存储的磁盘空间，大大地影响了应用系统的响应时间和性能，增加备份系统的负担，同时也浪费了巨大的企业投资成本；另一方面，数据是企业的生命和价值所在，国家审计、法规、规章也要求企业完成对关键数据的历史存储。

这些关键历史数据的存储要求最高的数据真实性、可用性和长时性，并且在最低的总体拥有成本下进行管理。

灾难备份：

灾难是一种由于人为或自然的原因，造成信息系统服务中断或延迟，致使企业无法正常运营。信息系统停顿的时间越长，企业的信息化程度越高，损失就越大。

随着企业集团化、跨地域经营，构架于 IT 系统之上的统一管理、统一决策、统一运营成了必然趋势。IT 系统成为了企业的大脑和神经网络，数据中心成了一个企业运营的关键，一旦出现数据丢失、网络中断、数据服务停止，将导致企业所有分支机构、营业网点和全部的业务处理停顿 ,或造成企业客户数据的丢失，给企业带来的经济损失可能是无法挽回的。

另外，随着科学技术的迅猛发展和信息技术的广泛应用，我国政府及各行业对信息系统的依赖也日益增强，尤其是银行、电力、铁路、民航、证券、保险、海关、税务等行业和部门的信息系统以及电子政务系统已经成为国家的重要基础设施。

重要信息系统的安全直接影响到国民经济的正常运行，直接关系到社会稳定和群众生活。而我国信息安全的防护能力较弱，安全保障水平不高，就企业信息化来说，大部分企业还没有建立统一的灾难恢复和业务连续性管理机制，信息安全和灾难恢复工作已刻不容缓。

我们来看一下国内发生的一些典型案例:

- 2003年北京首都国际机场因离港系统瘫痪而导致71个航班延误3000多旅客滞留。
- 2005年4月，中国某银行因硬件故障导致数据丢失，调用十几个分行人员手工追账一个星期。
- 2005年5月1日，黄金周的第一天。下午2点多钟，北京市铁路局的电脑售票系统出现临时性故障，致使全市各火车站的售票窗口、代售网点的售票工作全部处于瘫痪状态，时间长达一个多小时。售票系统出现问题的过程中，至少有近两千名乘客停滞在火车站，北京站公安段为此出动了300余名警力在现场维持秩序，以防发生拥挤等突发事件。
- 2005年6月，北京某证券股票交易系统出现故障，迫使股民望“红”兴叹……。
- 2005年8月，中国某行十个省一市的核心系统停机，从上午11点直到次日早上才逐步开始恢复。
- 2005年上海地铁四号线施工现场下陷，造成部分政府部门的服务停顿，数据陷于灾场。

众多的灾难过后，留给人们的思考就是如何减少损失、如何有效地防范风险、如何使业务不间断等等。

大量的事实案例证明 :重要信息系统必须构建有效的灾难恢复系统并建立业务连续性机制。灾难恢复是指将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态 ,并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

另外 ,国家有关决策和行业主管部门也出台了相关政策和指南 ,对灾难备份和灾难恢复有着严格和明确的要求。2004年9月 ,国务院信息化工作办公室组织国家重要信息系统八个主管部门（银行、证券、保险、电力、民航、铁路、海关、税务）、三地政府（北京、上海、广东）及万国数据服务有限公司的有关专家一起成立了工作组 ,编制了《重要信息系统灾难恢复指南》（以下简称 :《指南》）。2005年4月，国务院信息化办公室以文件的形式正式印发。

4.3.2.2 数据安全概述

数据安全有两方面的含义 :一是数据本身的安全 ,主要是指采用现代密码算法对数据进行主动保护，如数据保密、数据完整性、双向强身份认证等，二是数据防护的安全 ,主要是采用现代信息存储手段对数据进行主动防护 ,如通过磁盘阵列、数据备份、异地容灾等手段保证数据的安全。

数据安全是一种主动的防护措施 ,必须依靠可靠、完整的安全体系与安全技术来实现。简单来讲，有关数据安全的内容可以简化为下列三个基本点：

机密性

机密性又称保密性 ,是指个人或团体的信息不为其它不应获得者获得。在现有信息系统中 ,许多软件包括邮件软件、网络浏览器等 ,都有保密性相关的设定，用以维护信息的保密性。在现实环境中 ,数据的机密性面临多种威胁 ,如间谍软件、黑客等，都可能造成保密性的问题。

完整性

数据完整性指在传输、存储信息或数据的过程中 ,确保信息或数据不被未授

权的篡改或在篡改后能够被迅速发现。

在实际的信息系统中，完整性常常和保密性边界混淆。比如，被加密后的数据在传输中被黑客或恶意用户破解，并通过一定的数学工具，修改了密文中的有关数值或信息，数据接受者如果无法校对数据的完整性，将使用错误数据进行处理。为解决以上问题，通常使用数字签名或散列函数对密文进行保护。

可用性

数据可用性是一种以使用者为中心的设计概念，可用性设计的重点在于让产品的设计能够符合使用者的习惯与需求，也就是在确保数据机密性和完整性的同时，也要确保数据可以被使用者方便使用。而不能一味强调机密和完整，而忽视数据存在的根本意义是被使用和处理。

4.3.2.2.1 数据生命周期安全

为应对因数据生命周期所带来的挑战，我们必须从数据的整个生存周期考虑，针对数据生命周期的不同阶段，设计有针对性的解决方案。通过覆盖数据生命周期的整体解决方案，最终实现业务数据包括文件数据、应用数据的基于策略的自动管理，包括数据的分类、备份、发布、迁移、归档、删除，实现全面的数据存储管理自动化。在提高现有存储资源利用率的同时，提高数据的可用性。

整个解决方案按照标准的规范进行设计和部署，提供充分的灵活性和扩展性，满足数据保管方面当前和今后的法规要求。自动的数据存储管理减少了人为出错的可能性，提高了数据的安全性和可用行。

4.3.2.2.2 数据泄露保护

采取数据防泄漏安全的目的就是建立敏感数据的安全边界，通过采取相应的技术措施，为企业中的各种数据建立一个关于数据的安全边界。理论上来说，这些数据只要还在安全边界内，就能保证其是安全的。

数据防泄露保护需要一套完整的体系，也是多种系统的集成，用以解决不同类型用户的不同需求。根据所部署的位置的不同，数据泄漏安全保护可以分成基于网络的数据泄漏安全保护和基于主机的数据泄漏安全保护。

基于网络的数据泄漏安全保护通常部署内部网络和外部网络区域的互联接口处，所针对的对象是进出各网络区域的所有数据。基于主机的数据泄漏安全保护则部署在存放敏感数据的主机上，当其发现被保护主机上的数据被违规转移出主机时，基于主机的数据泄露保护方案会采取拦截或警报等行为。

两种解决方案没有技术上的优劣之分，主要根据用户的网络环境、信息化水平以及实际需求来选择部署实施。

4.3.2.2.3 数据加密

数据加密旨在帮助客户克服与部署全面的端点安全解决方案相关的挑战，通过将安全性构建在最常用的应用中，能够保护保存在任何地方的数据，从对外电子邮件、到文件服务器、直到 USB 闪速驱动器和 PDA 等可移动的存储设备。帮助企业一致地执行公司和法定安全策略。

通过基于平台的端点数据加密，能够通过扩展来提供大量的数据安全选项，具体取决于数据保存位置、共享方式和用户。统一的加密平台具有卓越的运行效率和可扩展性，能够适应增长。此外，多个加密应用利用单一框架，可以帮助用户加速部署、降低运行成本、并且释放管理资源去执行其他任务。平台上的多个加密应用，可将价值主张扩展到端点以外，实现以下目的：

- 保护已存数据，即使端点设备丢失或被盗也不例外
- 自动执行设备使用策略并且保护数据，因此，当端点设备上的数据被使用时，仍然能够优化数据安全性
- 监视并控制用于保存和传输数据的外部存储设备的使用情况
- 在发送、传输和接收期间保护电子邮件的安全
- 允许通过共享服务器进行协作并且保证机密性

- 经济高效地管理面向加密应用的策略和报告，根据需求的增长扩展解决方案企业网关级别提供安全的电子邮件保护；
- 在最有名的服务器操作系统平台上提供文件加密(包括主机)；
- 利用基于标 准的加密密钥管理以及可以集成的数字证书在应用层保护商业交易的安全；
- 经济高效地管理面向加密应用的策略和报告，根据需求的增长扩展解决方案；

4.3.2.2.4 数据归档

数据归档技术就是应对这一问题有效解决方案。和存储不同，备份用于高速复制和恢复来减少故障、人员错误或灾难的影响，数据归档的作用并不限于“恢复”一个应用程序或一个业务，还要能够方便地检索。数据归档系统的最基本目的是将历史数据安全地、低成本的存储起来，在需要时可方便地搜寻到。这种检索通常在一个文件、一份电子邮件或其信息内容中进行。因此，数据归档并不是生产数据的“拷贝”，而是一段信息的基础版本，经常是当前失效的或不再改变的数据。实际上，当数据停止改变或不被频繁使用时，最好把它们转移到一个文档，使之存于日常的备份窗口之外，但仍能随时接入。

用于数据归档的存储平台也同样重要。理想的情况是，数据归档存储系统应能满足长期保存活跃归档数据的需求，并易于扩展和管理，总拥有成本也要低于生产环境。先进的数据归档平台还能保证内容真实性、内容位置独立性以及具有内置复制功能。

由于应用目的的不同，数据保存和使用的策略也不相同，数据归档系统可以说是一个相当客户化、定制化的系统。

在选择和实施数据归档方式时，需要结合实际情况进行选择。譬如金融业需要历史数据用于利润分析、客户服务、信用度控制和反洗钱等应用。我们可以按照用户的数据的特点，分为 3 类：结构化数据（如数据库）；半结构化数据（如

邮件系统）和非结构化数据（如图像、录像）。

另外，归档后数据的存储，一般会和分级存储结合起来。数据的分级存储，就是按照数据所处不同阶段的重要性和使用频率的差异，将它们存储在最适宜的存储设备中，从而实现有效的管理和最低的成本。比如，在线数据通常存储在价格较高、可靠性较高的 SCSI 盘阵或光纤盘阵中，近线数据通常存储在价格相对便宜的 SATA 盘阵中，而离线数据则保存在磁带设备中。

数据归档中用户需要注意的关键点如下：

- 在期望保留时间内的数据恒久性：如果发现存储的数据无法读出了或改变了，这将是一个非常糟糕的现象。所选用的技术必须提供不会发生此类现象的安全措施。
- 符合诉讼或公司价值的数据真实性：永远要考虑选用能确保归档数据长期真实性的存储技术。

技术发展路线：技术的提高和改进不应该要求对已归档的数据进行周期性地迁移和更新。应该选择这样一种归档技术，它会不断提高容量、性能和功能，而且能保持对前面的产品向下兼容。归档的数据不会改变，因此要避免由于选择了差的技术，用户被迫不断迁移或更新这些数据。

4.3.2.2.5 灾难备份

为了灾难恢复而对数据、数据处理系统、网络系统、基础设施、技术支持能力和运行管理能力进行备份的过程称为灾难备份。灾难备份是灾难恢复的基础，是围绕着灾难恢复所进行的各类备份工作，灾难恢复不仅包含灾难备份，更注重的是业务的恢复。

灾备中心的建立，将为主数据中心提供一个“保险”， 一旦主数据中心出现问题，灾备中心可以立即接管业务，并在主数据中心恢复后将业务切回，以保证业务的不中断，这对要求 7×24 小时不间断业务的用户来说是十分必要的。可见，

信息安全是一个企业持续发展的重要保障，灾难备份与恢复因而成为企业最迫切需要解决的问题之一，是现代企业积极应对危机事件必要的技术和管理手段。

据国际标准 SHARE 78 的定义，灾难备份解决方案可根据以下列出的主要考虑方面所达到的程度而分为七级，从低到高有七种不同层次的对应的灾难备份解决方案。企业可以根据数据的重要性以及需要恢复的速度和程度，来设计选择并实现灾难恢复计划。

- 备份/恢复的范围
- 灾难备份计划的状态
- 生产中心与备份中心之间的距离
- 生产中心与备份中心之间是如何相互连接的
- 数据是怎样在两个中心之间传送的
- 允许有多少数据被丢失
- 怎样保证更新的数据在备份中心被更新
- 备份中心可以开始备份工作的能力

4.3.2.3 数据安全的工作及应用

4.3.2.3.1 数据生命周期安全

首要条件：

要实现企业信息生命周期管理，首要的条件是有完善的数据备份和恢复策略来保证数据的安全性。用户需要制订完善的数据备份恢复方案，通过网络或者 SAN 集中备份企业中几乎所有系统平台的数据到磁带机或磁带库。在此基础上，数据生命周期安全可以按照以下四个阶段进行。

第一阶段：对企业数据进行分类

利用对数据进行自动分类的存储资源管理工具和解决方案，将有效的业务数据分离出来，加以分类并制定不同的管理策略，将无用的数据及时加以清理。

对不同的业务数据进行合理的分类，对一些非业务数据进行隔离和迁移，对核心的业务数据根据管理策略进行自动的分类。有效的自动数据分类和管理策略的建立对于数据生命周期安全来说是极为关键的一步。

第二阶段，对存储硬件结构分层

构建合理的分层的存储硬件环境，满足不同类型的业务数据在不同生命周期阶段的存储要求。

- 采用完整的阵列、带库和 SAN 、NAS 的解决方案，可以满足数据分层管理的要求；
- 用户根据不同的存储设备特征建立分层的备份数据存储结构，对关键数据进行数据备份保护，根据管理策略实现数据保护的自动化。

第三阶段，根据数据类型决定存放策略

根据不同类型的业务数据的管理策略，实施合理的自动的分层数据管理，自动将不同生命周期阶段的数据存放在最合适的存储设备上。

- 自动对业务数据的访问周期进行统计并根据访问统计结果自动对数据进行分层存储；
- 根据不同的业务数据，结合存储设备的特点建立不同的存储池，处于不同周期的业务数据可以自由的迁移到不同级别的存储池中，实现存储资源的优化，提高数据的访问效率；
- 对于处于生命周期末期的业务数据，可以利用归档功能进行归档并保存在适合长期保管数据的存储设备中。

第四阶段，数据的有效保管和检索

利用先进的数据检索和分析工具对不同类型的数据进行数据处理，满足政府和行业法规要求，同时提高数据的利用效率。

- 内容管理功能可以对关键业务内容进行捕获、创建、整理、管理、通过工作流传送、存档并进行生命周期管理；
- 日志管理功能可以为商业应用软件提供生命周期管理的电子记录。
- 通常归档的数据都是比较关键的数据，所以对归档的数据提供更高层次的保护，只有在满足特定的前提条件下，系统管理人员才可以对这些数据进行修改、删除，以满足政府和企业法规的要求。

4.3.2.3.2 数据泄露保护

基于主机的数据泄露安全保护

对内部员工而言，导致数据泄露的途径很多，如通过打印机、光驱、IM 工具、网络文件传输工具、邮件、移动存储设备、USB、蓝牙、红外等接口等各种途径可以把关键信息传送到公司外部。

基于主机的数据泄漏安全保护以信息分类为基础，通过部署在终端上的 Agent 实现对数据的控制。基于主机的数据保护机制结合终端设备接口及终端应用协议控制、信息过滤，信息加密等技术可以实现全面的数据防泄漏目标。

接口管理

目的：控制数据通过各种接口泄露

- 能够对终端的各种设备接口进行控制，例如：USB 接口、串口、ATA、ATAPI、SSA、Fiber Channel、光驱、SCSI、RAID 等；
- 能够对终端的各种网络接口进行管理，例如：以太网接口、红外接口、蓝牙接口、VPN 接口和 1394 接口；
- 能够识别普通 USB 设备和 USB 存储设备；
- 能够识别固定设备和可移动设备，本地存储设备和远程存储设备；
- 支持对未知类型接口的管理；

移动介质控制

目的：控制数据通过各种移动介质泄露：比如 U 盘，软驱，可刻录光驱等

- 移动介质控制功能实现对移动存储设备的读写控制。
- 根据移动介质标识来决定是否允许接入终端，是否允许读写操作等；
- 根据文件类型、文件大小、文件来源等文件属性以及文件是否包含特定关键字来控制文件是否可以被从移动介质中读取或者被写入移动介质；
- 可以审计移动介质的操作，审计内容包括何时、哪台终端、哪个用户、使用的移动设备标识、进行的操作以及文件名称和大小等信息；

终端外联控制

目的：控制数据通过各种网络连接方式泄露

- 终端外联控制功能实现对外联方式的审计和控制，外联方式包括 Modem 拨号、GPRS 无线上网卡、CDMA 无线上网卡、红外、蓝牙、光驱、软驱、双网卡等。可以设置审计或者禁止使用这些外连方式。审计信息包括何时、哪台终端、哪个用户、使用什么外连方式、开始使用时间、结束时间、是否被阻止；
- 管理员可以为外联设置适用场景，如终端在办公环境中不能通过 Modem 拨号，但在外出差则可以 Modem 拨号通过 VPN 访问内部网络；

终端的网络行为控制

目的：控制数据通过各种网络应用泄露

- 审计和控制终端上网行为，比如控制终端用户可以访问的 WEB 网站
- 审计和控制终端用户通过 WEB 应用上传或下载数据，比如使用网盘
- 审计和控制文件的网络共享。比如控制终端用户可以和哪些主机、传输哪些类型的、传输的文件不允许包含哪些敏感关键字；
- 审计和控制使用 IM 软件，比如可以做到禁止某个时间段内使用这些聊

天工具

- 审计和控制使用 IM 传输软件，能够对终端用户使用即时通信工具传输文件进行监控和管理，比如禁止通过即时通信工具外传文件。
- 审计和控制 P2P 软件，比如禁止这些 P2P 软件的使用；
- 审计和控制其他各种网络应用的使用，比如各种各样的网络传输工具，网络游戏，telnet 等

电子邮件发送控制

目的：控制数据通过电子邮件泄露

- 支持常规邮件协议：POP,SMTP,NOTES；
- 控制和审计邮件的接受者，比如只允许向内部人员发送邮件；
- 控制和审计邮件发送的附件。比如附件的大小，文件类型以及是否包换敏感关键字等；
- 控制和审计终端设备能够通过哪些邮件服务器收发邮件；
- 控制和审计终端用户是以密件抄送方式发送邮件；
- 控制和审计使用 WEB Mail 方式外传文件；

文件共享

目的：控制数据通过文件共享泄露

- 控制和审计终端用户通过文件共享的方式外传文件，
- 控制和审计文件共享的方式，比如只允许通过 SMB 方式共享数据
- 控制和审计通过共享可以传输的文件，比如文件类型，文件是否包含关键字等
- 控制和审计文件共享的方向,比如只允许从文件服务上下载文件；

数据加密

目的：加密存于本地或在网络中传输的重要文件，防止因为文件被窃取而造

成数据泄漏

- 可以根据各种条件对数据进行自动加密。

比如：

1. 文件类型：比如设计图，源代码，财务资料；
2. 文件来源：比如文件下载自源代码服务器；
3. 敏感关键字：比如信用卡号，隐私数据等；

- 可以根据各种条件对邮件附件进行加密。

比如：

1. 根据邮件接收人，比如邮件收件人是否是内部人员邮箱；
2. 根据是否是密件抄送；
3. 根据附件的大小，比如大于 2M 的附件被认为有可能是电子图纸，不允许传输。
4. 根据附件的类型，比如 AUTO CAD 图纸，数据库文件等；
5. 根据附件是否包含敏感关键字，比如信用卡号，身份证信息等

