企业安全管理实施指南（GES）

第 1 章：有效的安全治理的特点 [1]

Governing for Enterprise Security (GES) Implementation Guide
Article 1: Characteristics of Effective Security Governance

Julia H. Allen，卡内基·梅隆大学软件工程研究所，CERT®

Jody·R. Westby，全球网络风险有限责任公司的CEO，卡耐基梅隆大学CyLab实验室兼职特聘研究员

February 2007

翻译：樊山

校对审核：贺新朋

2013-02

摘要：本文是设置实施管理安全实施指南系列的阶段。它首先提出了几个关键的定义：企业治理、IT 治理和安全治理。它描述了 11 个特征，旨在回答这个问题：“如果我看到了，我怎么会知道是否是有效的安全治理？”文章接着进行比较和对比有效和无效的安全治理行动，然后介绍领导人需要预见和处理的十个关键挑战。

引言

本文（本系列的后续文章中）是建立在企业治理和IT治理定义的基础上。然后，它扩展并诠释这些如何理解保护数字资产[2]和业务的企业安全程序 (ESP) 的治理。

一个广为接受的定义是由国际会计师联合会（IFAC）和国际信息系统审计与控制协会（ISACA）所阐述的企业治理结构如下所示：

> 企业治理是一组董事会和高级管理层行使的提供战略方向和目标，并确保实现该目标的职责和做法，确定风险的适当管理和验证，使组织的资源被负责任的使用[IFAC04]。

确定有效的企业治理，包括商业圆桌会议（Business Roundtable）[BRT05]：

- 为被治理单位的行为建立管理文化基调
- 指定了一个决策问责制和完整性，包括分配角色和职责，行为准则的框架
- 确定一个清晰、明确的组织的战略目标方向
- 指导、控制并强有力的影响单位以实现既定的期望
- 操作和及时披露财务报表准确地做出决定和结论
- 调整风险管理策略，并确保遵守
- 对业务和管理行为进行有效的尽职调查和审计
- 通过有效的控制、度量和执行政策确保决策的实施

- 使治理体系覆盖整个组织

治理延伸到管理组织使用 IT。IT 治理研究所声明[ITGI 03]：

IT 治理是董事会的董事及高级管理层的责任。它是企业治理的一个组成部分，由领导层、组织结构和流程组成，以确保该组织的 IT 支撑和扩展组织的战略和目标。

企业治理和IT治理越来越多地包括IT系统和信息的安全性。美国工业安全（ASIS）、信息系统安全协会（ISSA）、ISACA 协会的成员（Booz Allen Hamilton）检查安全风险和业务操作的融合。在他们的报告中，企业安全组织融合，这种融合他们采用 ASIS 的说明 [AESRM05]：

识别安全风险业务功能和流程在企业内部和业务流程管理解决方案的开发之间的依赖性，处理这些风险和相互依存关系。

企业安全管理的定义为[Allen 05]：

- 指导和控制组织建立并维持组织的行为（信仰、 行为、 能力和行动）中的安全文化
- 在业务处理中适当的安全是一个没有商量余地的要求

美国国家标准与技术研究院（NIST）在其出版物，信息安全手册：管理指南[Bowen 06]（Information Security Handbook: A Guide for Managers）中扩展信息安全治理这个定义如下：

……建立和维持一个框架支持管理结构和过程，以提供保证信息安全战略的过程

- 符合并支持业务目标
- 通过遵守适用的法律和法规相一致的政策和内部控制策略
- 职责分配

管理所有的风险。

最有效的安全治理和管理是当他们把文化和架构系统的有机结合在一起的组织行为和行动。 在这方面，一个团体或组织文化的定义是主要的，共同的态度、价值观、目标、行为和惯例为特征的运作。文化进而创建和维持政策、 流程、 人员和绩效之间的联系。有效的安全应被看作是组织的属性或特征。很显然，每个人都

积极主动地执行自己的角色和责任，创造一种文化取代无知和冷漠的安全。

为此，安全必须脱离技术持观望态度如同行为和责任完全被转移到软件开发和IT 部门一样。今天，董事会的董事，高级管理人员和管理人员都必须不懈的努力持续的驱使建立和加强有效的企业安全。如果企业安全的责任分配的角色缺少权力、责任和资源以落实和执行它-那么将无法把整个组织从横向和纵向连接起来-达到所需的安全级别，安全性将无法衔接，实现或持久。