基于网络的数据泄露安全保护

基于网络的数据泄漏安全保护主要依靠协议分析机制，通过部署在网络边界间的硬件设备，以流量过滤或代理的方式实现对进出特定网络区域的数据的发现、检查与过滤。基于网络的数据泄漏保护技术可以和基于主机的数据泄漏保护技术，提供更全面的数据泄露保护效果。基于网络的数据泄露保护方案主要通过以下方式来达到以上描述的保护目标。

数据发现

数据发现通过提供无代理网络和数据发现，可有效找到保密信息所在位置（笔记本电脑、台式机、文件服务器等）并加以分类。数据发现可提供整个企业

所存储数据的态势感知以支持数据安全策略。

数据监控

数据监控可提供所有内外部的业务通讯、电子邮件追踪、网络打印、FTP、HTTP、HTTPS、IM 等的监控。数据监控通过采用一种高级策略框架来帮助企业审计业务流程，可识别“哪些人正从哪里发送哪些数据，他们是以哪种方式发送这些数据的”，可以降低数据泄露风险并管理法规遵从情况。

数据保护

- 可以根据文件内容控制网络中传输的机密文件、设计文档等重要的数据资料以及隐私信息的泄露，提供安全合规性保证。
- 可以禁止非授权网络应用的使用，如上网代理服务、游戏等，阻止数据通过这些驱动被泄露。
- 可以监控各种网络应用对数据的传输，如：桌面共享、超级终端、IM 通讯、P2P 等对数据传输。
- 可以控制各种类型文件的传输，如视频、音频、图片和可执行文件
- 能解码各种压缩数据，检查压缩文件内容
- 可以根据其他多种条件控制数据泄漏：如时间、应用协议（不依赖协议端口）、应用的特征：比如 WEB 应用中的 URL，邮件应用的收件人、协议会话长度、数据解码方法等

4.3.2.3.3 数据加密

数据加密根据用户网络应用环境和实际需求，主要涉及到以下子系统。

服务器/网关级加密

越来越多企业开始建置加密系统，以保护敏感的企业机密，很遗憾的，为了解决各种加密的问题，保护邮件、硬盘、文档…等等，建置了不同的平台，导致管理上的困难，且浪费企业预算。

通过集中操控的安全策略，来保护机密数据、避免财务损失、避免衍生法律问题、避免因机密外泄而商业信誉受损。提供邮件、文档、硬盘、网络共享文件夹的加密保护，并有以下特色：

- 密钥管理-创建，分配和存放加密密钥而保持只有组织允许的授权人员访问加密的数据；
- 策略执行-传送集中操控的策略配置且移除不一致的或不正确的策略配置危险；
- 报告和记录-提供可见的加密保护当前状态以帮助和满足管理员和审查员的要求；
- 扩展架构-通过消除管理系统多余的各部分未来的加密软件购置费用减少时间和成本；
- 密钥的集中管理–自动生成密钥、导入/导出公钥或密钥对；
- 完全自主的策略定制–通过加密网页操控全公司的策略，拥有完全的自主权，最终用户完全不需要参与策略的制定过程；
- 完善的报告及记录功能–自动发送报告数据给系统管理者，每一封邮件的进出皆有详细的纪录文件可供查询；
- 简单的自动操作–保护敏感电子邮件，无需改变用户体验。
- 强制安全策略–根据集中操控策略自动强制执行数据保护。
- 加速部署–使用现有基础设施进行传送邮件加密。

客户端/桌面级加密

- 自动消息保护–自动加密、解密、数字签名并校验电子邮件消息，可依照本机独立或受集中管理服务器控制的中央管理策略工作。
- 多重方法保护数据–可使用压缩包、自解密文档，以及虚拟磁盘保存和保护您的敏感数据。
- 安全文件擦除–从你的磁盘安全且永久的擦除易被发现的敏感文件的所有痕迹。
- 多平台磁盘加密–为 Mac OS 和 Windows(两种系统的针对性 PGP 软件

是需要分别购买的)提供包含预引导认证的完整磁盘加密(开机便要求验证密钥密码，否则整个磁盘的数据都被 PGP 加密后保护着)

- 扩展国际键盘支持–使用超过 30 个国际键盘的预引导认证。
- 单点登录–使用当前已经存在 Windows 密码进行验证以简化登录操作。
- 多重方法保护数据–可使用 PGP 压缩包(PGPzip)、PGP 自解密文档(PGP SDA ,PGP Self-Decrypting Archive) ,以及 PGP 虚拟磁盘(PGP Virtual Disk)保存和保护您的敏感数据。
- 远程应用程序传送支持–保护 Citrix 和 Microsoft Terminal Server 会话数据。
- 同步文件–确保文件在网络中、服务器中、备份中都保持加密状态。。
- 角色分隔–在保证安全性的情况下为满足一般用户 ,文件拥有者和管理员的不同需求，将采用不同的权限分配，限制每个使用者的操作能力到所需的最小值。

移动终端加密(Windows Mobile 6 and BlackBerry)

- 虚拟磁盘–自动加密解密存储在磁盘卷内的内容，与加密客户端兼容；
- 加密压缩包–简单的创建加密的数据文件。使用密码或证书对多个用户保护正在传送的数据。与加密客户端兼容；
- 自解密文档–允许快速加密存储为 Windows 下的可执行文件包 ,以用于没有运行加密软件的数据交换环境

4.3.2.3.4 数据归档

数据归档管理工作包含如下内容：

确定哪些数据需要归档

并不是所有的数据都需要进行归档。在采购归档产品前，应该将数据进行分类。企业中存在哪些数据？哪种类型的数据需要为法规遵从及日常业务需求进行归档保护。数据分类不只是 IT 人员的事，人事部、法律部、财会部和其他重要

部门，都应该被要求能够鉴别重要的应用软件和文档类型。Exchange 服务器记录、病人记录或医学影像文档可能需要进行归档，而市场营销 PPT 或用户 MP3 文件可能就不需要归档。另外还需要考虑每种数据类型应该保存多长时间。明确需要归档哪些数据并保存多久，将有助你决定存储需求，并为归档管理工具建立可扩展的需求。

制定数据归档的遵从要求

数据归档必须能够满足必要的数据保护期限。数据保护期限通常同纸版记录和文件的保存期限是一致的。比如，如果纸质记录要求保存 7 年，那么电子版本通常也要求保存 7 年时间。数据保护的四大要点：一定要找到一种合适的数据删除方法；除非有法律目的，不要过了数据删除期还保留着数据；确保数据删除符合法规遵从；数据保存期间的变化将影响已经归档的数据。同时，归档面临着长久保存的标准化和存储介质自然退化的巨大挑战。存储介质对数据进行可靠保存的时间有限，且磁带的读写标准在若干年后可能不可用。企业不得不处在一个进退两难的境地：要么保留旧的设备以读取旧的存储介质，要么周期性地把数据更新到当前可用的新的标准介质上（比如重写一次光盘或硬盘）。因此，需要进行全面的考虑，制定出遵从要求。

归档产品是否提供保存和删除需求

评估归档产品时，必须要考虑它的数据保护和删除功能。归档产品同其他支持归档的软件工具一样，必须能够满足必要的数据保护期限。数据保护期限通常同纸版记录和文件的保存期限是一致的。比如，如果纸质记录要求保存 7 年，那么电子版本通常也要求保存 7 年时间。数据保护的四大要点：一定要找到一种合适的数据删除方法；除非有法律目的，不要过了数据删除期还保留着数据；确保数据删除符合法规遵从；数据保存期间的变化将影响已经归档的数据。

数据整合和自动化的程度

存储管理不能手动迁移、跟踪及删除每个文档。任何归档产品必须具有自动

化功能。引擎工具必须能够自动把有用的元数据添加到每个文档中，然后通过搜索工具将元数据整合到用户需要的本地文档中。政策管理工具必须能够在某些级别限制数据类型的同时，通过数据类型，应用数据迁移和保护。由于允许工具在不同的存储级别进行数据迁移、保存和删除，所以要求与其他工具实现高度整合。

互操作性和异构性程度

新的归档存储系统必须能够同政策管理和数据迁移工具进行很好的互操作；新的软件工具也必须能够提供异构功能，以支持现有的归档硬件；归档软、硬件的自动化功能必须实现无缝整合。在这一点上进行实验室测试非常重要。

归档技术、存储介质和工具的使用寿命

归档面临着长久保存的标准化和存储介质自然退化的巨大挑战。存储介质对数据进行可靠保存的时间也许只有 10 年，今天写入的磁带在 20 年前使用的标准磁带驱动器中可能是不可读的。企业不得不处在一个进退两难的境地：要么保留旧的设备以读取旧的存储介质，要么周期性地把数据更新到当前可用的新的标准介质上（比如重写一次光盘或硬盘）。

结合实际制订备份策略

归档不等于备份。基于磁盘的归档文件可能是公司数据惟一的工作副本。基于磁盘的归档需要 RAID 实现一般数据的保护，归档平台是整个备份过程的一部分。可靠的归档往往是每几个月在磁带上执行一次完整备份，每天或每周执行一次增量备份，以保护改变了的数据。像数据重复删除这样的数据缩减技术可以降低整个归档的容量大小，加速备份过程。

追踪和汇报特点

追踪文档发生任何活动，并汇报给存储管理员。在有些情况下，追踪和汇报只能帮助管理员管理数以千计的归档文件的普通变化。在其他情况下，追踪和汇报却是法规遵从的重要元素，这包括追踪不同级存储间的数据迁移，为了解是哪

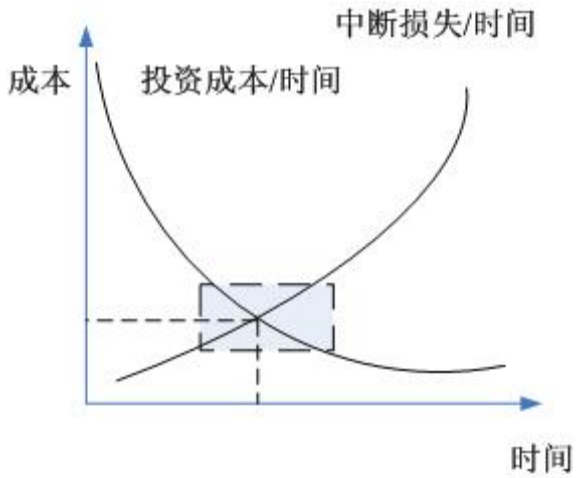
些用户在查找数据而进行的标记搜索和访问，当归档数据被修改时通知 IT 人员，以及汇报删除旧有数据。

4.3.2.3.5 灾难备份及恢复

信息系统灾难恢复的建设是针对于高风险、小概率事件准备的，对于大部分用户来说，灾难恢复系统在多年内可能由于没有灾难发生而无需切换，一些用户对于灾难的发生或多或少抱有侥幸心理，觉得灾难恢复系统可建可不建；但对任何个体来讲，灾难发生后意味着极大的的损失，甚至 100%。

对于准备建设灾难恢复系统的用户来说，应如何建设灾难恢复系统，投入多少才能有效保护企业资产并避免浪费呢？

根据经验，业务中断损失和中断时间之间可以用曲线表示出来，同时方案投入和恢复时间的关系也可以用曲线表示出来，这两条曲线之间的关系如下图：



图示 14：方案投入和恢复时间关系

如上图所示，这两条曲线的交点是最佳投资点，在这一点上可以实现投入和收益的平衡点，结合用户可以容忍的损失数据和中断时间，从而制定企业灾难恢复策略和预案。那么在规划灾难恢复策略和方案时，这一点对应的时间和最佳投资分别是多少呢？这需要专业咨询人员根据企业信息及业务系统现状进行灾难恢复需求分析。

在了解灾难恢复需求分析的原则和所需的用户支持的基础上，我们该如何进行灾难恢复需求分析呢？一般按照如下过程分析：

1、数据的收集

一般采用问卷调查、会面访谈和召开研讨会的方法来收集数据

2、数据的分析

根据己收集的数据进行分析，理清用户业务流程和数据流程。

3、结论达成共识

通过数据分析，需求分析团队对分析结论达成共识。

4、最终结果

分析结论提交给用户审查，并根据用户的反馈意见进行修改和完善，最终得到用户的认可。

5、结果展示

需求分析团队向用户高层汇报分析结果，并期望得到用户高层的认可，从而做为下一步骤制定灾难恢复策略的输入项。

在灾难需求分析阶段，主要涉及到风险分析、业务影响分析和灾难恢复目标策略制定内容，三者之间有着密切关联关系。

风险分析是标识信息系统的资产价值，识别信息系统面临的自然的和人为的威胁，识别信息系统的脆弱性，分析各种威胁发生的可能性，并定量或定性描述可能造成的损失。

风险分析完成后，得到企业一系列存在风险的业务系统范围，业务影响分析则是对这些存在风险的业务系统的业务功能、以及当这些功能一旦失去作用时可

能造成的损失和影响的分析，以确定企业关键业务功能，并评估业务中断影响，确定这些业务系统的恢复需求，为下一阶段制定灾难恢复策略提供依据。

根据前面的风险分析和业务影响分析，我们得到了企业所存在的各种风险及其程度，也分析了解了企业灾难恢复系统建设的需求和业务系统的应急需求和恢复优先顺序，也完成了系统灾难恢复的各项指标。我们应当根据风险分析和业务影响分析的结论制定风险防范策略和灾难恢复策略。灾难恢复策略是从信息系统建设的角度，理解和实现最终用户的需求的方法和计划。

灾难恢复等级的划分

灾难恢复等级的划分对于我国灾难恢复建设领域是一个重要的事件。在灾难恢复等级划分阶段，需要确定七个要素并划分等级，可以引导企业全面考虑灾难恢复体系建设的各个相关方面，防止片面强调个别要素而忽略整体，对于我国灾难恢复建设领域统一、规范概念，指导信息系统灾难恢复规划和建设，客观评定灾难恢复体系建设，对各行业制定相关管理办法和监管要求，对我国灾难恢复领域建立自己的统计和评价体系提供了标准规范。

灾难恢复等级的划分并不是一个强制性的要求。各单位灾难恢复体系的建设必须充分考量本单位、本部门的需求，从满足需求节约成本的角度规划本单位、本部门的灾难恢复体系建设。但是在建设过程中应参考灾难恢复等级划分中关于各个要素的规定，并且最终的建设结果应满足本行业规范中对于灾难恢复等级的最低要求。

灾难恢复策略的制定和实现

灾难恢复策略是基于企业或机构对于灾难恢复需求的确切了解的基础上作出的，其根本目的是为了达到在灾难恢复需求中描述的实现目标。灾难恢复策略是指导整个灾难恢复体系建设的纲领性文件，描述了灾难恢复需求的实现步骤和实现方法。但是，灾难恢复策略不等同于具体的技术方案，灾难恢复策略的制定是原则性、方向性的。

我们可以认为灾难恢复需求是站在信息系统用户/企业拥有者的角度提出的要求和目标,而灾难恢复策略是从信息系统管理者的角度通盘考虑了信息系统现状、成本和可行性之后给出的对于实现方式、实现计划的描述，而恢复方案则是根据灾难恢复策略的要求，从实施人员的角度给出的具体执行层面的选择和描述。

在确定了灾难恢复策略后，应根据灾难恢复策略确定具体的建设方案和建设计划。该阶段主要涉及以下内容：灾难备份中心的建设，数据备份系统建设，备份网络的建设，技术支持和运行维护管理，灾难恢复预案的建设。

4.3.3 应用安全

4.3.3.1. 应用安全的挑战和需求分析

Internet 发展到今天，基于 WEB 和数据库架构的应用系统已经逐渐成为主流，广泛应用于企业内部和外部的业务系统中。在网络高速公路不断拓展、电子政务、电子商务和各种基于 WEB 应用的业务模式不断成熟的今天，却有报道称全球电子商务的发展正在下滑。究其原因，根源在于近两年关于网络钓鱼、SQL 注入和跨站脚本等带来严重后果的攻击事件的频频报道，严重影响了人们对 WEB 应用的信心。根据 Gartner 的报告，目前网络中常见的攻击已经由传统的系统漏洞攻击逐渐发展演变为对应用自身弱点的攻击。企业在安全建设中，应用安全已成为一个日益关注的主题的建设重点之一。下面将对应用系统常见的弱点及其特征作简单分析。

应用系统常见的弱点和危害

- **SQL 注入**

SQL 注入是应用系统中最常见，同时也是危害最大的一类弱点。导致 SQL 注入的基本原因是由于应用程序对用户的输入没有进行安全性检查,从而使得用户可以自行输入 SQL 查询语句，对数据库中的信息进行浏览、查询、更新。

基于 SQL 注入的攻击方法多种多样，而且有很多变形，这也是传统的工具所难以发现和定位的。

- **XSS （Cross Site Scripts）**

跨站脚本攻击属于被动模式攻击，这种攻击的对象是应用系统的最终用户。通过在应用系统插入可执行的脚本，用以获取用户系统中存贮的 Cookie 和 Session 信息。通过这些信息进行加工和重放，就可以轻而易举地进行用户身份仿冒。

- **数据库拒绝服务攻击**

和传统的网络拒绝服务（例如 SynFlood）不同，针对数据库的拒绝服务攻击更加容易发起。通常情况下，一个数据库实例的并发连接数是有限的，如果一个应用程序在处理它和数据库的连接时不当，那么攻击者就很容易利用它对数据库发起大量的“正常连接”，消耗尽数据库和应用程序之间的连接缓冲，以达到数据库无法对应用程序提供正常的数据服务。

- **Cookie 和 Session 欺骗**

B/S 结构的应用系统通常都是采用 Cookie 或者 Session 的验证机制来对某一个用户的身份进行识别和跟踪。Cookie 或者 Session 实际上就成为了用户身份的令牌，如果令牌的设计和验证存在问题，那么导致的最直接危害就是用户身份被仿冒。

- **其他包括常见的弱密码、文件包含等 6000 多种应用弱点。**

应用系统弱点的特征

应用系统的弱点和传统的网络系统弱点有着明显的不同：

- **没有统一性**

操作系统或者网络由于其提供商有限，所以其弱点大部分集中在这几种类型之上，一般情况下，厂商都会提供统一的安全补丁或者解决方案。应用系统则不然，不同的应用系统开发的人员的是不一样的，而且没有两个一摸一样的应用系统，不同应用系统中的弱点是没有共性而言的，每一个应用系统都是唯一的、特有的，里面的弱点也同样符合这个特点。

- **传统的手段难于防范**

传统的安全防护方法(例如防火墙、入侵检测等)对于应用中弱点无能为力，这是由应用系统的功能属性所决定的。应用系统的弱点存在于 OSI 模型的最高层，而传统的安全产品都是工作在 3-4 层的，从这一点来说，传统产品对于应用的安全问题是没有任何帮助的。

- **危害更加直接**

数据是 IT 系统中最有价值的资产，应用系统是数据展现和交互的窗口，应用系统中出现的问题，将直接威胁到数据的安全，其危害甚至的毁灭性的。

4.3.3.2. 应用安全概述

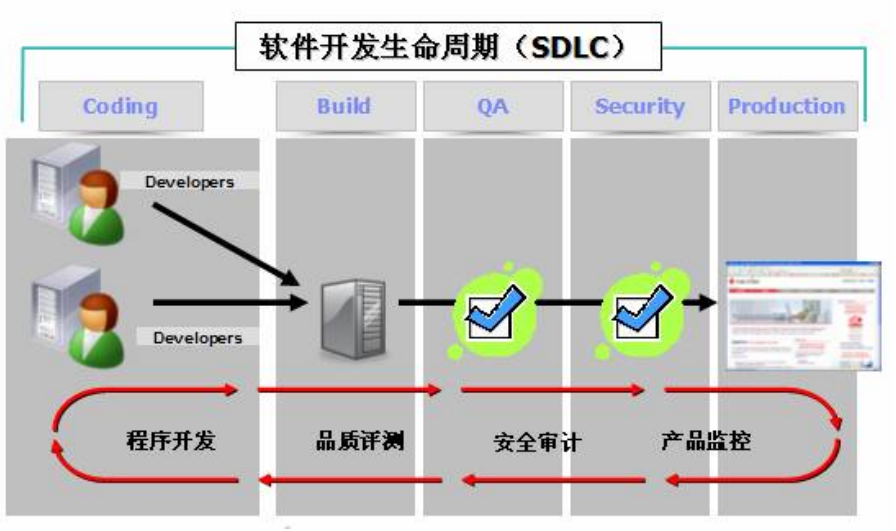
应用安全，就是保障应用程序使用的整个生命周期过程中所有过程和结果和解的安全。是针对应用程序或工具在使用过程中可能出现计算、数据传输的泄露和失窃，通过相关安全工具、策略和控制流程来消除隐患。为叙述方便，本文将应用安全分为如下四个部分分别阐述和介绍。

- 应用开发生命周期安全
- 业务流程的安全
- 应用开发环境的安全
- Web 应用安全

4.3.3.2.1 应用开发生命周期安全

应用开发生命周期将软件工程学和系统工程的理论和方法引入计算机系统的研制开发中，按照用户至上的原则，采用结构化、模块化自顶向下对系统进行分析和设计。具体来说，它将整个应用系统开发过程划分为独立的六个阶段，包括系统分析、程序设计、系统测试、运行和维护以及系统评估。这六个阶段构成应用系统的生命周期。

应用开发生命周期中的安全



图示 15：应用开发生命周期安全

应用开发生命周期安全，包括以下过程：

1) 开发过程中的安全保障
2) 质量管理过程中的安全保障
3) 在集成和发布阶段中的安全保障
4) 对诊断结果进行全面的分析和报告

应用系统安全架构如下：

应用系统安全可按安全技术维度、生命周期维度、安全运维管理维度的三维安全架构进行规划、设计、实施和运维。

安全技术维度包括鉴别和认证、访问控制、内容安全、冗余和恢复、审计和响应技术。信息安全技术体系渗透在每一个信息资产的安全要求和保护之中。五种技术之间有相互的依赖和联系，安全技术体系主要在安全体系框架文档中阐述。

信息系统维度分别从存储、服务器、终端、操作系统、数据库、数据、应用软件等阐述应用系统各个组成部分的安全技术要求和规范。

工程生命周期维纬度分别从应用系统规划安全、应用系统设计安全、应用系统实施安全、应用系统运维安全等方面阐述在应用系统整个生命周期过程中的安全技术要求和规范。

应用安全规范设计主要从应用开发和维护过程为重点，对技术要求和规范进行阐述。

4.3.3.2.2 业务流程安全

业务流程安全需要针对关键应用的安全性进行的评估，分析应用程序体系结构、业务流程、设计思想和功能模块，从中发现可能的安全隐患。同时包括检查应用程序开发、维护和操作流程，以及其他相关部分，包括运行平台、所使用的数据库、所提供的网络服务等。

4.3.3.2.3 应用开发环境安全

应用的安全还需要保障应用开发环境的安全，应用环境安全体系建设根据实施的目的和时间不同可以划分为以下三个阶段：

图示 16：应用系统评估

应用系统评估是全面了解应用系统安全现状的过程，是一个必不可少的部分，从评估可以客观地获得当前应用系统的安全现状，为下一个规范设计奠定基础。

规范设计是根据评估的结果，结合客户的自身的现状有针对性地给出应用安全规范，用以规范应用的整个生命周期。

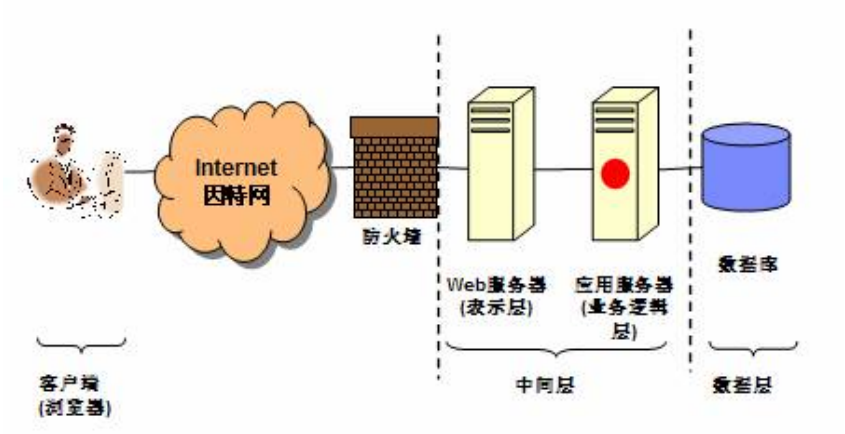
改造实施是根据安全规范，对现有的应用系统进行安全改造，消除在评估中发现的弱点，搭建安全的应用基础平台。

4.3.3.2.4 Web应用安全

Web 应用可以帮助企业发展与客户间更紧密的交互，并改进与企业员工间的协作。但是，在过去的几年里，几乎各行各业所有规模的企业对于与 Web 相关的威胁的数量都在激增。这些攻击多半都是面向 Web 应用的。更惊人的是，截至 2008 年底，在所有已公布的 Web 弱点中，有近四分之三的弱点没有提供补丁。在过去的 6 个月内，基于严重的 Web 应用弱点的结构化查询语言（SQL）注入式攻击数量增加了 30 倍。这一不断增长的攻击通过利用 Web 弱点更改后端代码，操控用户输入数据，从而攻击 Web 站点，窃取敏感目标数据。攻击增加的一个原因在于正在开发的 Web 应用的数量——这一数字正在激增。虽然这些应用具备很多优势，但其用于共享信息的新的协作技术的交互性，也使它们特别容易受到影响，遭到攻击。

Web 应用是由动态脚本、编译过的代码等组合而成。它通常架设在 Web 服务器上，用户在 Web 浏览器上发送请求，这些请求使用 HTTP 协议，经过因特网和企业的 Web 应用交互，由 Web 应用和企业后台的数据库及其他动态内容通信。

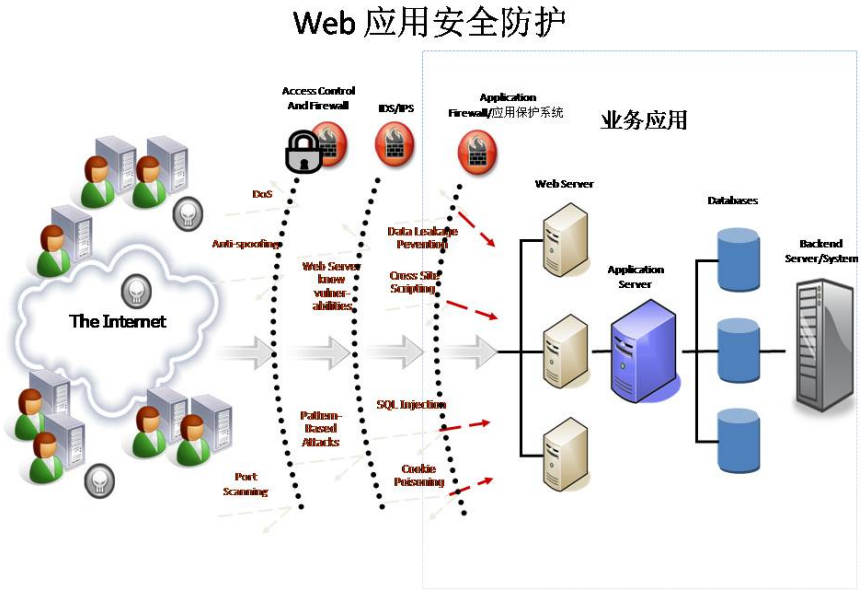
尽管不同的企业会有不同的 Web 环境搭建方式，一个典型的 Web 应用通常是标准的三层架构模型，如下页图所示：



图示 17：Web 应用通常是标准的三层架构模型

在这种最常见的模型中，客户端是第一层；使用动态 Web 内容技术的部分属于中间层；数据库是第三层。用户通过 Web 浏览器发送请求（request）给中间层，由中间层将用户的请求转换为对后台数据的查询或是更新，并将最终的结果在浏览器上展示给用户。

Web 应用安全概览



图示 18：Web 安全概览

在企业 Web 应用的各个层面，都会使用不同的技术来确保安全性。为了保护客户端机器的安全，用户会安装防病毒软件；为了保证用户数据传输到企业 Web 服务器的传输安全，通信层通常会使用 SSL（安全套接层）技术加密数据；企业会使用防火墙和 IDS（入侵诊断系统）/IPS（入侵防御系统）来保证仅允许特定的访问，不必要暴露的端口和非法的访问，在这里都会被阻止；即使有防火墙，企业依然会使用身份认证机制授权用户访问 Web 应用。

但是，即便有防病毒保护、防火墙和 IDS/IPS，企业仍然不得不允许一部分的通讯经过防火墙，毕竟 Web 应用的目的是为用户提供服务，保护措施可以关闭不必要暴露的端口，但是 Web 应用必须的 80 和 443 端口，是一定要开放的。可以顺利通过的这部分通讯，可能是善意的，也可能是恶意的，很难辨别。这里需要注意的是，Web 应用是由软件构成的，那么，它一定会包含缺陷（bugs），这些 bug 就可以被恶意的用户利用，他们通过执行各种恶意的操作，或者偷窃、或者操控、或者破坏 Web 应用中的重要信息。

据上述分析，对 WEB 应用的实时安全保护，应重点针对应用层的跨站、SQL 注入等常见攻击进行过滤和防御。由于企业存在大量自主开发或由 ISV 开发的应用来提供更为丰富的服务， 但开发这些应用的团队在网络安全方面的编程经验和测试规范各不相同，因此很难保证所有应用都能够有效防范黑客的攻击。如何在不修改代码的前提下快速保护应用存在的漏洞成为企业应用平台迅速扩展业务的必要条件。

WEB 应用安全保护应建立在基于应用的完备的基础架构安全（网络防火墙、入侵保护等）的前提下，通过应用扫描、渗透测试、应用保护系统等环节共同构成贯穿整个应用安全生命周期的防护体系，并通过之间的规则共享和动态更新实现更为完整高效的应用层安全。PCI DSS 标准明确建议 WEB 应用安全应包含定期的扫描和专业测试查明应用潜在漏洞，以及在应用前端部署 WEB 应用防火墙，达到透明快捷的防护而无需更改后台代码。应关注的是，WEB 应用的保护是一个连贯的过程，因此应用的扫描结果与应用保护系统的规则应体现连贯性和整体性。

4.3.3.3 应用安全的工作及应用

4.3.3.3.1 应用开发生命周期

一个根本、底层的战略手段就是加强企业全员的应用安全意识。正如前面所阐述过的，对于应用而言，无论是开发人员、测试人员、质量管理人员还是项目经理、企业高层，都会对其功能和性能做更多的关注，这也是由于早期应用多为 C/S 架构的应用，安全问题并不突出。但是在当今的环境，就不得不将安全作为应用质量的基础。

应用的质量模型告诉我们应用的质量需要从这几个方面着手衡量，对于应用，就必须将安全性作为质量模型的基础条件。

图示 19：适于应用系统开发的质量模型

要加强全员应用安全意识，就需要对每一个相关角色落实安全要求。

1) 对于需求分析、设计人员而言，是否已将产品的安全性考虑到产品的需求设计中，从而保证在项目初期，安全因素已被关注；

2) 对于开发人员，在应用中实现了身份认证等安全功能，并不意味着在编程中已考虑到了应用安全性，它们还必须掌握应用安全编程规范等技术；

3) 对于测试人员，不能保证产品已具备安全性，还需要借助其他工具或平

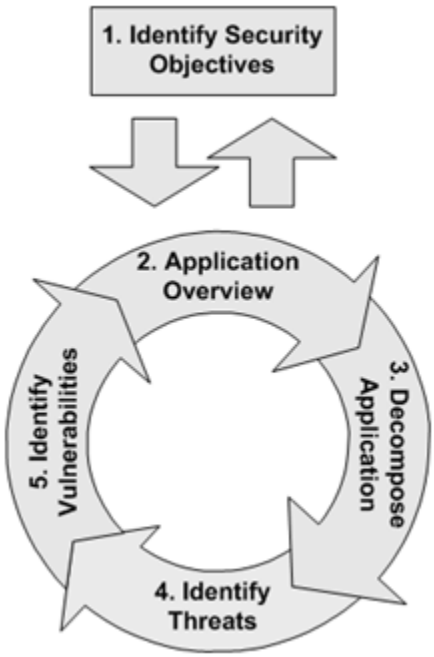
台，对应用的安全隐患，进行自动化的扫描，得出全面的安全性报告；

4) 对于质量管理人员，产品的质量过关，也不等于产品已经安全可靠，他们和测试人员一样，需要借助工具，掌握应用全面的安全隐患汇总和分析。

在企业全员都具有了应用安全意识之后，必须将该意识贯彻到项目的具体工作之中，除了要求每个人具备严谨认真、不断学习的态度之外，还需要借助先进的工具，对开发的应用进行自动化的安全隐患发现、分析、报告、提供修复意见等工作，建立人工检查和自动化工具配合的完整保障措施。

4.3.3.3.2 业务流程安全

业务流程安全工作通常按以下流程展开：



图示 20：业务流程安全评估

整个评估过程分为五个步骤，分别是：

- 确定安全目标
- 创建应用业务流程概述
- 分解业务流程和应用程序

- 确定威胁
- 确定漏洞

每一个步骤都有输入、输出。输入中的有些信息如业务目标、软件需求等资料需要客户方提供，也可以通过进行访谈提供检查列表、回答问题、专题会议等方式确定。

4.3.3.3.3 应用开发环境安全

应用安全规范设计

■ **需求阶段**

需求阶段是整个应用生命周期的起始点，这这个阶段决定了整个应用系统的安全目标和实现方法。

确定安全性关键功能，对软件需求项的安全关键性程度进行识别和区分，确定需求阶段对各需求项的安全关键性进行描述，以便在软件需求生成各阶段适当的相关措施。

软件安全性需求不应包括与非软件引起的系统安全性有关的需求。

- 应用系统的安全组件需求；
- 在需求分析阶段应明确安全需求和与安全相关的相应需求；
- 用户数、终端数、在线并发数；
- 用户角色的划分和权限的分配；
- 应用系统性能要求；
- 现有网络现状和网络性能要求；
- 数据量估计、数据存储方式和周期；
- 系统安全级别和数据保密性要求；
- 其他对网络、存储、服务器、终端、操作系统、数据库、数据等方面的安全需求；

- 应用系统安全功能需求；
- 应用系统数据的需求。

■ 设计阶段

应用系统的安全设计主要包括两方面的内容：一方面是对承载系统本身的安全要求，即承载系统的应具备一定的安全特性（外部系统），另一方面，对系统设计开发过程本身也要进行控制，如在不同的设计开发阶段进行评审和验证，确保设计开发的系统满足规定的质量和安全要求（内部系统）。

- 外部系统的安全设计

外部系统包括和其他应用系统的数据交换方式，传输架构等，这些方面的安全性需要在其他和安全相关的设计和规划的项目中进行评估和改造。

- 内部系统的安全设计

- 身份认证
- 区分公共区域和受限区域
- 密码策略
- Session 和 Cookie
- 认证和授权
- 输入和数据验证
- 配置管理
- 敏感数据

- 应用软件应包含数据安全设计：包括数据库的安全、数据采集、数据传输、数据处理、数据存储、数据备份和恢复的安全。对重要的、敏感数据应进行加密和完整性保护。
- 处理诸如信用卡号、地址、档案等用户私人信息的应用程序应该采取专门的步骤，来确保这些数据的保密性，并确保其不被修改。

- 会话管理
- 加密
- 参数操作
- 异常管理
- 审核与日志
- 应用数据安全设计
- 数据处理安全
- 系统运行日志设计

- **实施阶段**
  - 应用开发的整体环境要求
  - 应用开发的文档安全要求
  - 应用系统的代码安全要求
  - 设计和流程规范
  - 输入输出数据
  - 权限和令牌结构
  - 应用系统的测试安全
- **应用系统维护安全管理**
  - 环境准备
  - 评估和检测
  - 变更管理
  - 操作管理
  - 维护管理
  - 版本管理
- **软件编码规范**
  - 编码前准备
  - 安全性关键软件的编码规则
  - 确定编码和测试标准
  - 使用边界测试工具

- 代码静态分析
- 输入数据检查
- 输出数据检查
- 验证阶段

4.3.3.3.4 Web应用安全

通过前面的分析，我们知道，WEB 应用安全保护是建立在有效的基础架构安全（网络防火墙、入侵保护等）的前提下，通过应用扫描、渗透测试、应用保护系统等环节共同构成贯穿整个应用安全生命周期的防护体系，并通过之间的规则共享和动态更新实现更为完整高效的应用层安全。下面将对 Web 应用安全的主要工作和应用做简单介绍。

Web 应用安全扫描

应用程序扫描是通过将审计的程序代码部署在测试环境或者预发布环境，然后通过专业的应用漏洞扫描软件进行 WEB 程序漏洞扫描。应用程序扫描能够自动的获取所有应用页面并进行漏洞分析。

企业可以采用优秀的 WEB 漏洞扫描工具。通过网络爬虫测试网站应用安全，工具应该具有以下功能：

- 跨网站指令码（XSS）检测
- SQL 程序代码注入攻击检测
- Files that can be found with the GHDB – Google hacking database
- 程序代码执行
- 目录遍历检测
- 网站程序原始码暴露检测
- CRLF injection 检测

- 跨页框指令码检测
- 具有自动查询备份文件或目录功能
- 具有自动搜寻具有敏感性数据的档案或目录
- 具有自动搜寻一般档案，如 记录文件，应用程序追踪，CVS 网站容器
- 具有自动查询目录清单功能
- 具有搜寻弱点权限之目录功能，如可以新建、编辑、或删除档案之目录
- 具有自动搜寻可用的网站服务器技术之功能

渗透测试

渗透测试是一种从攻击者的角度来对主机系统的安全程度进行安全评估的手段，在对现有应用系统不造成任何损害的前提下，模拟入侵者对应用系统进行攻击测试。渗透测试通常能以非常明显，直观的结果来反映出系统的安全现状。该手段也越来越受到国际/国内信息安全业界的认可和重视。

- **渗透可行性分析**

渗透测试主要依据已经发现的安全漏洞，模拟入侵者的攻击方法对系统和网络进行非破坏性质的攻击性测试。

渗透测试利用安全扫描器和富有经验的安全工程师的人工经验对指定的服务器进行非破坏性质的模拟入侵攻击，目的是侵入系统并获得渗透测试对象的最高权限。事后将入侵的详细过程和细节以报告的形式提交给用户。由此确定用户系统所存在的安全威胁。并能及时使安全管理员发现系统维护和管理中的不足，以降低安全风险。

渗透测试是工具扫描和人工评估的重要补充。工具扫描具有很好的效率和速度，但是存在一定的误报率，不能发现高层次、复杂的安全问题；渗透测试需要投入的人力资源较大、对测试者的专业技能要求很高（渗透测试报告的价值直接依赖于测试者的专业机能），但是非常准确，可以发现逻辑性更强、更深层次的弱点。

渗透测试主要针对系统主机进行，因此将占用主机系统及其所在的网络环境的部分资源。对于其它的资源没有特殊的要求。在有周密计划、良好组织的前提下由有经验的专家来进行，不会对系统造成破坏。

- **渗透测试方法及对系统的影响**

黑客的攻击入侵需要利用目标网络的安全弱点，渗透测试也是同样的道理。它模拟真正的黑客入侵攻击方法，以人工渗透为主，辅助以攻击工具的使用，这样保证了整个渗透测试过程都在可以控制和调整的范围之内。