相反，普遍认为安全是一个技术问题，甚至是尽最大的努力购买基于软件的安全解决方案与建立安全开发的软件和业务系统遭遇“相当大的阻力，因为问题大多是组织和文化而并非技术” [Steven 06]。在今天的互联环境中，需要整合有效的安全保障，法律，管理，运营和技术方面的考虑。

这种提升安全性的一个独立的技术问题角度向关注企业的问题转变。因为安全现在是一个业务问题 [3]，组织必须启用、协调、部署并指导其核心资源和能力，所以安全风险管理需要与公司的战略目标、运行准则、合规性要求、技术体系架构相结合。为维持企业安全，组织必须走向一个具有战略意义的、系统的和可重复的、资源高效利用和有效性、保持一致实现目标的安全管理过程 [Caralli 04]。这一过程，需要考虑到政策、程序和技术的事实是动态的。

本文介绍了如何确定作为治理关注点是否被安全有效地解决。他比较和对比了有效与无效的做法，并介绍了一些确保一个安全计划成功执行所必须面对的挑战。。

11 个有效的安全治理的特点

一个最好的解决组织安全治理和管理问题的措施之一是，领导者定期公布的一组与安全的最佳做法和标准是一致的信念、行为、能力和行动。这些措施有助于建立安全意识的培养。它们可以表示为对组织目前的行为和状态的陈述：

整个企业范围内的问题

安全管理作为一个企业的问题，横向、纵向跨越整个组织的职能。这里所描述的企业安全计划（ESP）的范围包括人、产品、设备、流程、政策、程序、系统、

技术、网络和信息（P6STNI）[Westby 05]。

领导责任

在组织的安全性方面，行政领导了解他们所服务的社区（包括互联网社区），和重要的国家基础设施以及经济和国家安全利益的保护的问责制和和所肩负的职责，他们是利益相关者。

高层领导人显式地从事企业安全计划的管理和监督，并支持这项工作，提供足够的财政资源、有效的管理、基于风险的策略和年度审查和审计。企业管理人员接受与他们的数字资产（系统、网络、应用、信息）相关的安全风险的责任和所有权。

从业务需求角度看待

安全性被看作是一个业务需求，直接与战略目标、企业目标、风险管理计划、合规性要求，和顶级政策相辅相成。管理人员在整个企业中了解如何把安全服务作为一个业务推动者。“一个有效的安全计划的实施归根到底就是明晰组织自身的利益”[BSA03]。

安全性被认为是一个开展业务的成本和投资费用，而不是一个或酌情预算项目。安全策略被设置为顶级组织和业务单元，职员不允许单方面决定他们想要怎样的安全。这就是说，适当的策略异常流程允许业务继续，同时又可确保领导者有足够的监督。足够和持续的资金和足够的安全资源的分配是给定的。

基于风险

根据组织的容忍度，包括合规性和责任风险、业务中断、声誉受损及财务损失的风险确定怎样的安全是足够的。合理可预见的内部风险和外部风险暴露进行检查，如果有必要可重置容忍级别，因为这是审查组织的绩效和风险的正常过程的一部分。

角色，责任分离的职责定义

合格的人员被分配到领导岗位-首席信息官（CIO）、首席信息安全官（CISO）和/或首席安全官（CSO）[4]、首席风险官（CRO）、首席隐私官（CPO）。， 考虑

到帐户的职责分工、责任和风险管理的责任，要明确界定企业领导的安全角色和职责并独立报告。

处理和执行政策

安全性要求的实现包括通过明确的政策和程序所支持的人，程序和技术解决方案，包括控制、培训、监视和执行。并对贯彻运用和加强符合安全策略的进行奖励、表彰。

充足的资源投放

拥有充足的资源、权力和时间的关键人员包括 IT 和安全人员来建立和保持企业安全的核心竞争力。这包括就威胁、脆弱性和风险的业务连续性使用的安全专家，技术的部署和继续教育。

员工意识和培训

访问数字资产的所有工作人员了解他们的日常职责，保障和维护组织的安全状况。意识，动机，以及遵守公认的，预期的文化规范。定期和持续的进行安全意识与有针对性的和工作描述中反映安全责任的培训。