由于采用可控制的、非破坏性质的渗透测试，因此不会对被评估的系统造成严重的影响。在渗透测试结束后，系统将基本保持一致。

应用防火墙/应用保护系统

通过应用扫描 ,渗透测试等环节可以有效发现应用系统存在的漏洞和相关的安全问题。除了针对这些漏洞进行代码修改之外，为了实现快捷方便的防护和补丁，通常可采用应用层保护系统来实现。应用层保护系统逻辑上包含 WEB 应用防火墙系统和数据规范安全保护系统，物理上可体现为一套架构。

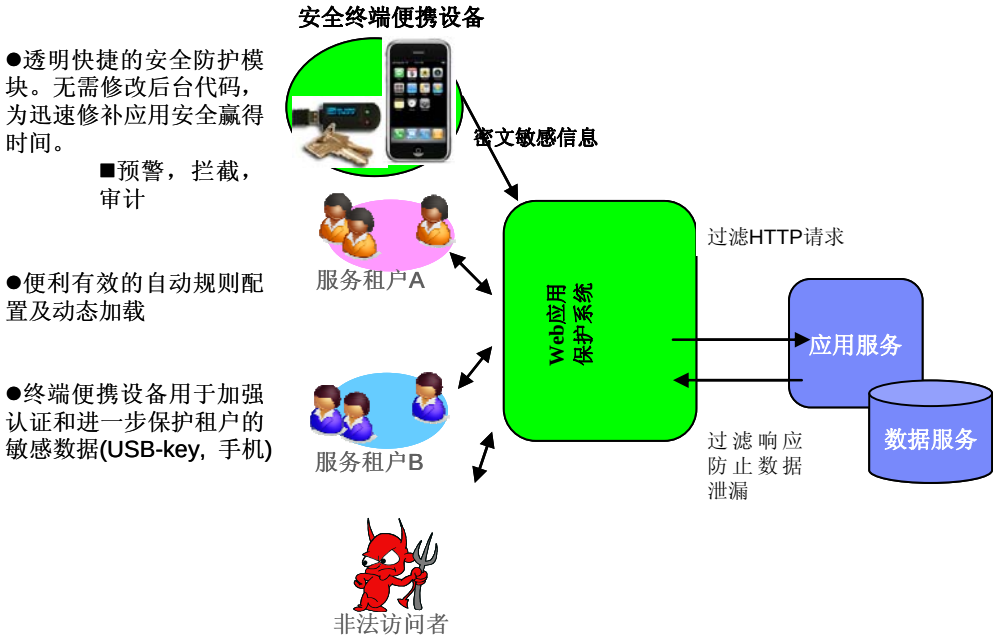
- **WEB 应用防火墙系统**

服务器端 WEB 应用防火墙部署在客户端与应用服务器之间，在不改动应用代码的前提下可防范多种当前针对 WEB 应用服务的攻击，因此为应用安全保护有效赢得了时间。 特别应结合对现今网络应用的趋势提供针对 Web2.0 ,AJAX，mash-up 业务集成等场景的攻击类型的防御。WEB 应用防火墙的选择标准应包含以下几个重点：1）部署方便，易于与现有 WEB 架构集成并能兼顾未来的扩展性； 2）支持类型广泛，对 Web2.0, AJAX, mash-up 等场景都能很好支持，能有效判断黑客以各种编码格式进行的规避； 3） 同时支持黑名单和白名单定义，提供基本规则集，并允许管理员可自由根据 URL, IP, 请求字段等约束条件灵活扩展规则定义；4）提供自动或半自动化工具辅助管理员规则配置以降低安

全规则维护成本，并能结合应用安全的扫描结果进行整合维护；5）对误报率的有效控制，并提供与应用体验协调的用户信息提示；同时应提供详细的安全分析展示工具，便于管理员快速维护，对应用系统安全状况有全面了解。

- **数据规范安全保护系统**

数据规范安全保护系统对应用的商务数据安全和用户隐私信息进行保护，可基于手机等便携设备进行定制，充分提高用户访问 Web 应用时的身份认证，交易，和隐私安全，并提供给用户可感知的安全。基本功能包含对应用上下行的数据检测，屏蔽或模糊化对敏感信息的泄露，以及根据企业定义的规则进行相应的规范性审计。



图示 21：WEB 应用保护系统架构

4.3.4 基础架构安全

随着企业 IT 信息化的发展和深入，日趋复杂的信息系统对企业 IT 基础架构提出了更多的要求，网络技术和计算机应用几乎普及到中型企业的每一个职能

部门，信息化所带来的高效率和高风险并存。

对公司的网络、服务器和端点主动实施威胁和安全漏洞的监视和管理对于公司钳制新兴威胁 ,防止它们对系统组件以及相关人员和业务流程产生负面影响至关重要。由于新兴威胁是有组织的攻击并且通过渗透公司网络使公司蒙受巨大经济损失，因此，企业越来越重视识别和抵御快速增长的新兴威胁。

4.3.4.1 基础架构安全的挑战和需求分析

■ **网络及边界安全的挑战**

- 病毒和恶意代码的泛滥，零天攻击攻击不断涌现

大量商业化和自动化的黑客工具的出现，越来越多的零天攻击，造成大量的企业、机构和个人的电脑系统遭受程度不同的入侵和攻击，或面临随时被攻击的危险。企业如何跟上不断推陈出新的恶意代码的脚步？如何能够真正做到前瞻性防护？如何在基础架构层面保护脆弱的 WEB 应用？

- 内部威胁

内部工作人员能够较多地接触内部信息，对信息安全带来的威胁更大。比如他们可以窃听网络上的信息，窃取用户密码、数据库等信息。研究表明，公司因安全事件造成的损失 86%是由内部人员引起。

随着移动设备的广泛应用——PDA、笔记本电脑和手机成为办公室人员的必需品，经常出外工作的员工会将移动设备与企业系统做信息同步处理，极有可能将电脑病毒带至企业内部网络，从而威胁网络安全。从 2003 年开始后爆发的 Slammer、Sobig、Blaster、Conficker 等病毒对企业网络造成了重大的破坏。

- 安全设备/网络设备管理和维护

企业可能已经部署了一些安全设备，但有可能策略配置不当或疏于管理，或者安全告警没有及时处理，这一方面可能是因为管理人手和精力有限，另一方面

也可能受限于管理人员的技术水平，使得这些设备并没有能够发挥出应有的作用。所以很多企业常常感觉虽然已经部署了各种安全设备，但却仍然时时受到安全事件的困扰。

- 海量安全事件，监控和管理非常困难

信息安全事件随时发生，及时掌握问题并采取必要的防御手段已经成为企业正常运行的必要工作之一。为了能够及时地检测、响应安全事件，并找出风险的根本所在，企业的信息安全技术人员需要处理诸多设备生成的海量数据，因而，信息系统规模庞大、应用复杂的企业常常面临诸多棘手的问题。如何能够在降低基础架构管理的整体成本的同时，有效地处理这些海量数据？

- 不能清楚了解基础架构的安全状态

新发现的漏洞数量持续增长，2008 年新发现的漏洞数量多达 7000 多个，但很多企业缺乏检测机制和工具，根本无法了解网络中可能存储在的安全隐患。只有了解自己，才能做到防患于未然。

- 内容安全

很多信息在网络上以明文的方式传播，很容易被搭线窃听。企业网络中有很多重要机密信息/文件，这是企业的重要资产，如何保证这些机密信息的安全？如何防止这些机密信息被有意或无意地泄漏？

■ 主机系统安全

主机系统安全的问题包括：

1）如何检查进入服务器的流量？阻止试图入侵和提取关键数据的恶意代码；

2 如何尽早发现服务器的安全风险？目前绝大部分的攻击行为都是利用了系统漏洞进行传播或者渗透的，实时掌握目前企业自身所使用到的系统和应用

平台是否有存在被最新披露的安全漏洞对于运维人员来说可以真正帮助企业有效的规避一些安全风险，确保自身 IT 基础架构的安全。

3）企业面临各种安全遵从的压力：随着大量的 IT 安全的法律法规的出台，企业面临着非常大的安全遵从的压力（如 PCI 认证，“信息安全等级保护”要求，HIPPA、SOX、ISO27001 等等），而几乎每个安全遵从要求中都对主机安全有着明确的定义，因此如何在这么多安全遵从的夹缝中找到一条既符合自身企业业务发展需求而又不违背遵从要求的服务器安全标准成为摆在企业面前的一个难题。

4）对于发现的安全风险缺乏必要和完整的管理流程：目前很多企业会通过一些漏洞扫描工具来对自身服务器进行安全评估，但是面对这些被发现的安全风险并没有一套完整的跟踪处理机制来进行管理，从而导致这些安全风险没有被及时处理或者由于分工不明确而出现推诿现象，最终反而加大了服务器的安全威胁。

5）如何实现企业数据丢失防护（DLP），满足企业数据丢失的防止战略和前瞻性的保护；

6）如何可以将服务器防护功能无缝接入到企业的 IT 基础设施。

7）如何实现服务器应用审计，在制订应用或网络锁定策略之前，对运行和访问网络的应用进行快速审计。

8）如何实现服务器安全策略统一制定，确定服务器上只运行获得授权的服务和应用，防止安装未经授权的程序。

9）如何实现服务器网络访问策略统一制定，确定只有获得授权的应用可以访问网络，并为入站和出站流量设置端口和 IP 限制。

10）如何确定敏感文件、关键系统二进制和配置文件的完整性，并能将实时文件完整性监控与文件系统基线相结合，跟踪未经授权的用户所进行的更改。

■ 终端桌面安全

终端用户已成为网络安全的主体，并且用户的风险正在逐渐增大；目前，企业在终端桌面安全方面面临的问题主要有：

1. 恶意代码泛滥成灾

近几年来，恶意代码层出不穷，数量持续增加。研究表明，2007年新爆发的恶意代码数量近410,000个，平均每天就有一千多个新增的恶意代码；恶意代码种类繁多，传播途径非常多样化，零天攻击越来越多，让终端用户防不胜防；以前攻击者最常用的方法是诱使用户安装恶意代码，包括：电子邮件附件、即时消息、P2P应用程序交换文件、弹出广告、免费音乐下载或其它免费软件；现在在Web网站上种植木马、后门等病毒，已经成为黑客们惯用的手法。而一台终端感染病毒/蠕虫、木马，往往危及整个网络。

2. 终端用户对安全现状缺乏足够认知

可能很多企业员工可能已经意识到操作系统补丁的重要性，但他们往往忽略了其它应用系统存在的问题。研究表明，客户端浏览器的高风险漏洞占到50%以上，远远高于操作系统的漏洞；对于近年来利用pdf、mpeg、office文件传播病毒的情况，企业用户更是缺乏足够的警觉。

3. 网络非法接入

外来人员可以随意将笔记本、PDA等设备接入企业网络，一旦这些终端设备携带病毒，很可能造成企业网络病毒泛滥或内部机密文件被盗取，严重威胁企业网络的安全性和机密性。

4. 移动存储设备的有效管理

现在U盘、MP4等诸多移动存储设备已经广泛的融入了人们的日常生活之中，企业员工随意使用这些移动存储设备的情况非常普遍，但是已有很多的病毒

木马将移动存储设备作为了一项常规传播手段。比如年初造成法国空军飞机停飞的Conficker病毒，正是通过一位在家工作的法国士兵使用U盘而导致蠕虫传播进入网络。移动存储设备的广泛使用为病毒的泛滥提供了温床。

5. 非法外联

员工通过Modem随意拨号上网，旁路了企业部署的各种安全措施，为病毒、木马攻击企业内网提供了理想的通道，黑客也极可能以该主机为跳板攻入内部网络，窃取内部机密资料，严重威胁到内网的稳定运行和内网中内部数据的安全。

6. 补丁统一分发和管理

终端桌面上运行了大量的程序，操作系统、office办公系统、IE、Adobe等等，这些程序可能随时都会发布新的补丁，如何能够让全网内每台终端都能及时打上各种重要补丁，维持较高的补丁水平，确实是让企业感到头疼的问题。

7. 安全策略强制执行

企业制定了一系列的安全策略，但往往由于缺乏技术和手段，难以确保和强制终端桌面遵从，使得安全策略形同虚设。

8. 终端桌面安全产品品种繁多，缺乏统一管理

终端桌面安全产品包括有防火墙、防病毒、防泄漏、防入侵、补丁管理、内容管理等等，品种非常丰富，往往这些单一产品各自为政，缺乏统一管理界面，为管理和维护带来了麻烦和提升了成本；另外，由于在终端上安装了过多的终端桌面单一产品，将导致终端桌面上运行的引擎过多，从而极大地耗费了系统资源，影响了终端的正常运行。

4.3.4.2 基础架构安全概述

4.3.4.2.1 网络及边界安全

在当今信息化社会中，IT 已经成为商务活动的重要渠道，企业通过 IT 与客户、合作伙伴和雇员进行联系，传递信息，企业的发展和竞争力的提高越来越依赖于企业的信息化程度，而在 IT 基础架构日渐成为企业不可或缺的重要工具时，能否为其提供可靠的安全保障显得尤为重要。

安全漏洞、黑客侵袭、人为错误，病毒干扰，信息泄漏，混合威胁，……种种来自内部、外部的问题，使企业的 IT 基础架构的安全难以得到保障，在网络、IT 系统广泛应用的今天，这是每个企业都面临的问题和挑战。

4.3.4.2.2 主机系统安全

通常主机上有企业的核心应用和重要的信息和数据，对于企业来说，核心应用服务器是整个 IT 基础架构中的重中之重， 如何有效地提高主机的安全防护效率以及完善主机的安全管理流程是企业的 IT 部门首先需要考虑的问题。

随着 IT 技术的飞速发展，IT 基础架构的安全逐渐被企业用户所重视，而其中的主机安全逐渐成为一个潜在的巨大问题，如何保障自身应用服务器的安全，及早了解服务器上存在的安全隐患 ,以及对于被发现的这些安全风险如何进行管理，是目前许多 IT 人员关注的焦点。

由于目前大规模的业务电子化，大量的企业信息系统被广泛的应用；随之而来的就是大规模信息化所引发的信息安全问题。目前国家相关的监管机构也意识到相关风险的存在，制定出台了一系列的信息安全相关标准，规范和指引以满足信息安全的保护要求。企业如何能够识别相关的要求，评估目前信息系统的现状与要求的差距，并且快速反应，有针对性的进行处置是目前企业 IT 部门的重要任务之一。

任何一个初步建立起来的系统，其自身安全问题是很多的，即便是经过了谨慎的配置，但由于安全动态发展的特性，新的问题还是会不断涌现的。系统自身由于配置或者操作管理不慎造成的漏洞，几乎是目前绝大多数黑客或者自动化的黑客工具——病毒蠕虫赖以攻击的绝好条件。同时，目前大多数企业的系统管理员还停留在简单的系统管理层面；许多系统管理员对于相关的系统安全性的理解也停留在一个简单或者比较片面的用户帐户和口令的安全性上，而会忽略到很多主机系统基本的安全配置问题。

4.3.4.2.3 终端安全

随着计算机的普及和深化应用，企业对信息系统的依赖性越来越强，员工的日常办公和业务运行都已经离不开电脑和网络。由于终端数量众多，并且散布在企业网络的各个地方，且终端的类型也多种多样包括PC，手机，PDA等，终端安全已逐渐成为目前企业网络安全中存在的最让人头疼的主要问题之一。终端安全管理不当会导致企业容易遭受更多的网络攻击，引起生产力损失、机密信息的泄漏，以及其它代价高昂的损失。

据国际IT权威机构的估计，大约40%以上的受控系统遭受的不同程度的安全危害与桌面终端安全有关。

另外，内部员工毫无顾忌地使用与工作无关的网络应用，如网络聊天、网络游戏等，也给管理工作带来困难，给企业发展造成不利影响。

4.3.4.3 基础架构安全的工作及应用

4.3.4.3.1 网络及边界安全

企业应该从三个层面考虑网络安全，即网络架构安全、网络安全技术部署和网络设备安全配置，并通过不断的评估和优化提高企业整体的网络安全水平。

- 网络架构安全

- 安全域划分和安全边界定义
- 结构冗余性
- 服务器和终端桌面的安全接入

➢ 网络安全技术

- 访问控制
  - 防火墙/访问控制列表（ACL）
  - 网络准入控制（NAC）
  - 广域网流量控制
- 防病毒/防黑客
  - 防病毒
  - 入侵防护系统
  - Web 应用防火墙
- 内容安全
  - 虚拟专用网（VPN）
  - 防泄漏（DLP）
  - 垃圾邮件防护
  - 网页过滤
- 认证和授权
  - 网络设备接入的 AAA
  - VPN 接入的 AAA
  - 无线网接入的认证和授权
- 审计跟踪

- 漏洞扫描系统
- 安全事件管理平台

➢ 网络/安全设备配置/维护

- 定义正确适用的安全策略/访问策略
- 定期扫描，发现网络/安全设备中的漏洞，及时升级和为系统打补丁
- 安全报警及时处理

4.3.4.3.2 主机系统安全

主机安全防护应从网络层、应用层、内容安全、安全管理等多个层面加以考虑。主要目的是对主机节点进行全面防护，和网络安全防护配合，形成有层次的立体防御体系。

1）网络层安全防护

主机系统抵御网络攻击的技术主要有四种，包括主机防火墙、主机入侵防护、缓冲区溢出保护和主机防病毒。其各自的主要用途如下：

- 主机防火墙。防火墙通过阻断对特定端口、单个或某 IP 地址段、以及特定协议和服务的访问，来抵御针对这些资源的攻击。
- 主机入侵防护。入侵防护功能具有深层次的数据包检查能力，检查数据流量，在向用户报告针对主机所发生的攻击行为的同时，阻断攻击行为。主机入侵防护可以与网络防火墙配合形成更为立体的防护体系，阻断躲过防火墙的攻击行为，确保主机系统的正常运行。
- 缓冲区溢出保护。缓冲区溢出防护实时监测并阻止利用缓冲区漏洞的各种攻击，即使攻击行为利用了未知漏洞，缓冲区溢出防护仍然可以通过检测主机缓冲区的合法长度进行阻止。形成入侵防护的最后一道防线。
- 防病毒。利用基于病毒库的检测技术和基于行为的检测技术，有效的防御已知甚至未知的病毒威胁，保护主机系统安全。

2）应用层安全防护

应用程序安全防护用来保护主机免受基于应用的攻击。应用程序控制技术能够在攻击的开始阶段保护主机免受威胁，应用程序控制能通过策略制订和静态规则来减小受攻击面。另外，应用程序控制还可以主动限制主机可以运行、联网应用程序，起到一定的主动安全防御的作用。

3) 内容安全防护

这里的内容主要指主机系统中的重要文件、数据、信息等。在主机系统的安全防护工作中，内容属于需要重点保护的核心资产。内容安全防护的主要目标是防止重要文件被破坏，包括篡改、非法访问和使用，以及数据损坏和丢失等。内安全防护通过对关键文件的实时审计和监控，结合终端的数据加密、数据防泄露等技术，实现以上防护目标。

4) 安全管理

主机系统做为运行信息系统重要应用，保存重要数据的节点，其运行情况、被访问情况、系统配置和维护情况、自身安全情况都需要得到全面的管理。通常涉及以下几个主要方面：

- 主机弱点管理
- 补丁管理
- 主机系统日志/应用日志审计
- 安全事件管理和响应

只有通过对以上方面持续不断地安全管理和维护，才能有效保证主机系统的整体安全。

4.3.4.3.3 终端安全

根据终端安全的需求，企业应采用先进的管理技术和完善的管理制度建立统

一的终端安全的监控、管理系统，提高终端设备的管理效率，保护终端安全，从而保障网络和信息系统的安全。

终端安全应该实现的目标是：

- 通过统一的安全基础框架，将所有的安全功能应该纳入统一的管理。
- 通过网络准入控制，实现对接入企业内网的终端访问网络资源的权限进行认证、授权和审计。
- 通过定制安全防护策略，对终端系统进行安全加固。
- 实现终端各种补丁程序自动化更新，减少系统漏洞。
- 制定终端安全管理相关制定，并强制执行。
- 对重要/机密文件进行加密，实现对重要/机密文件的保存和传播环节进行安全控制和保护。
- 通过定期开展终端用户安全意识教育，提升终端用户的安全认知水平。

具体功能应从终端基础安全、终端数据安全、终端系统维护、安全管理配置几方面加以考虑。

终端基础安全

入侵防护系统

提供主动防护，可对各种入侵行为和攻击性流量进行拦截，阻止各种网络攻击行为的发生。

防火墙

实施访问控制策略的系统，对流经的网络流量进行检查，拦截不符合安全策略的数据包。在不妨碍终端正常通信的同时，能够阻止其他用户对计算机的非法访问。

防病毒

针对已知病毒、木马、蠕虫提供保护，检测、移除间谍软件。

终端数据安全

网络准入控制

自动阻断非法主机或者不合规（比如防毒软件版本）的主机接入网络。

防泄漏

杜绝终端主机上的敏感或机密信息和/文件被盗取。

加密

提供加密的能力，实现对重要/机密文件在存储、传播过程中可能产生的泄密风险进行控制。

安全配置管理

配置管理

帮助终端安全地配置系统，也可和各种法律法规的配置检查清单相结合。

策略管理

主要实现桌面终端安全防护策略、桌面终端接入策略、桌面终端网络外联策略、U盘等外设使用策略等。

合规性

利用由标准组织提供的安全专业能力和指导方针，通过基于法规遵从的配置检查清单安全地配置系统。监控桌面终端是否符合遵从企业制定的安全策略。

终端系统维护

资产管理

能够通过管理软件自动收集形成软、硬件信息清单，可对终端的硬件和软件资产变更进行审计和处理，统计软件许可使用情况。

补丁管理

自动监控和向终端分发各种补丁 ,包括操作系统和各种应用程序的补丁。

软件分发/删除

通过制定有效的软件分发策略和分发机制、以及操作系统定制，实现户特定应用软件和操作系统的自动安装

电源管理

通过终端电源管理，在获得最大电源节约的同时，避免中断IT系统管理，减少碳排放。

4.3.5 物理安全

为了在一个企业里有效地实施企业安全计划，我们必须了解和处理与物理基础设施相关的业务和技术风险。IT 安全治理、风险管理与合规提供物理安全相关的风险种类指导、计划和响应的指导。

保护组织的物理基础设施可能指防护或预防对因某一故障或物理基础设施的损失而造成的对业务连续性的可能影响。保护组织的基础设施可能涉及间接威胁和漏洞的保护，例如实用服务的丢失，物理访问控制的渗透，或关键有形资产的丢失所造成的影响。有效的物理安全需要集中的管理体系，它可以关联来自不同来源的信息，包括：财产、雇员、客户，公众场所和地域天气等。

例如，对于我们的数据中心及周边环境，用摄像机和集中式监控设备是非常重要的，可以确保对组织 IT 资产的访问管理。因此，对于防范盗窃和诈骗的相

关组织，如银行、零售商店或者公共机构，应确定和实施一个综合性的物理安全监视战略，包括监测、分析和集中控制。这种方法使得组织可以从多种来源提取智能的数据，相对人工监测环境可以提前应对威胁，以降低成本和减少损失的风险。

在处理和映射到组织的 IT 安全领域中物理安全解决方案后，可以考虑建立一个更加技术的安全架构的各个方面。在下面部分中，参照 IBM 企业信息安全架构，可以指导组织的 IT 安全专业人士确定能在所有领域可行并符合安全建设原则的物理安全环境，以及整个物理区域和环境的基本服务。

4.3.5.1. 机房物理安全

4.3.5.1.1 机房物理安全的挑战和需求分析

企业的 IT 系统基本上都部署在计算机机房内，机房的物理安全是企业整体安全框架中非常重要的部分，但并不是每家企业都对机房的物理安全有足够的重视，或者即便重视但不清楚现有的机房物理安全措施是否满足要求、以及是否有效。此外企业也缺乏对于机房物理安全相关标准、规范的了解，这些都是困扰企业的问题。

计算机机房物理安全是包含在信息安全整体框架里面的，但是不同于其他安全服务能力如网络安全、身份管理等，在企业中通常缺乏熟悉该领域的专业人员，这部分工作有时由安保或综合管理部门来承担，这样并不利于信息安全的统一管理。

如果计算机机房物理安全控制措施的缺失或者不足，企业 IT 系统所面临的风险就会急剧加大，一旦发生安全问题，其后果和影响就会十分严重。所以，在这个环节上不能有任何的疏忽。

4.3.5.1.2 机房物理安全概述

计算机机房物理安全涉及到计算机机房物理环境的防护、计算机机房场地安全、操作室场地安全三方面，具体包括：

- 物理环境的防护
  - 大楼物理位置的选择
  - 外部关键区域和关键通信设备
  - 大楼周界照明系统
  - 机动车通道控制
  - 停车场和车库
  - 大楼周边保护
  - 大楼外围通道
  - 窗户和玻璃幕墙
  - 大堂及其公共区域
  - 装卸区
  - 办公室场地
- 计算机机房场地安全
  - 门禁和访问控制
  - 防盗窃和防破坏
  - 防雷击
  - 防火
  - 防水和防潮
  - 防静电
  - 温湿度控制
  - 电力供应
  - 电磁防护

- 禁带物品
- 其他安全

■ 操作室场地安全

- 门禁和访问控制
- 防盗窃和防破坏
- 防火
- 防水和防潮
- 防静电
- 温湿度控制
- 电力供应
- 电磁防护

4.3.5.1.3 机房物理安全的工作及应用

计算机机房的物理安全应该在数据中心设计、建设的阶段就规划好、部署好，并且在机房投入运行后由内部或外部的专业人员定期进行检查、评估，以保障相应措施的合理性、有效性，降低企业的安全风险。

计算机机房物理安全的设计和评估工作首先要满足国家的相关规范，同时也要参照业界的最佳实践和方法论，这其中主要包括：

《信息安全技术信息系统安全等级保护基本要求》

《GB9361-1988 计算站场地安全要求》

《GB2887-1989 计算站场地技术要求》

计算机机房物理安全的设计工作一般是和数据中心、机房的设计、建设同步进行的，具备相应技能的专业技术人员和企业的信息安全负责人、基础设施负责人等相关人员进行详细的需求调研，收集和整理需求信息，同时通过场地的

实地勘查了解机房场地的外部环境、场地布局等实际情况。在完成信息收集的基础上，参照国家、行业的相关标准和规范，以及业界的最佳实践和方法论，为企业进行计算机机房的物理安全的规划设计。完成后的设计要求会提供给机房装修、弱电、布线等设计人员，作为详细设计的依据。

计算机机房物理安全评估工作的依据和设计工作一致，评估工作主要通过访谈、实地考察、阅读管理规范、检查日常记录等方式检查现有的机房物理安全措施是否符合要求，如果不符合将给出偏离的描述和整改的建议。

4.3.5.2. 视频监控安全

4.3.5.2.1 视频监控的挑战和需求分析

在今天的社会环境中，几乎每个城市、代理机构、教育机构、公众运输中心、金融机构、公用事业设备和医疗中心都必须针对威胁制定保护其财产、员工、客户、公民和 IT 基础设施安全的计划。此外，所有业务部门在努力降低运营成本、提高生产率、增加利润以及客户满意度的同时，都面临着保护他们的客户、员工和资产的挑战。使用监控手段更有效地管理安全风险和业务问题的例子包括：

公众安全

不断增加的威胁，驱使许多政府机构部署监视摄像机和感应器来提供重要设施周围的态势感知。例如学校校园必须做到保护出入口，维护 IT 网络安全，防止故意破坏行为和避免授权问题。

机场/海港/铁路

公众运输企业和机构必须保护乘客、工作人员和物理资产免于恐怖威胁或安全破坏，并遵守监管要求。

零售店

零售行业采用监视设施以减少诈骗、盗窃和管理错误。零售商店也使用视频和分析资料，用以确定促销展示的效力，及计算不同区域的顾客数量来优化商店布局以及销售的成效。

金融机构

许多银行需要 24 小时人工监控内部操作和自动柜员机（ATM）。监控和分析的目的是减少抢劫威胁以及欺诈行为。许多银行通过一个中央指挥和控制中心来集中监控视频、语音和交易信息，以巩固跨分支机构的安全控制。

4.3.5.2.2 视频监控安全概述

监控技术的进化

企业几十年来将监控作为一项对盗窃、诈骗、暴力等犯罪活动威慑手段。在过去的十年里，监控技术发展成为不仅用于帮助组织机构更加快速地发现和响应威胁，还可以帮助企业着眼于提高业务运营。监控技术的三个时代通常被形容为：

- 模拟
- 数字
- 智能

模拟视频监控

视频监控最具有代表性的是根据特定业务需求在敏感或有战略意义的位置部署模拟摄像头，并和闭路电视（CCTV）相连以进行实时监控。这不但震慑了犯罪活动，而且还记录了人员和财产的动向。移动视频监控的方法，例如在巡逻汽车，公共汽车和火车安装摄像头，也经常被用来记录事件。

使用模拟摄像头产生的成百上千的录像带，之后必须由保安人员观看。除了储存的录影带，聘用保安人员来亲自监控成百上千的摄像头的费用也可以让人望而却步。此外，录像带可能是低画质的，并且会随着时间日益恶化。

更为重要的是，研究表明，一个人被分配坐到视频监视器前一天好几小时观看特定事件是一个低效的安全措施。实验证明，仅仅观看和分析监控电视屏幕 20 分钟，大部分人的注意力都将下降到远远低于可接受的水平。监视电视屏幕是既枯燥又令人昏昏欲睡的。此外，磁带的手动搜索可能会需要很长时间才能提供用以协助调查所需的重要信息。

而且，视频通常只能从一个单一的不能分享的终端观看。这限制了将信息发布到整个企业的能力，不利于减少企业范围内的威胁和警报。最后，模拟视频系统不能满足从安全数据中提取商业智能信息的要求。

数字视频监控

今天，视频监控仍然和以往一样重要，但它担任了新的角色。数字视频、IP 摄像头、网络录像机、网络视频、消费级摄像头和视频智能的出现，为企业开辟了广泛的应用，能为企业提供增强的功能和商业价值。

数字视频监控（DVS）使企业能够建立有效的风险管理战略，这将帮助他们管理和保护商业信息和技术资产，预计脆弱性和风险，以及维护随时获取信息的渠道。

许多组织机构有零散的解决方案，并且面临着拥有多个互不相连的系统的挑战。通常，IT 安全和物理安全的分离，不允许组织机构利用现有的 IT 基础设施和应用，比如已有的身份（ID）管理和交易系统。完全割离的 IT 安全和物理安全系统，操作额必需完全分离，这不仅效率低，而且带来了更大的劳动强度和昂贵的成本。

迁移到一个数字视频监控解决方案将有助于解决一些以录像带为基础的模拟系统的局限性。DVS 可以通过如下方法帮助企业实现安全投资的更高回报：

- 通过加强的智能聚集，实现对安全事件进行实时检测和可能预防
- 事后调查时使用基于事件的查看方式，无需按时间顺序审查录像带

- 减少监控摄像头和更换磁带的需要
- 通过威慑潜在的商店扒手和监控工作人员，增加产品的安全性
- 为欺诈性索赔提供证据
- 增加室内和停车场安全

智能监控

智能监控，智能视频监控，视频分析，智能视频和智能分析都是典型描述下面这一概念的名称：在摄像头和传感器上应用自动信号分析和模式识别，目标是从视频和传感器流中自动提取“有用信息”。

智能监控通过整合企业内部硬件，软件和服务来优化安全，从而达到集成物理安全和 IT 安全的目的。智能监控的一个主要组成部分是一个智能监控分析器，它提供了实时决策和事后人员和活动的事件关联分析的能力。

智能监控的架构和功能

智能监控系统重要组件是智能监控分析器，这一技术主要指的是：“自动地分析和抽取视频源中的关键信息。” 如果把摄像头看作人的眼睛，而智能监控分析系统则可以看作人的大脑。它提供了对实时或录像视频序列进行高效分析的独特能力。智能监控分析器通过传感器（如视频摄像头、雷达或音频输入）监控或分析产生于实际环境中的事件。

智能监控的框架要具备以下能力：

- 视频/传感器分析能力
- 能够集中处理多种来源事件信息的框架
- 能集成至企业业务流程的框架

智能监控分析器为最终用户提供了以下类型的功能：

- 实时告警：用户可以为单个摄像头/传感器或多个摄像头和传感器定制包含多个条件的“告警定义”。智能监控分析器根据该告警定义利用它的分析能力评估各传感器检测到的事件。每当“告警定义”被触发，智能监控分析器可提示用户事件发生。
- 用户驱动的查询：用户（人或应用程序）可使用智能监控分析器对已归档的事件元数据执行基于内容的查询。例如，智能监控分析器可找回某个摄像头所有关于“一辆红色的轿车”驶过停车场的事件。

智能监控分析框架 - 智能监控分析器框架提供了一组功能，用于设置、管理和操作一个含有摄像头、传感器以及由交易系统所提供的事件的大型系统。该框架支持：

- 用户管理：这类服务提供将用户添加至系统并以特定权限访问摄像头的能力。
- 系统管理：这类服务包括管理摄像头、分析引擎、地图、分析器产生的元数据内容的能力。
- 元数据索引和搜索服务：这类服务利用智能监控引擎所获取的元数据，进行解析后存入关系数据库，并为应用程序提供从元数据搜索和获取事件的 Web 服务。这个元数据数据库不仅为告警，同样为事件建立了完全索引。
- 扩展服务：这类服务允许对基础数据模型进行扩展，以集成新的信息源，从而便于对智能监控分析器进行定制以迎合企业需求。

智能监控分析技术：智能监控分析器综合了几类视频分析技术。一般而言，每种分析技术都包含了复杂算法，以处理视频/传感器信号，从中提取并结构化地表示信息，以支持智能监控分析器的实时告警和搜索功能。视频分析技术包括：

- 行为分析：这种分析技术用于分析摄像头视野内物体的移动。这个功能是基于对摄像头视野内多个移动物体的检测和跟踪能力，同时对这些物体进行分类，并提取多种物体属性，诸如颜色、形状和大小。在记录所有事件信息的

同时，提取的信息用于产生一系列告警（例如：运动检测、越界、废弃物体）及搜索功能（例如：搜索红色轿车）。

- 车牌识别（LPR）这种分析能力定制用于检测一帧视频图像中是否存在文本，并将视觉字符识别技术应用于提取车牌号码。LPR 需要进行字符集定制（如英语，阿拉伯语），样式，格式以及在不同地区差别很大车辆牌照外观。为了正常运行，LPR 需要车牌图像满足最小像素并且具备适当的照明和视角。
- 人脸检测：这种分析能力被设计成从视频中自动检测人脸图像。人脸检测在视频中创建了索引并标记了什么时间点人脸在视频中出现。系统生成了一个关键帧表示人脸，因此生成了一系列摄像头视野内出现过的所有人脸（接近摄像头）。
- 事件集成：这种能力能够集成来源于其它传感器（诸如感应门传感器、HVAC 传感器、音频等）的事件以及其它 IT 系统（诸如 POS、电话日志）的事件流。一旦综合起来，事件信息能够被交叉关联到基于视频的事件，如行为分析、LPR 和人脸检测。

智能监控告警：智能监控的告警是基于用户设定的条件来实现的，先进的智能监控系统支持以下基本视频告警：

- 运动检测 - 检测特定区域内的移动
- 越界 - 检测从特定方向越过用户所指定边界的行为
- 区域 - 检测特定区域内的特定行为，如进入、离开、开始及结束
- 遗弃物体 - 检测被遗留下来的物体
- 物体移走 - 检测一个物体被移走
- 方向性移动 - 检测物体的移动方向，如果和用户定义的移动方向一致就告警
- 摄像头移动/遮盖 - 检测摄像头状态，如移动或被遮盖
- 摄像头停止移动 - 检测支持摇摄/倾斜/缩放（pan-tilt-zoom，PTZ）的摄像头停止移动

4.3.5.2.3 机房物理安全的工作及应用

智能监控在不同的企业中有着广泛的应用，例如：

市政管理监控

通过部署在商业街道、车站广场等区域的摄像头，实时监控乱设摊点，乱停自行车等违章行为，发现异常及时产生报警通知城管等市政管理部门，协助市政管理。

交通管理监控

通过部署在高架、马路、高速等区域的摄像头，实时监控违章停车、越线等违反交通法规的行为，同时通过结合车牌识别技术在匝道口、出入口提取车辆的车牌信息，提供违章车辆监控和刑侦辅助调查功能。

公众场所监控

在广场、公园、居民小区室外等区域监控老人意外跌倒、儿童失足落水、广告牌意外跌落等异常事件并及时报警通知监控人员。

人流统计

统计医院、商场等通道口进出的人数，在管理和查询后台系统可以查询人流数量，并提供长期的统计信息和趋势分析。

重要部门监控

针对外国领事馆、政府机构、要害部门监控违法闯入等意外事件。

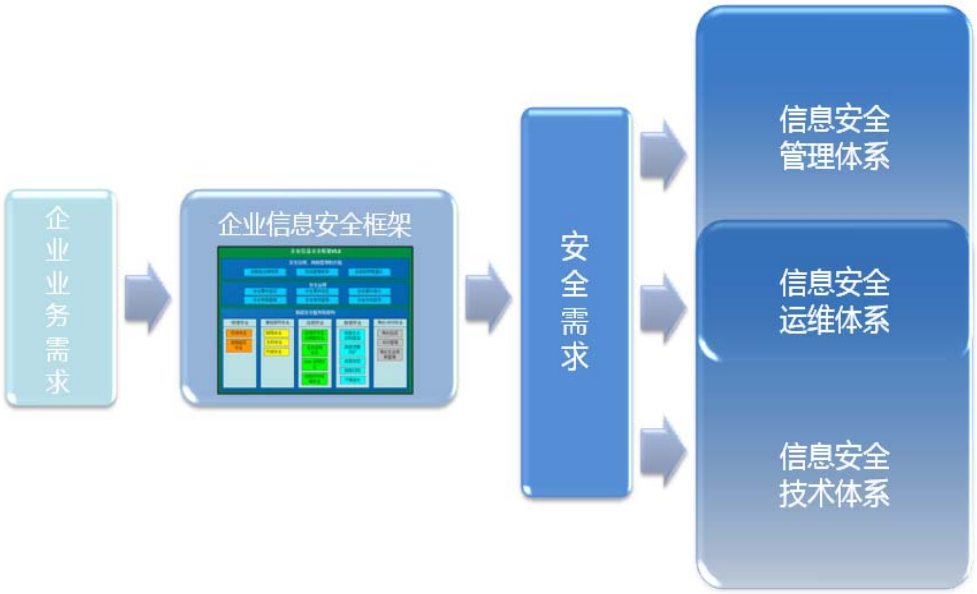
高危设施的监控

全天候监控加油站、危险品储罐、化工厂、石油输送管道等高危设施，实时监控异常情况的发生。

第五章 企业信息安全框架的应用

5.1 企业信息安全体系总体建设方法

企业信息安全框架参考了众多企业所积累的经验，充分吸取行业中的最佳实践。在具体运用中可结合信息安全相关方法论、模型及标准，将所有的内容与要求基于企业的业务需求和的现状转化到信息安全设计与规划的具体项目中分别予以实现并提供了可参照执行的演进思路。从企业需求出发，参照企业信息安全管理框架，通过评估和风险分析等方法，定义企业安全需求，根据企业的安全需求定义企业信息安全建设的内容和方向（如下图所示）。



图示 22：企业信息安全建设思路

5.2 企业信息安全架构

5.2.1 企业安全架构（ESA）定义

企业安全架构根据企业的业务需求定义所需具备的安全能力和功能。企业

安全架构帮助企业相关人员在信息安全建设方面在战略层和操作层作出正确的选择。它帮助企业在业务安全需求和信息安全能力之间建立起联系。

企业安全架构必须是战略层次的定义，必须可以有较长的生命周期以指导信息安全体系的建设；企业安全架构不宜具体到某一特定的解决方案，拓扑或配置。企业安全架构是辅助企业在 IT 建设的整个生命周期，包括选择、采购、设计、实施和运行的各个阶段进行决策的工具。

企业安全架构着眼于在整个企业组织架构中贯彻信息安全架构， 而非针对单独特定应用系统的具体功能性组件和运维节点，致力于建设一套能平衡企业组织架构中复杂业务流程、应用和系统相关风险的战略性架构设计。

企业安全架构设计具有战略意义，它将比设计规范、拓扑图或拓扑配置拥有更长的生命周期，它可发展成特定的方案。如果太过具体，它就会受限于当前的环境；如果太过广泛，它就不能起到提供指引的作用。应谨慎以防止架构变成某个具体实施的蓝图。

企业安全架构有以下作用:

- 企业安全架构通过提供安全功能要求和实施方法来确保企业内实施一致的安全解决方案。
- 根据业务需求事先定义所需的安全技术和解决方案。
- 确保安全解决方案的相互可集成性以及相关的安全管控措施的到位和配合。
- 确保安全组件的可重复利用，保护投资。

5.2.2 企业安全架构的通用性特征

企业安全架构(ESA)具备以下特点：

企业安全架构是一项长远的控制观点,而不是一个战术观点。

目前企业的信息安全建设面临着大量的供应商所提供的各种各样的技术可

以实现各种复杂的安全控制措施。而各种异构的解决方案的重复建设和低效率将成为安全架构需着手解决的问题。总的趋势是为特定的执行情况而部署这些机制作为战术上解决方案。而为了提供一个统一的观点和基于成本的考虑，优秀的企业安全架构的设计是具有战略意义；意味着企业安全架构比规划蓝图,设计规范,拓扑图和配置等具有更长的生命周期. 如果是过于具体,反而将制约当前的情况. 如果是过于空泛或一般,则无法提供决策和指导.在企业整体技术环境下，企业安全架构将为相关鉴别,选择,采集,设计,实施,部署和运维提供决策依据.