开发生命周期要求

安全性要求是针对整个所有的系统/软件开发生命周期的各个阶段，包括启动、采购、工程需求、系统架构和设计、开发、测试、运营、维护和废弃。

计划、管理、可度量和度量

安全被视为常态的战略、 资本和业务规划周期的一个组成部分。安全已被集成到战略和运营计划，并实施有效的控制和度量的可实现的、可测量的目标。评价和审计计划确定的安全弱点和不足之处，对业务连续性的要求，并根据行动计划和里程碑（POAMs）衡量进展。

高级领导人根据定义的性能参数衡量这项工作。管理者检视安全如同他们的责

任并理解这些，他们在安全性方面的整体表现是衡量自己团队的表现。

任何新项目的启动、获取或关联都应该积极考虑安全性作为正在进行中的项目管理的一部分。

评估和审计

董事会风险与审计委员会进行定期评估和审计的 ESP。他们确保该程序的所有组件维护和组织 ESP 持续维持所需的安全状态。

有效与无效的安全治理

有效与无效的安全治理的比较和对照进一步说明一组行为和行动是非常有用的。有时缺乏一个更准确的指标衡量质量、价值或文化规范的存在。表 1 给出了在企业内部从不同的角度的比较。

表 1：有效与无效的安全治理

有效	无效或者不存在
董事会成员理解信息安全对于组织和需求而言是非常重要的,因此每季度要对破坏安全防护的策略进行更新。 董事会建立了董事会风险管理委员会（BRC）了解安全符合适用的法律和法规在减轻组织风险中的作用。 BRC 进行定期审查 ESP。 董事会的审计委员会（BAC）确保年度内部和外部审计的安全程序执行和报告。	董事会成员不理解信息安全在他们的领域的责任，只专注于企业管治及利润。 可能在所有的问题中安全是解决临时问题 可能所有的评估都发生在重大事故发生之后 BAC 遵从内部和外部审计师的评估需求。但是没有审计计划来指导选择。
BRC 和执行管理团队设定一个可接受的风险水平。这是基于全面和定期的风险评估，要考虑到合理的可预见的内部和外部	CISO 定位样板文件的安全政策，插入组织的名称，并有 CEO 签署。 即使存在安全计划文档，他也没有对应到

的安全风险的危害程度。 产生的风险管理计划与公司的战略目标保持一致，为公司的安全政策和程序奠定基础。	组织的风险管理或战略计划，并且没有获得系统和其他数字资产的安全性要求
跨组织的高级管理人员、法律总顾问、CFO、CIO、CSO 和/或 CRO、CPO、人力资源、内部沟通/公共关系以及采购人员组成的安全团队定期举行会议，讨论安全计划的成效、新的问题并协调解决存在的问题。	CEO、CFO、法律总顾问、人力资源、采购人员和业务部门经理负责检视信息安全，CIO，CISO，IT 部门不涉足。 CSO 处理物理和人员的安全，很少和 CISO 交换意见。 特别是法律总顾问很少就合规性要求或合同安全条款与管理人员和技术人员进行通讯，或在一个临时的基础上进行通信。
CSO / CRO 报告组织 COO 或 CEO 应明确划分独立的 CIO 的职责和权利。 业务政策和程序强制责任分工 (SOD) 和提供制衡和审核跟踪信息不被滥用。	CISO 向首席信息官报告。CISO 负责所有与系统和信息的所有权相关的活动。 CRO 不与 CISO 交互或认为安全是本组织的主要风险。（另见注释 3）
风险 （包括安全) 在整个业务流程决策点的固有关键步骤都记录在案，并定期检讨。 执行管理层认为企业领导者负责其特定的业务单位开展风险管理活动（包括安全性）。 企业领导者接受为他们系统的风险，并批准或拒绝他们的操作。	所有的安全活动发生在安全部门，安全工作的一个竖井内，并没有被集成在整个组织。 企业的领导不知道他们的系统相关的风险或为他们的安全状态概不负责。
关键系统和数字资产记录在案并指定了所有者和定义的安全要求。	未记录系统和数字资产，没有分析潜在的安全风险对操作、生产效率及盈利能力的