企业安全架构的目标是共同的。

一个企业的安全架构应该支持多组织,多部门和多业务单元，描述安全控制及措施的长期技术趋势。它允许多种具体实现取决于现实的时刻,应小心避免安全体系成为特定实施的蓝图。企业安全架构应该为整个组织机构提供一个全面风险管理的指导。

企业安全架构提供了一个统一的共享安全控制的远景。

通过提供共享服务的模型,企业的安全架构着眼于从整体的角度来检查安全控制措施，识别出已有安全控制措施下的潜在风险,提供一个长远的改进计划. 同时,这也是一个安全管理最佳实践的基本组成。

企业安全架构提供了一个灵活的方式来处理当前和未来的威胁。

企业安全架构的所有基础组件的开发和部署只需要做一次。在基础结构已经确定的前提下 ,其它架构组件就可以更容易处理。如果基础架构引入新的举措，是不会引入新的弱点的。如果外部新的弱点被引入,则安全架构需要通过风险评估重新评估。

总而言之，企业安全架构(ESA)应该符合下述相关论述:

一个有效的安全规划是承认随着时间的推移所有的信息资产的价值和风险是不相等或恒定不变的。

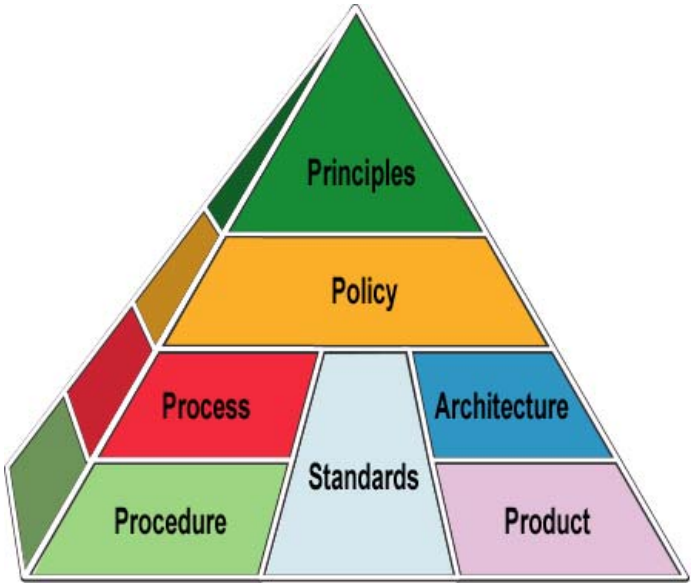
一个有效的安全方案运用最合适的技术来保护相关的资产，并结合执行和质量保障计划把风险减少到可接受的水平。

高品质的安全规划，包括经常性的管理审查和技术评估以确保安全控制措施的有效并提供相关的反馈，使技术和方法适应资产的价值和风险随着时间的变化。

5.2.3 企业安全架构的结构

信息安全金字塔描述了企业安全架构的构成，同信息安全框架（ESF）一样，企业信息安全架构要求对信息安全问题有自上向下的全面的思考。在安全金字塔中的每一层都提供了比它上层更详细的安全概念，并且它的以上各层都是建立在它之上的，直到指定的安全程序和安全产品可在组织里实施。下图描述了信息安全框架的基本内容，从上到下越来越详细。

Security Principle (安全原则)
描述信息安全的业务需求价值。
Security Policy (安全政策)
描述信息安全的目的、方向、远景及责任。
Security Standard (安全标准)
信息安全实施规则，包括技术、方法及其它细节。
Security Process (安全流程)
跨部门实施政策标准的活动、工作及程序。
Security Procedures (安全作业指南)
描述个人在流程上的详细工作。
Security Architecture (安全架构)
描述信息安全与 IT 架构如何结合的细节。
Security Products (安全产品)
信息解决方案所选的产品及工具。



图示 23：信息安全金字塔

企业信息安全架构（ESA）是整个信息安全架构的一部分，并作为一个整体，决定了整个企业 IT 安全的性能和所支持业务的能力。

企业安全架构首先应该确定企业业务方面的安全需求，然后平衡商业驱动因素和可接受的风险。这种业务方面的安全需求的确定来源于内部和外部因素的分析。因此企业安全架构首先应从以保障业务目标而所需具备的安全能力进行识别，还必须符合业务方面的需求，并提供法律和规章方面的遵守。

对于如何通过提供一个全面的方法来构建新一代安全解决方案 、提供基于风险分析的方法来实施安全解决方案，企业信息安全架构以文件的方式提供指导，并用于支持企业安全体系结构和安全解决方案 。

企业安全架构既提供功能图也提供功能部署图。

企业安全架构完整地覆盖了企业信息安全工作的全部内容，并详细说明在今后的活动里可以如何利用这些架构指导工作。企业安全架构概述了每一个关键要素。

设计该企业信息安全架构是用于提供必要的安全概念来保护企业的业务流程和业务信息免受来自内部和外部的威胁 ,通过开发与应用适当的技术来保护最重要的资产 ,结合质量流程把风险降低到可接受的水平。它通过提供架构指南和为安全方案设计提供帮助来实现此目标。

5.2.4 企业安全架构组成

企业安全架构定义了组成上述企业安全架构框架所需的元素，定义了信息安全的能力和功能。企业安全架构不仅包括功能描述，而且包括了实施方法。

企业安全架构提供了安全架构和相关的组件以帮助建立企业风险管理方案。企业安全架构由以下部分组成：

- 安全原则 –描述整个企业业务发展对信息安全的需求和价值
- 安全策略–从业务的角度定义一系列的安全准则，为信息安全管理提供方向和指南。

- 安全模块 – 用于构建逻辑安全模型的核心安全组件（功能性的和基于流程的）。
- 信息资产库 – 帮助理解必须加以保护的资产，以及资产的价值。
- 安全服务 – 描述功能性及流程性的安全控制措施的功能和作用。
- CIA/服务矩阵 – 安全服务的选择指南，以确保在风险管理解决方案种的重复使用。

5.2.4.1 安全战略

安全战略体现了企业高层经理对企业安全架构的需求，体现了业务对安全的要求，反映了信息安全的价值。安全原则对未来安全方面的抉择提供了依据。

通常业界通用的安全原则如下，企业需要根据通用安全原则和本企业的业务需求明确企业自身的安全原则。

- 最少准入特权 (Least Privilege)
- 深入防御 (Defense in Depth)
- 狭窄进入通道 (Choke Point)
- 最弱点原则 (Weakest Link)
- 故障无碍位置 (Fail-Safe Stance)
- 全面参与安全控制 (Universal Participation)
- 防御手段多样化 (Diversity of Defense)
- 防御机制简单化 (Simplicity)
- 安全机制区域划分 (Compartmentalization)
- 内外安全防御能力 (Protect against insider as well as outsider threats)

5.2.4.2 安全策略

安全策略从业务的角度定义一系列的安全准则，为信息安全管理提供方向和指南。安全策略定义信息安全目标并通过定义必须遵守的安全要求来为管理层、用户、应用开发者等相关人员提供指南。

5.2.4.3 安全模块

安全模块是构成企业安全架构的基本安全元素。安全模块分为两种：安全流程模块和安全功能模块。每个模块定义基本的功能或流程。

5.2.4.4 安全流程模块

信息安全的目标是确保业务的连续性，减少安全事故的影响。信息安全管理和信息安全技术同样重要。

信息安全流程模块的定义将参见 ISO27001 标准。根据企业的特点，结合 ISO27001 定义企业的信息安全管理体系和流程。ISO27001 从十一个方面阐述一个企业信息安全管理体系（ISMS）应该具备的管理和控制措施。共包括了 39 个控制目标和 133 个控制措施。

安全政策	
信息安全策略	提供管理信息安全的方针和支持
组织安全	
信息安全基础设施	在组织中管理信息安全
第三方组织方访问的安全	维护组织信息运行设备和第三方组织访问的信息财产的安全。
外包	当信息处理流程的职责被外包到其它组织时，维护信息安全。

资产分类和控制	
资产责任	对组织资产进行专门的保护。
信息分类	确保信息资产得到一个专门的保护级别。
人员安全	
安全在职位责任中的描述	减低人为对设备的失误、行窃、欺骗行为造成的风险。
用户培训	确保用户关注和了解信息安全威胁，训练有素，在日常工作中能执行组织的安全策略。
对安全事故和故障的反应	将安全事故和故障的破坏减到最小，并且检测和研究这些事故。
物理和环境安全	
安全区域	避免对商业许可和信息非授权访问，破坏，干涉。
设备安全	避免损失，破坏或者危及财产以及避免商业活动的中断。
一般控制	避免危及信息和信息运行载体的安全以及避免它们被偷窃。
通讯和操作管理	
操作程序和操作责任	保证对信息的正确和安全的操作。
系统计划和可接受范	将系统错误的风险减到最小。

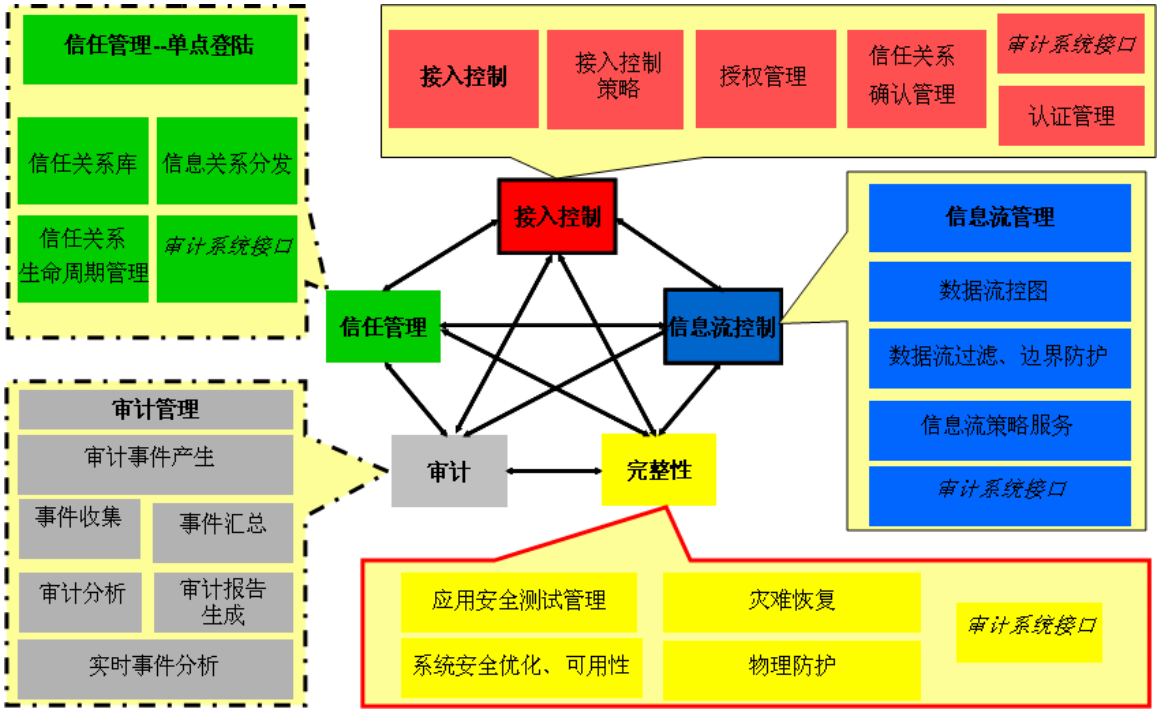
围	
对病毒的防护	保护软件和信息的完整性。
日常管理	保持信息运行和通讯服务的完整性和可用性。
网络管理	确保网络中信息的安全措施和支撑基础设施的保护。
媒体的处理和安全	避免对财产的破坏和商业活动的中断。
信息和软件的交换	避免组织之间相互交换的信息的缺失，更改或误用。
访问控制	
访问控制的商业需求	对信息访问进行控制
用户访问管理	防止非授权接入信息系统。
用户责任	防止非授权访问。
网络接入控制	网络服务的保护。
操作系统接入控制	防止非授权计算机访问。
应用接入控制	防止对信息系统中的信息的非授权访问。
检测系统接入和使用	检测非授权活动。
移动计算和远程办公	当使用移动计算和远程办公设备时候确保信息安全。
系统开发和维护	
系统的安全需求	确保信息系统中内建了安全措施。
应用系统的安全	防止应用系统中的用户数据的丢失，更改和误用。
密码控制	保护信息的机密性，真实性或完整性。

系统文件的安全	确保 IT 项目和支持行动是以一个安全的方式管理的。
开发和支持过程的安全	维护应用系统软件和信息的安全。
信息安全事件管理	
报告信息安全事件和弱点	确保与信息系统有关的安全事件和弱点的沟通能够及时采取纠正措施。
信息安全事故的管理和改进	确保使用持续有效的方法管理信息安全事故。
业务连续性管理	
业务连续性管理的方面	减低业务活动的中断并在主要的错误或灾难的影响方面保护至关重要业务流程。
符合性	
符合法律要求	避免违反任何刑法和民法，避免违反法定的、统制的、契约的条例，和任何安全需求。
安全策略和技术实现的检查	确保系统符合组织安全策略和标准。
系统审计的考虑	对于系统审计流程，应该最大化其效用，最小化其冲突。

具体安全流程模块的解决方案在“安全管理体系建设方案”章节进行详细介绍。

5.2.4.5 安全功能模块

所有的安全功能模块按功能区分，可以分为接入控制、信任管理、信息流控制、审计和完整性 5 个子系统，如下图所示：



图示 24：安全功能模块功能区

五个子系统的每个子系统相关的组件在下面列出。这些组件来自基础功能构建模块，并在每个独立的安全子架构使用。

在设计企业安全架构时，需要根据企业的环境来定义 5 个子系统的具体功能。这些安全功能模块共同工作，构成了企业的信息安全系统。

信息流控制

信息流控制子系统负责在一个计算解决方案中对信息流把关，控制信息的可见性，并且保证信息的完整性。

逻辑组件	描述
信息流管理器	流管理器代表信息流控制子系统的中心，负责协调其它流控制子系统的组件。
信息流翻译器	流翻译器将对流内容进行修改并将其编码，特别在贯穿以下路线时： a) 安全区域边界 b) 网络网络边界 c) 传输或或应用级别网关 流翻译器的例子有：防病毒内容过滤，无线网络连接有线网络的网关，路由器等。
安全交易	安全交易组件将进行通讯加密。 应该存在相应的支持措施，这些措施能加强企业相关的安全策略的执行，使得能够在信息传输和接收时不被非授权的泄漏（保密性）。将根据企业安全策略对完整性的要求来确保传输对象的完整性。安全措施将确保信息在传输和接收时不被更改，删除，插入和回放。 当使用坚固的加密方法后： • 该组件可能对用户数据的接收进行确认，并确认其没有被更改，删除，插入和回放。 • 通讯管道在逻辑上与其它(非安全的)通讯管道可以是分开的，并能确认传输终端的身份。 • 该组件可以支持安全状态信息和配置信息的变更检测功能，在已定义变更衡量标准[例如，消息验证编码，哈希算法]中，这对于

逻辑组件	描述
	安全子系统与远程受信节点通讯时能够保持一个安全状态是至关重要的。 • 确认将会被执行，以使完整性安全性状态信息和配置信息得到保证(对于保持安全状态数据至关重要)，当完整性无法得到确认时，会自动重传。 一个弱的加密方法可能不会提供以上全部功能。
地址关联	地址关联将会加强信息流控制规则，信息流控制规则可能包括以下主体类型和信息安全属性： d) 源主体的网络层次地址或应用层次地址； e) 目的主体的网络层次地址或应用层次地址； f) 传输层协议； g) 信息流到达和离开的信息流控制接口 它可以根据关联规则，通过对信息流地址(网络级别标识)的分配和重分配，来控制信息流。 例如代理服务 proxy，网络地址翻译 NAT 和 DNS。
策略服务	策略服务管理信息流控制策略规则。策略可以由授权用户管理或由外部导入。 策略服务为其它子系统提供信息流控制策略信息和服务。 例如，当认证信息和安全属性信息从安全子系统传输到一个远程被

逻辑组件	描述
	信任节点过程中，应提供适当的保护以防止信息在传输过程中的泄漏。 可导入策略的例子包括病毒和入侵攻击的特征库。
流过滤器	流过滤器防止没有明确允许的信息流的传播。它根据许多因素过滤信息流： a) 流规则库 b) 信息流的自然特征(如果可以确定的话) c) 相关协议暗含的操作影响 流过滤器可以部署在几个层次： a) 接口层次 b) 网络层次 c) 源/目的层次 d) 应用 e) 内容 f) 设备驱动 g) 消息 h) 队列 以下是主要的流过滤器例子： 流过滤器 - 边界：在一个解决方案中，作为包，信息等每个片段穿过物理和逻辑节点的守关者。

逻辑组件	描述
	流过滤器 - 群：启用并管理群。群存在于一个区域内，或在多个区域之中，可以根据附件，一般的媒体接入地址/协议，一般的网络地址/协议，或者一般的应用地址/协议来识别和过滤。 流过滤器 - 隐私：将所有隐私数据类型映射到隐私策略，并在提供数据访问之前由隐私策略服务进行判断是否允许访问。它提供以下核心功能： • 对于隐私数据进行把关操作。 • 将策略映射到隐私数据。 • 将许可映射到隐私数据 • 根据隐私策略保证隐私数据的合法地运用于商业领域。 流过滤器使用隐私策略和许可作为它的流规则库，并在应用/数据层控制隐私数据的访问。
证书请求者	该组件代表流控制子系统和证书子系统之间的接口，该接口用于获得证书进行加密和解密。
隐私数据转换器	隐私数据转换器将对隐私数据进行特定的隐私相关的操作，而不是标准的创建，读取，更新，删除操作。隐私相关的操作可能包括： 非个人化隐私数据：将某些字段删除使该数据无法定位到具体的个人。例如，提取人员的名字，但保持他的系统身份和工作职位。 个人化隐私数据：向数据集增加某些字段使其可以定位到个人。 聚合隐私数据：为商业用途整合隐私数据，以确保数据是无法定位

逻辑组件	描述
	到个人的。例如，提供一个部门的工资数据的统计。 匿名隐私数据：删除可以追溯到个人的所有相关数据。例如，删除除了工作职位的所有的属性。

信息流控制子系统可能包括以下功能：

- 流许可或禁止
- 流监控和控制
- 传输服务和区域：在域之间开启的或信任的隧道，开启的信任路径，媒体转换，人工传输，区域之间的导入或导出
- 内容转换和过滤：阻止加密流量或内容

信任管理

信任管理子系统负责生成，分发并管理信任数据对象，在一个计算解决方案中，信任数据对象负责在多个平台、流程和安全子系统之间传送身份和许可。信任管理子系统使用的信任对象可以存在于做出信任决定所需的任何安全的形式，格式或位置中。

逻辑组件	描述
证书管理器	该组件将提供身份生命周期管理，并确保专有的证书的发行并使它与定义的策略保持一致。 除此之外，工作流也用于一个或多个证书的审批。 该组件将提供自助服务的证书管理功能。例如，允许客户更改密码的功能。

逻辑组件	描述
	自助服务管理应该符合隐私相关的策略，例如，允许用户采用假名。
身份存储	身份存储将存储和维护属于个人身份的安全属性，这些安全属性包括用于身份验证授权的密码（秘密信息）。 当一个帐户将过期时，身份存储组件将可以： a) 根据策略允许授权的管理员禁止/重新授予一个身份帐户的证书。 b) 当一个密码信息过期时，在验证授权之前要求身份拥有者建立一个新的密码信息。 身份存储将提供授权身份，授权身份拥有检验身份存储子系统数据完整性的功能。该组件提供授权身份，授权身份拥有检验存储安全属性完整性的功能。 身份存储将也有存储历史身份属性的功能，例如，当一个身份不再可用时，用于访问被保护历史数据和资源的用户证书和 email 加密密钥。 身份存储将也提供假名的匹配，像隐私需求说明那样。
证书状态管理器	证书状态管理器将维护子系统中所有证书的正确状态。无论基于计划内的（例如，正常合法时期，计划满期，等）和计划外的（例如，已分离关系，妥协，等）。为了接收状态的通知，证书状态管理器与其它子系统连接。
确认管理	确认管理器通过接口和协议，负责为对经授权请求者提供证书的现

逻辑组件	描述
器	时状态服务。 该组件是进入证书子系统的公共接口。
分发管理器	分发管理器将把用户的安全属性和代表用户身份的 ID 标识[证书管理器]关联起来。 该组件将提供多种平台，网络和应用上分布式安全子系统的证书的同步。 分发管理器将根据目标系统所期望的格式提供数据格式转换。该组件支持传输，编址和目录存取[例如 LDAP]机制，保证证书和密钥信息[证书[X.509]/PKI]的分发。 该组件可能将相异的身份来源和证书相关信息聚合到身份仓库。
证书生产器	该组件将根据标准和策略中格式和内容的要求生成各种形式的身份标识。 该组件可能使用如伪随机数字生成器去产生密钥信息，例如密码或挑战握手种子数。 生成的密钥信息可能包括证书，公钥和密钥，密码和生物学证书。 证书生成器负责身份的创建和生命周期管理。 证书生成器也可能提供匿名和生成匿名证书支持。
证书策略服务	证书策略服务将提供了一定的策略，以确保密钥信息满足安全需求标准和策略。他包括了密码格式的标准，例如密码长度的要求和要

逻辑组件	描述
	求至少包括数字和非数字。 该组件确保安全策略中有关密钥的策略的执行和使用。例如，确保用户在首次使用用户/密码时，更改密码。 证书策略服务确保身份的重用策略的执行，以确保历史信息根据法律法规和策略的要求进行保留。 证书策略服务中应该同样有支持隐私需求的策略，例如确保个人不能直接由假名或匿名登陆的证书所识别。
证书别名管理器	证书别名管理器将在一个证书系统中分配别名身份。在分布式目标访问控制系统中，它负责管理并维护身份的主证书和任何关联别名（第二）证书的关系。 证书别名管理器也应该支持在异构系统中其相关访问的一致性和匿名管理。
隐私交互管理器	隐私交互管理器负责协调个体与其相关个人可识别信息（personally identifiable information,PII）的关系。组织或个人都有可能引发这种交互。 内部交互的例子： • 个人请求访问其个人信息 • 个人授予/撤销别人使用其个人信息的许可 • 个人决定参加或退出接收市场宣传活动信息 • 个人发出本人信息已经更改的通知

逻辑组件	描述
	外部交互的例子： • 由于一个特定理由请求别人同意获取/访问其个人信息 • 通知个人有关其个人信息的使用

信任管理子系统可能包括以下功能：

- 单用户与多用户机制，使用加密手段或不使用加密手段
- 密钥信息的产生与确认
- 用于保护安全流程或商业流程的身份和证书
- 用于保护资产的身份和证书：完整性或不可见性
- 用于访问控制的身份和证书：由于用户 - 主题绑定的目的而进行身份标识，验证和访问控制
- 在法律所要求绑定的交易中用于识别的证书
- 身份标识和验证的时间和时限
- 证书的生命周期
- 由于隐私而使用的匿名和假名机制

访问控制

访问控制子系统在一个 IT 解决方案中的目的是控制访问，通过使用证书和属性的安全机制一起，经过身份标识，验证，授权增强安全策略。访问控制子系统使用的证书与属性在信任管理子系统中进行维护。

逻辑组件	描述
访问控制管理器	访问控制管理器代表访问子系统的控制中心。该组件是访问控制子系统的公共接口，它负责其它所有的访问控制组件的协调。

逻辑组件	描述
	访问控制管理器将与隐私策略服务一起协调关于隐私策略的请求。
身份标识管理器	该组件将根据以下规则检查用户提交的身份证书的正确性： a) 检查证书在结构和内容上是有效的 b) 检查现有密码是有效的，或提供密码的拥有证明 c) 检查证书没有被废除
状态/会话管理器	状态/会话管理器将负责源组件与目标组件、目标组件的控制的转换的绑定初始化。 状态/会话管理器将通过一系列机制保持并加强源组件与目标组件之间的逻辑连接的状态。这些机制包括但不受限于：状态表，会话身份，代理连接，cookies 等。 状态/会话管理器将根据安全策略规定的时候间隔对一个交互式的会话上锁。使用的机制可能包括： a) 清除或覆盖显示设备，令当前内容不可读取 b) 关闭用户数据访问/显示设备的任何活动，而不是解锁该会话。在解锁该会话时，状态管理器将要求用户验证。 该组件将通过安全事务组件为安全相关功能初始化通讯过程。
验证管理器	该组件将判断提供的证书是否正确地标识该身份。这包括确认该帐号是否被禁用。 验证管理器将也支持隐私相关功能，包括假名验证和匿名验证。

逻辑组件	描述
访问控制策略服务	访问控制策略服务允许授权用户更改访问控制策略规则库。策略可能包括： • 授权策略如控制可供使用的时间。 • 登陆策略如处理角色冲突的策略（职责分离）。 • 授权相关策略（在安全策略中）如同一身份的会话最大并发数的限制。 • 隐私策略如限制访问个人可识别信息。 该组件将可对每个访问请求进行隐私策略的评估。
授权管理器	该组件将确认经验证的用户符合特定的访问控制策略的要求。 授权管理器应该支持粗粒度的和细粒度的授权概念。
用户/主题绑定	该组件允许请求与流程或服务的关联。 该组件典型地使用于当一个使用它自身访问控制机制的环境被需要去相信由其它验证系统认证的身份。已经通过验证，在其它环境中提供的身份标识和验证信息可以在作为凭证进行授权。用户/主题绑定可以采用 Kerberos 和一个 Java 信任关联解释器（TAI）。 为了支持隐私需要，用户也可能需要通过绑定隐藏其标识。
角色管理器	该组件将管理组织中的角色。访问权限将与角色关联。 角色管理器将提供创建，删除和修改角色并将角色与访问权限关联。

逻辑组件	描述
注册管理器	该组件将用户与角色关联，管理用户注册和角色更改，管理审批及相关工作流。该组件将维持用户标识和角色的关联。 用户注册将直接通过界面进行或由一个外部应用（例如 HR 系统）触发。 用户接口应该包括用户自助服务功能，以允许用户申请角色分配。
证书检验器	该组件代表访问控制子系统和信任管理子系统之间的接口，该接口用于标识，认证和授权过程中审核证书。
隐私策略服务	隐私策略服务管理所有组织的隐私策略。它是隐私相关应用程序的隐私策略信息的来源，同时，也是向与组织交互的个体展现隐私策略信息的来源。 该组件也管理策略与功能的对应关系。在执行一个操作前，它应该预先评价了应该询问哪个策略。 个人隐私信息的显示和解释将以该组件为来源。一种策略定义的格式是 W3 P3P XML 隐私策略格式，它也可以在 web 浏览器中解释。
隐私资源管理器	隐私资源管理器协调所有隐私数据的请求和检索，同时协助遵守隐私策略。

访问控制子系统可能包括以下功能：

- 访问控制功能
- 访问控制监控和执行

- 身份标识和验证机制，包括密钥信息的验证，加密（包括加密和签名），和单用户、多用户的验证机制
- 授权机制，包括属性、权限、许可
- 访问控制机制，包括基于主题和对象的属性访问控制和用户主题绑定

日志和监控

日志和监控子系统在计算环境中负责获取，分析，报告，存档并找回事件记录和必需的证据。

分析和报告可以是实时分析，如入侵检测组件，或事后分析，如调查取证分析。

逻辑组件	描述
事件管理器	事件管理器代表日志&监测子系统的控制中心，负责事件处理的协调。 该组件将提供工作流功能，来管理和上报安全事件（如安全报警）。
事件收集器	事件收集器应该记录每个审计相关的信息，至少包括以下信息： a) 事件日期和时间（通过可信赖时间组件） b) 事件的类型 c) 主题和用户身份（通过会话管理器组件） d) 事件的结果（成功或失败） e) 引起该事件的系统进程 安全策略中将定义所需记录和审计的事件的详细信息。 事件收集器将根据隐私策略接收隐私事件。

逻辑组件	描述
事件生成器	事件生成器是所有日志事件的来源。系统平台，网络和应用节点将可能在系统中生成日志事件。事件生成器生成符合审计和安全策略要求的事件。该组件可通过嵌入到平台的方式或通过传感器代理的方式实现。 事件生成器应该支持： a) 一个应用程序接口（API），该接口允许应用程序向安全审计记录添加数据。 b) 允许只有明确授权的用户能选择生成哪些事件。 c) 有能力检验安全状态和对于安全状态有至关重要作用的配置信息的完整性。
事件存储	事件存储组件将存储事件到日志中，日志放置到持久存储器中。 事件存储组件禁止对事件日志进行读访问，除非该身份得到明确的读访问授权。保护事件日志不被非授权地删除，并能防止和检测对其的修改。 当审计日志超出事先设定的阀值，应设置报警功能，避免审计事件的丢失。
事件相关器	事件相关器将把环境中多个平台的安全事件组织到一个逻辑组中。根据事件的类型整合和确定安全事件。安全事件管理器应该实时处理事件。 该分析应该寻找对安全有重要影响的事件或模式，并通知事件关联

逻辑组件	描述
	组件。该分析通过事先由安全管理员定义的规则来检测安全问题。也可以通过定义哪些是允许的正常行为来发现和检测非正常行为。关联分析应该提供可定制被审计对象的能力，因此它将可选择或排除某些可被审计的安全事件，可根据以下属性来过滤被审计的安全事件： a) 对象标识 b) 用户标识 c) 主题标识 d) 主机标识 e) 基于成功或失败的事件类型
事件分析器	事件分析器组件将提供执行过滤和对事件日志排序的功能，过滤和排序基于以下属性： a) 假定的主题/用户身份/地址 b) 日期范围 c) 时间范围 d) 地址范围 事件分析器将会分析隐私审计轨迹以确保符合隐私策略，并分析违背隐私的操作。
事件报告器	事件报告组件将以一个符合用户习惯的形式产生事件日志报告。该报告支持必要的服务管理和报告需求。

逻辑组件	描述
	因可能需要满足立法机关的需求，该事件报告也将用于隐私符合性的报告。
事件存档器	该组件管理关于事件和环境信息的长期存储。

日志和监测子系统可能包括以下功能：

- 安全审计数据收集，包括获取相应的数据，安全传送审计数据，和时间同步。
- 安全审计数据的分析，包括通过简单试探法或复杂试探法去评估，检测，违例分析和攻击分析。
- 超过阀值时的警报，警告条件和关键事件。

完整性

在计算机解决方案中，完整性子系统负责维护至关重要的组件和流程的操作的正确性和可靠性。

许多完整性子系统组件将不会放在普通/共享节点上（安全架构）。这些组件（性能/可用性管理器，错误管理器，连续性管理器和恢复管理器）会存在于独立的 IT 解决方案中。

逻辑组件	描述
资源管理器	资源管理器将管理资源的上限，如以下资源 a) 所有受支持的操作系统控制的资源 b) 多用户或多进程资源如内存,磁盘空间，和交互处理器

逻辑组件	描述
	c) 单个用户，定义的用户组或主题可同时使用的通讯路径。
完整性管理器	完整性管理器负责保证端对端解决方案和所有的功能管理器符合它们本身的职责。 一个例子是确保访问控制器执行策略规定的验证和授权（如安全策略中规定的）。 该组件应该可与事件发生器组件通讯，当检测到偏差时通过警报或告警器发送通知。
恢复管理器	恢复管理器将负责对操作失败和操作中断及时修复，这些操作必须从一个以前的状态点重新开始。恢复组件支持的操作有：备份，存档和存储。
时间管理器	时间管理器组件负责维持分布式系统之间的时间同步。例如，a)审计记录的时间应该确保系统中所有平台，网络，应用节点产生的审计记录时间相同。b)数字证书集合中的有效期应该始终由所有证书有效性检查器和有效性检查组件解释。
连续性管理器	连续性管理器负责不会因为一些操作出现状况而影响操作的可靠性，保证工作的持续性。
时间源	时间源组件代表解决方案中所有系统所遵从的时钟。这可能是非正式的，如根据设置系统的技术人员的手表设置系统时钟，也可以是正式的，如确定可信赖的时间源。一个可信时间源将会由一

逻辑组件	描述
	个与外部世界同步的可信赖的，外部时间源提供。系统所有节点的时间会同步，并提供用户业务事件的单一视图。这可能是一个 GPS 卫星事件源或一个无线电时间源。这使得每个审计记录的事件的日期和时间与系统中每个其它审计事件是同步的。
测试管理器	一个将会管理测试组件和测试流程的组件。从一个技术观点看来，测试管理器可能是一个弱点扫描器，一个执行预定的病毒扫描的服务，等。
错误管理器	一个管理识别并回应组件和流程错误的组件。例如，一个确认安全组件在正确工作的应用。注意该组件可能在某种程度上比单单确保可用性的组件（性能&可用性管理器负责的）使用得更多。
性能&可用性管理器	管理组件和流程的性能和可用性的组件。 如管理网络子隧道以确保至关重要的通讯的可用性。
物理完整性保护	提供信息和组件的物理保护的组件。

完整性子系统可能包括以下功能：

- 资源完整性和可靠性。
- 数据对象的物理保护，如密钥，物理组件，如电缆，硬件等。
- 包括容错，错误修复，自检测等的持续操作措施。
- 用于时间度量和时间戳的精确时间源。
- 根据资源分配或配额来安排服务的优先级。

- 使用安全区域划分来进行功能隔离。

5.2.4.6 信息资产库

信息资产库帮助企业理解哪些信息资产对于企业是最关键的，这些资产现有的保护措施如何，还存在哪些安全风险。

信息资产库关注每个资产的保密性，完整性和可用性。从而了解每个资产的安全需求，以提供合适的风险管控措施。

5.2.4.7 安全服务

安全服务定义了企业可以提供的安全功能和流程，它是由不同的安全模块组成的。

5.2.4.8 CIA/服务矩阵

CIA/服务矩阵将安全服务映射到资产的三个属性：保密性，完整性，可用性。此服务矩阵帮助理解和选择相关的安全控制。

5.3 企业信息安全管理体系的建设

5.3.1 安全管理体系总体框架

信息安全管理体系是信息安全保障体系的一个重要组成部分。信息安全管理体系框架是从企业管理的层面出发，按照多层防护的思想，为实现信息安全战略而搭建的。

信息安全管理体系由几下几部分组成：

安全政策，标准——管理规定

信息安全政策与标准是信息安全管理、运作、技术体系标准化、制度化后

形成的一整套对信息安全的管理规定，是安全意识培养的内容来源，是组织管理控制和审计的依据，是技术方案必须遵从的基础要求。

安全意识培养——宣传教育

员工在信息安全方面的自我约束、自我控制，是信息安全管理体系的一个重要层次。安全意识培养是信息安全管理控制的基础，实际工作中大部分的信息安全控制需要依靠员工的主观能动性。

安全组织——管理控制

通过完善的组织架构，明确不同安全组织、不同安全角色的定位和职责以及相互关系，对信息安全风险进行控制管理。这里包含了“管理”和“监控”两方面的含义，特别是对专职的信息安全管理部门而言，“监控”是极其重要的职责。

管理控制的落实需要通过标准、安全意识培养和审计工作进行保障和监督，同时它又是信息安全标准、安全意识培养和审计工作开展的重要对象。

审计——监督

审计监督是企业内部风险控制的重要组成部分。内部审计是企业内部控制的一种自我监督机制。信息安全审计一般是在信息安全管理控制的基础上，由企业内部相对独立的专职部门对信息安全管理控制的效果进行监督。

风险评估——发现问题

信息安全风险评估的目标是了解支撑企业关键业务运作的信息系统的安全状况，评估核心信息资产所面临的风险，发现信息安全实践中的薄弱环节和改进机会，明确信息系统的安全需求，提出信息安全控制措施改进方案。

5.3.1.1 信息安全政策和标准体系框架

企业的信息并不是存在于真空中的，而是和复杂的企业在法律和财务方面的要求相关。企业的每一位员工都应当了解自身所担负的信息系统安全职责。对于任何能够正常运作的企业来说，必须制定能够满足企业要求的相应的安全政策和标准并付诸于实施来防范一切可能出现的安全隐患。

安全政策和标准体系的建设应充分考虑以下几个方面的因素：

- 对公司环境的理解
- 参考国际标准，如：ISO 27001，安全架构 (ISO 7984-2)
- 遵守中国的安全法律法规，如：计算机系统安全保护条例

5.3.1.2 信息安全意识培养

信息安全意识培养是信息安全工作中非常重要的一个环节，对信息安全工作来说，信息安全意识教育主要是要发挥员工在信息安全方面的主观能动性，通过自律的方式来实现安全保障。在实际工作中，大部分的信息安全风险需要在这一层面得以控制。

信息安全意识培养工作主要是针对人的工作，而其范围非常广泛。由于几乎所有的员工都可以直接或间接的接触信息系统，或信息系统中的信息，因此根据全员参与原则，信息安全意识培养工作涉及企业内部的所有员工。