	影响。系统和资产所有权没有明确规定。
在业务和技术层面的变更管理有成文的策略和程序，适当的职责分工。 对故意的未经授权更改并确定影响的行为“零容忍”[6]。	变更不被记录或控制，变更管理过程不存在或无效。。 CIO（代替 CISO）确保所有必要的更改的安全控制，实际上 SOD 是不存在的。
员工有遵守安全政策和程序的责任。以下行为会被追究责任，这包括报告任何恶意的安全漏洞，故意的妥协或怀疑有违反政策和程序的内部行为。	政策及程序被开发，但是没有强制执行或问责制。没有进行例行员工检查控制跟踪。
ESP 实现行之有效的安全实践和标准以支持业务运营。	根本没有或仅实现最小的安全标准和安全实践。所使用的这些不被看作企业的当务之急。
采用既定的，标准化的过程，在一个一致和知情的情况下购买和部署安全产品，工具，管理服务和顾问公司的服务。 他们会定期审查，以确保它们持续满足安全要求和成本效益。	在没有任何真正的研究或性能指标能够确定他们的投资回报率或效益的情况下购买和部署安全产品，工具，管理服务和顾问公司的服务。 因为它使用的产品、工具、管理服务以及顾问公司的方式，导致该组织所拥有的安全是一种虚假的安全。
组织在业务流程中审查企业安全计划、安全流程以及安全的角色。 ESP 的目标是持续改进。	组织没有企业安全计划也不去分析它的安全性改进的过程。 组织用一种临时的方式响应最近的威胁或攻击来解决安全性，经常重复同样的错误。
由 BAC 进行独立审计。通过 BRC 独立评估。领导和董事会讨论结果。 及时采取纠正措施，并评估。	重大安全事故之后进行审核和评估

落实企业安全计划面临的十大挑战

开展企业安全计划，并采取必要的治理行动并维持它需要坚韧和毅力。组织在前进的道路上可能会遇到重大的挑战。由于这些计划的企业性质，这些挑战可能发生在所有的各级组织和 ESP 的各个阶段。理解和及早考虑如何响应对 ESP 过程及有效性是极为有利的。

好消息是挑战一旦被掌握，可以成为机会。有效地解决这些挑战的领导者，可以利用成功的解决方案为客户、业务伙伴、员工创造一个可信的环境，缔造商业机会。

挑战通常要考虑的问题

- 了解无处不在的访问和分布式信息的影响
- 重视企业范围内的安全问题的本质
- 克服缺乏应对计划
- 建立适当的组织结构和职责分工
- 了解复杂的全球性法律合规要求和风险责任
- 评估安全风险和危害组织的程度
- 确定和调整资源投入保持在适当的水平
- 处理安全的无形影响
- 协调部署不一致的安全最佳实践和标准
- 克服在创造和维持一个安全意识的文化遭遇的困境

无处不在的访问,分布式信息

许多董事会和高管不明白与全球网络相连的互联网的本质，这对于组织和其合作伙伴和客户群分布在整个信息的访问有多少帮助。风险和机遇越来越多地来自于你连接到（你的系统和网络）谁和谁连接到你。

“以太网之父”罗伯特·梅特卡夫，假设网络的价值是网络节点的数量以平方级在增长。它很可能使全球的风险增加到一个更高的指数，我们有今天的互联网，人们可以基本上到达所有地方。假设它们存在于所有的国界，已经大大延伸，无论

是预期的或意想不到。

今天的市场是由消费者准备和直接提供给任何人访问，他们希望与世界各地建立业务往来，有权以任何理由选择并十分简便的改变自己的选择。有时，顾客的需求和要求是不同的–甚至在–确定或规定的需求和业务需求都可能不同。重要的是要了解并减轻造成的冲突和安全风险。

例如，使用强大的，多层次的认证和访问控制保护需要保护的敏感信息访问是业务的需求。办理业务的客户、合作伙伴、供应商可能要求提供方便和快速访问这些信息的方式。业务和客户需求之间的紧张关系往往是不甘心推定双方都经历的过程中，识别敏感信息和分类，根据分类方案，在各级保护条款下达成一致。
不幸的是，情况往往并非如此。

企业安全的本质

安全性必须支持和保护业务流程。了解达成安全要求的教育广度和范围。那些负责安全的人员经常会发现很难说服高层领导认识到用一种系统的方式实现企业安全的必要性，。对于大多数组织和人而言，安全性，如保险，可能是一个抽象的概念，可能是永远不会发生的假设性事件。