信息安全意识培养工作是通过宣传教育来达到以下三个目标的：

- 提升员工信息安全意识
- 保证员工了解自己的信息安全职责
- 保证员工掌握必要的信息安全方面的专业技能和理论

人的因素一直是信息安全系统中相当薄弱的一个环节，由于人为因素而造成的信息安全方面的损失要远高于其他非人为因素的损失。而通常情况下，在人

为因素造成的损失中由于企业内部人员所造成的损害又占了大部分。内部员工造成的损失从原因来看主要有：过失和失误、欺诈犯罪以及不满员工的破坏行为。信息安全意识培养和专业技能培训主要是为了降低过失和失误这方面人为因素所造成的损失。同时，通过向员工宣传和教育他们承担的责任以及违规处罚的措施，也可以有效地抑制内部员工欺诈和破坏等情况的出现。

信息安全意识培养工作的开展主要依赖三种手段：信息安全宣传、信息安全培训和信息安全教育。

信息安全宣传的目的主要是让每个员工认识到信息安全方面的关注问题，了解信息安全的重要性，明确信息安全工作的目标和宗旨，提升员工的信息安全意识。一般信息安全宣传至少应包含以下一些基本内容：

- 安全事件对企业内用户和企业的影响；
- 信息安全战略目标和原则的意义；
- 企业信息安全方面政策标准的解释说明及其背后的控制目的；
- 企业的信息安全计划和目标；
- 信息的分类分级基本情况；
- 各人承担的信息安全方面职责以及违反相关规定的行为后果；

信息安全宣传的对象是全体员工，因此在选择实施方式和渠道时一般采用那些能够在短时间内迅速接触到广大员工的方法，同时经过一定的包装使之更易于为人所接受。通常采用的方法有：

- 安全意识宣传的录像和广播
- 海报和传单
- 内部刊物或企业网站
- 用户登陆时出现的提示和宣传信息
- 各种形式的讲座和讨论
- 有大批员工参与的各种会议

信息安全培训的目的主要是为了传授一些必需的安全技能和能力，使学习者能完成某一方面的工作。相对宣传，培训的形式更为正规，同时相比宣传的一次性的活动，培训更注重经过一段时间更具体地将某个特定角色或岗位所需要的知识和技能教给相关人员。因此培训的内容更加有针对性，企业中和信息系统相关的不同角色其培训的内容也各不相同。

信息安全教育是指将许多不同特性的安全技能和能力整合成一个知识体系，通过加入各种学科的概念、基本原理等内容，为企业培养信息安全方面有远见的专家和专业人员。在安全教育中不再像培训一样只关注实际工作中的技能，而是将其上升到了理论体系和原理的高度，因此都是由专门的社会组织提供安全方面的专业课程和教育。一般在完成一项安全课程教育后会获得相关的资格和证书。

三种手段之间的区别可以由从下面这张表中明确看出：

信息安全意识培养			
	宣传	培训	教育
特征	了解“什么”	了解“如何做”	了解“为什么”
内容级别	信息	知识	原理
学习目的	识别和记忆	掌握技能	理解

对于员工安全意识的培养应当形成一个连续不断的体系，从安全宣传开始，逐步发展到安全培训，然后发展出安全教育。首先组织中所有的员工都有安全意识培养方面的需求，通过宣传来提升安全意识；然后通过宣传和培训手段让所有的人都了解自己的信息安全职责，其中培训手段主要是针对那些职责和角色对于信息安全威胁、漏洞和防护措施有特殊职责要求的人员；最后，通过培训和教育来培养那些期望成为专业信息安全人员的员工。

5.3.1.3 信息安全组织

从安全的重要性来看，企业一定要有一个常设的安全组织，该组织配备一些专职的安全人员，特别是 IT 的安全人员、审计人员。通过完善组织架构，明确不同安全组织、不同安全角色的定位和职责以及相互关系，对信息安全风险进行控制管理。

信息安全组织是指所有接触信息资产的组织，即不仅仅包括内部的各相关部门，还要包括接触企业的第三方组织，包括供应商、业务伙伴、外包商、甚至客户等。第三方组织的信息安全也是信息安全组织管理中的一个重要课题。

信息安全组织架构是参与信息安全工作的各部门进行分工协作开展工作的结构，是根据其在信息安全工作中扮演的不同角色进行优化组合的结果，反映了各类组织在信息安全工作中的不同定位和相互协作关系。信息安全组织架构设计并非对企业的组织架构进行重组，而是在原有组织架构的基础上针对信息安全的需求进行的提炼和完善。信息安全组织架构主要包括参与信息安全决策、管理、执行和监督工作的部门。

信息安全组织架构是企业内开展信息安全工作的基础。在企业的日常管理过程中，存在着多项信息安全管理事宜，需要对其中的重要事件进行决策，从而为信息安全管理提供导向与支持；对于所制定的信息安全管理方针需要进行有效的贯彻和落实；另外，对信息安全管理方针贯彻落实的情况还需要进行监督。以上各种情况都需要一个完善有效的信息安全组织架构来支撑。另外在未来信息安全保障体系建立的过程中，各种信息安全项目的开展将成为信息安全工作的一项重要内容，这也需要有相应的组织予以支持。

5.3.1.4 信息安全审计监督

信息安全审计是指企业为验证所有信息安全政策、标准、程序及其他相关规章制度的正确实施和检查信息系统符合安全实施标准的情况，以及检验安全运行效果，信息安全控制措施是否得当所进行的系统的、独立的检查和评价，是企

业信息安全保障体系的一种自我保证手段。

信息安全审计需要保证相对的独立性，因此需要由独立的内部审计部门来负责。

信息安全审计的具体工作主要是评价信息安全工作的开展情况，某些情况下也会使用信息安全监控工具。

企业开展信息安全审计工作的目的是：避免违背有关法律法规或合同约定事宜及其他安全要求的规定，确保企业信息安全管理体系符合安全方针和标准要求，作为自我保障和改进机制的一部分，在保证信息安全管理体系持续有效运作的同时，不断的改进和完善。在信息安全管理体系中，信息安全审计在保障管理控制措施有效执行的同时还需要验证这些措施是否能有效实现信息安全工作目标。

5.3.1.4.1 信息安全审计监督体系

根据信息安全审计的定义，信息安全工作开展的依据是内部制定的信息安全政策与标准。其工作的主要内容包括以下几个方面：

1、信息安全政策与标准的符合性

检验企业内各级单位是否按照上级信息管理部门的要求制定了相应的文件化的规章制度、操作守则及其他相关措施。

2、信息安全政策与标准的执行情况

检验企业内各级单位的员工在工作中遵照既定规章制度执行的情况，同时检验被审计单位在以往信息安全审计结束后所明确的纠改措施是否落实。

3、检验信息安全控制措施的效果

对信息安全各项控制措施的运行效果进行检查、分析，以确定这些控制措

施是否能够有效保障信息安全工作目标的实现。该工作主要包括：

- 对被审计期段内的信息安全事件进行审查、分析。这项工作需要信息安全执行机构和管理机构提供完整、详细的信息安全事件发生、处理以及纠改措施制定和执行情况的记录，并提供必要的工具帮助对这些记录进行整理、分析。
- 信息安全控制措施的有效性验证，控制措施有效性验证的内容包括：

  - 流程验证--审计人员可以根据信息安全执行机构或管理机构提供的信息安全控制流程进行分析，以确定流程是否能够有效的控制风险。这其中也包括验证审计人员获得的信息的不可否认性和完整性。

  - 系统结构验证--信息安全审计人员可以根据安全需求对某些系统架构的安全性进行评估，例如对监控系统进行评估，以确定监控系统获得数据的不可否认性和完整性。

  - 技术验证--信息安全审计人员可以借助技术手段以日志分析、穿透性测试、漏洞扫描等方式对信息系统的安全性进行验证。

5.3.1.4.2 信息安全审计工作开展指导

信息安全审计工作的开展中需要考虑到以下几项关键因素：

1、采取企业政策标准与国内、国际信息安全标准相结合的策略

一般审计主要以企业的政策标准为基础，但由于目前企业的信息安全政策与标准仍在完善中，有一些领域暂时还没有完整的政策或标准，因此需要借鉴一些具有公信力的国内、国际标准。可以参照相关的国内、国际标准审计，包括在信息和相关技术审计方面的 COBIT ，以及在信息安全方面权威的标准 ISO27001 等，从控制点的角度出发来对信息安全进行审计，从而保证对信息安全方面的控制符合国内、国际的标准。

2、从事信息安全审计的人员需要相应的专业技能培训

由于信息安全方面审计的特殊性，对于参与审计的相关人员需要组织必要的培训，如果有可能需要尽量选用一些获得认证资格的审计人员。

3、可以有效的利用第三方进行信息安全审计，但同时必须进行严格的控制

第三方审计组织，尤其是一些国际上提供相关服务的机构，由于其拥有先进的审计方法，同时从企业外部公正独立的角度开展工作，因此对于企业的信息安全审计是一种有效的补充手段。但是，由于信息安全审计工作中将接触大量企业的信息安全敏感资料，因此对于将信息安全审计项目外包给第三方的情况必须有严格的控制措施。

5.3.1.4.3 信息安全风险评估

信息安全风险评估的目标是了解支撑企业关键业务运作的信息系统的安全状况，评估核心信息资产所面临的风险，发现信息安全实践中的薄弱环节和改进机会，明确信息系统的安全需求，提出信息安全控制措施改进方案。

信息系统安全风险评估的主要工作内容有：

- 识别评估范围内的信息资产，用合适的价值尺度对其价值进行估计，描述信息资产对业务的关键程度和敏感程度，初步确定信息资产应满足的安全保护水平目标；
- 采用现场检查，与相关人员面谈，问卷调查，文档收集和查阅，技术测试等方法，收集和评估该信息系统在安全政策标准，物理安全，人员安全，运作安全，系统安全，网络安全等方面的控制措施和薄弱点；
- 根据收集的资料，进行威胁分析、薄弱点分析、业务影响分析、风险分析，确定信息资产在机密性、完整性、可用性、可审计性、不可否认性方面存在的风险；
- 根据初步的风险分析结果，选择可行的安全控制措施，评估和接受残余风险；
- 编写和提交最终的风险评估报告。

风险评估规范应该明确定义风险评估的操作步骤，包括每一个步骤的工作内容，使用的方法、技术和工具，以便系统地从威胁、薄弱点、影响等方面来识别和评估风险。

信息资产安全管理规范涉及信息资产在获取、使用、维护、管理、处置的整个生命周期中采用合适的控制手段，确保信息资产的安全。其内容应包括：信息资产的范围和责任人；信息资产清册的编制和维护；信息资产的分类分级；不同保护级别的信息在获取、复制、存储、传送和销毁等活动时，应采取的控制和保护措施，以满足各级信息资产的保护要求。

信息安全风险评估的主要收益包括：

- 明确核心信息资产面临的主要风险，信息安全风险已经成为企业面临的一个重要风险。通过对支撑关键业务运作的信息系统进行全面的、细致的风险分析，使得各级管理部门和业务部门对信息安全方面存在的风险有一个更清晰的认识，为解决信息安全方面存在的问题提供有价值的建议。
- 平衡信息安全风险和投入，风险分析明确了核心信息资产面临的威胁及潜在的损失，确定了这些核心资产的安全保护需求，为平衡安全风险和安全投入提供了重要的依据，以最少的安全投入获得最大的安全回报。
- 培养信息安全风险评估队伍，通过与外部服务供应商合作，实施业务信息系统的风险评估，掌握信息安全风险评估的过程、方法和工具，积累实践经验，在内部培养一批具有信息安全风险评估技能的人员，为将来在全企业范围内对信息系统进行风险评估准备人力资源。

5.4 企业信息安全运维体系的建设

企业安全运维包含威胁分析与预警，安全状态和事件的监控，安全事件或事故的响应，以及基于安全管控目标的操作行为和日志审计系统。这些安全运维的任务主要可通过安全事件监控、响应、审计和相应的安全策略体系共同完成。安全运维体系包含服务于企业信息安全管理战略的管控目标和策略及相关的技

术支持手段，企业信息安全运维体系的建设通常体现为安全运维中心的建设。

随着企业信息系统的建设，必将部署越来越多的安全产品，如入侵检测系统，防火墙，防病毒等，这些产品产生的大量安全事件分散在各个不同的安全系统中，大大增加了日常安全事件维护和判断的复杂度并消耗了大量的安全维护人员。

与此同时如果要对系统（主机、网络、应用、服务）有全面的了解和控制，就一定要使用完善的日志系统。要记录的内容是针对某一个特定系统的事件，包括谁、做什么、何时、何地、为什么五个方面的内容。基本支持系统和关键系统必须要使用日志功能，日志记录的事件类型由系统拥有者和系统管理员决定。各个系统每天也在产生着大量的日志，需要耗费大量的人力来维护。

因此，通过建立安全运行管理中心来解决以上问题，明确信息系统中需要受到监控保护的对象，并建立相应的事件采集系统、事件收集汇总存储系统以及关联性分析系统并建立定期的针对某些事件信息数据进行安全审计的机制。确保目前采用的所有的安全产品和解决方案的有效性。集中发现网络、系统和应用中用户行为的违规问题，根据既定策略识别非授权访问、入侵等现象，并进行定性和定量的分析。通过对受控对象的活动进行安全审计，为系统、网络、安全管理人员及高层管理人员提供一个监督、检查当前信息系统运行状况的有效手段。

规划实施集中统一的安全运行管理中心，将分散在各信息安全监控基础设施管理系统中的各类事件数据信息统一收集汇总并进行必要的格式转换，将事件数据集中到一个统一的事件数据库中，并实现统一监控管理。同时，也要建立初步的监控信息知识库和监控关联性分析引擎。

在建立了安全运行管理中心之后，会产生大量的安全事件相关信息，针对这些事件信息为了能够支持业务上、系统性能上、独立的系统安全上、系统开发上、安全培训上的审计要求，必须建立信息安全审计机制。

由于在安全运行管理中心中，知识库和监控关联性分析引擎涉及的技术复

杂且实际情况多种多样不断变化,因此对于知识库和关联性分析引擎也应当不断的进行完善和更新以满足业务上持续发展的需求。

为了正确发挥监控关联性分析引擎的功能，各个系统的时钟应该保持同步。如果考虑到实现的复杂度和投资，可以考虑使用网络时间协议（NTP）来通过 GPS 同步系统的时钟，但是最终企业信息化系统是需要有自己的时钟源的。没有同步的时间信息,就无法准确分析复杂事件的发生过程,也就失去了日志的意义。

通过实施安全运行管理中心项目可以达到以下效果：

- 统一的管理模式——建立统一的管理模式，实现信息资源共享，更快的响应和解决问题，提高管理效率和管理质量，更好地适应管理需要。
- 规范化的管理流程——采用先进的科技手段，促使所有安全监控、响应、处理、恢复流程规范化。
- 自动化的管理操作——提高操作的效率和准确性,降低人工失误和遗漏造成的风险。例如：作业的自动调度、软件的自动分发、事件的自动处理、性能参数的自动收集、资产的自动汇总、数据的自动备份等。
- 高级的维护管理——通过对系统现状的统计和分析,智能地预测系统资源使用状况，主动防范系统运行中可能出现的故障和风险。
- 量化的评估标准——通过分析监控记录的历史数据,产生系统性能的量化分析报告，为决策分析提供可靠的依据。
- 科学的考核体系——建立科学的运行管理考核体系,实现对运行人员维护工作的量化考核，提高服务水平。
- 防患于未然——通过对安全相关事件的分析和处理,对隐藏在事件背后潜在的安全风险进行有效的分析和识别，防止一些可能的潜在安全事件的发生。

5.5 企业信息安全技术体系的建设

5.5.1 安全技术设计目标

一个合适的安全技术解决方案，不但需要理解安全管理的要求，用最小的投入得到最大的回报，同时也为安全运维管理提供了易于操作的平台。

在对安全技术规划实施时，需要考虑以下内容：

- 整体安全性的规划。
- 对于不同的安全功能机制加以整合以达统一控管及互补的目的。
- 考虑对其它同时进行的项目的影响。
- 从基础的、负面影响最小的安全措施入手。
- 具有未来的扩充性，不致因容量问题而须改变整体架构。

安全措施的设计与实施应当根据信息资产所面临的风险所定。安全措施的设计应以达到安全保护目的为原则而非最大限度的投入。

5.5.2 安全技术体系的建设

信息安全技术按照其所在的信息系统层次可以分为物理安全技术，基础架构安全（网络、主机和终端），应用安全技术，数据安全技术，身份和访问管理五大种类。可对应到前述企业安全架构中所述的接入控制、信任管理、信息流控制、审计和完整性 5 个安全子系统。

企业安全技术体系的建立原则是要建设与管理制度相对应的企业的安全架构设计。一般企业已部置了一些安全产品，还没有清晰的设计企业的安全架构，安全管理制度与安全架构所带来的执行力有些脱节，由此带来企业的安全管理制度的执行力不够。

在解决方案设计、具体的安全技术的采用上，需要考虑到当前企业应用系统中常见的安全弱点。同时针对安全评估得出的详细安全风险进行安全加固。每一个安全弱点都有相关的攻击手段与之相对应，针对企业当前应用系统中的主要安全弱点与攻击手段。将应用本身、应用承载主机、应用承载网络的主要技术风险作的应对在技术体系设计中加以考虑。

第六章 结束篇

本书主要介绍了当前企业在所处的信息环境中面临的信息安全问题 ;信息安全的基本原理和内容及其发展趋势 ;架构企业级安全体系框架的方法和框架的应用方法。

随着信息系统及网络在企业活动中占据越来越重要的位置 ,企业对信息安全的需求也日益高涨。部署一个可靠的，强大的，可伸缩的，经济的安全框架，并能对各种各样的突发事件做出准确 ,及时的响应 ,已经成为现代企业的基本需求。通过本书的论述，我们希望对您所在企业的安全信息系统的建设有所帮助,起到抛砖引玉的作用。

参考文献

在本规范的编写过程中，参考了以下资料：

[1]《安全之道--IT系统安全白皮书》（IBM中国技术支持中心，）

[2] 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）

[3] 《关于信息安全等级保护工作的实施意见》（公通字［2004］66号 ）

[4] 《信息安全等级保护管理办法（试行）》（公通字[2006]7号）

[5] 《中华人民共和国计算机信息系统安全保护条例》（中华人民共和国国务院令147号）

[6]《信息安全技术 信息安全风险评估规范》

[7] 《信息技术 信息安全管理实用规则》（ISO17799 :2005）

[8] 《信息技术-IT安全管理指南》（ISO13335）

[9] 《信息系统安全自我评估指南》（NIST SP 800-26）

[10] 《信息系统风险管理的指南》（NIST SP 800-30）

[11] 《信息和信息类型与安全目标及风险级别对应指南》（NIST SP 800-60）

[12] 《商业银行信息科技风险管理指引》

[13] 《Introducing the IBM Security Framework and IBM Security Blueprint to realize business-driven security》（IBM Redbooks, July 2009）

[14] 《Understanding SOA Security Design and Implementation》（IBM Redbooks November 2007）

在撰写过程中我们也参考了国际商业机器（中国）公司全球服务部实施和咨询团队的部分项目文档。

附　录

企业信息安全框架的对应

为应对企业信息安全建设的需求，企业信息安全框架的各个层次和组件可以对应到相应的安全服务和技术工具，企业可以根据自己信息安全建设需求从安全治理、风险管理和合规、安全运维、安全技术服务和架构对应层面找到对应的安全技术和服务方案。具体对应关系如下图所示。同时，在技术体系的建立过程中，也可以根据对应关系，同时提供技术架构的参考。

图示 25：企业信息安全框架的应用