安全责任分布在整个组织，需要跨组织的互动，合作和执行。它不能委托给组织内特定的部门或视为单纯的技术问题。如果对企业安全没有一个明确的了解，发挥至关重要的作用的人员和流程可能很容易被错过。组织内的许多职能部门需要互动，以创造和维持一个有效的安全解决方案，包括战略、法律、技术、组织、经济和社会因素。[Westby 05]

在技术层面，这包括确保安全能够贯穿整个系统开发生命周期的所有阶段，其中涉及的需求、设计、开发或获取的软件为基础的系统，而不是等到部署系统。[Bowen 06]

缺乏一个应对的计划

领导者往往不知道在哪里或如何开始。他们缺乏一个行动框架-如何设置优先级、分配任务、开始并监督执行。

现在对企业的安全有国际公认的方法，它可以帮助企业确定应该做些什么，应该谁做。在本系列文章中提供的指导，可以帮助董事会和高管更好地了解如何处理企业的安全。领导者如果没有这样的做法，将不清楚如何分配责任、分配保障资金、确定投资回报并测量性能[BSA 03, Westby 04b]。

组织结构和职责分工

有许多领导者经常用一个临时的方式给这个领域内的首席信息官（CIO）错误地分配安全责任。如果首席信息安全官（CISO）被任命，通常这个角色给 CIO 报告，这违反职责分离（SOD）的原则。CIO 和 CISO 与 IT 功能和成本方面的要求经常有冲突的，他们可能不是在一个位置去利用必要的资源和权力，在多个业务线或部门解决安全性问题。因为在 CEO 或董事会层面通常很少关注这个问题，信息安全的力度经常被错误的组织结构所削弱[BSA03，CGTF04]。

由于业务的 IT 和业务安全问题的紧密结合，一些组织可能最初要求 CISO 向 CIO 报告。然而在这种情况下，需要解决明确职责分工，以避免利益冲突。这包括可能在一个被削弱的安全文化背景下，导致将安全需求的资源分配给 IT 业务活动，并发送一个安全性不是最高优先级的信息。

复杂的全球性法律框架

企业安全性要求能产生广泛的国际、国家、州和当地的法律和法规，以及国际标准、政策和法律合同。在世界各地，越来越多的隐私和安全要求是相互矛盾的，在最好情况下，建立不同层次的要求，[Smedinghoff 06, Westby 04a]。 “组织可能面临不同的挑战性的措施”，并监测这些措施以满足各种报告要求[Bowen 06]。此外，总是在不断变化法规环境，所以安全计划需要进行审查并定期调整，以确保它们符合目前的合规要求和潜在责任检查。

了解隐私和安全要求更为复杂的是难以适应跨界数据流动和满足法规遵从性要求的安全违反通知和数据保留法律。此外，大量的不同的法律中有关网络犯罪活动产生进一步的复杂性，必须组合在 ESP 中。[Westby 03]

了解安全风险

安全活动往往由于资金不足而导致风险和事故危害的严重程度不成比例，因为安全责任没有正确瞄准业务操作和风险。确定正确的安全级别是在有效的风险评估基础上产生的业务决策的结果。这种评估包括分析在可预见的内部和外部风险与他们的危害程度。重要的是，董事会和高管利用既定的风险评估指导，并了解来自他们的危害可能会流入到他们的组织[Bowen 06, BSA 03, Stoneburner 02]。当这些风险被有效地克服，安全风险也可能保持和提升企业价值，创造市场竞争优势的机会。

难以量化的成本/效益

解决在企业级的安全性往往难以证明其合理性。所采取的行动，以确保一个组织的资产和流程，通常被视为灾难预防而不是生产收益（如保险），这使得它很难确定如何最好地证明投资的安全性以及到什么程度。

安全投资的效益往往只出现在那些未发生的事件。因为它是不可能验证产生负面的影响，组织规避成本上产生什么样的价值？这个难题已经不仅是困扰安全性，以及类似正在努力提高软件质量，进行适当的测试，保存数据到文档，保留当前的配置和硬件/软件清单记录[Braithwaite 02]。

不同于保险，损失的原因基本上是已知的或变化非常缓慢，被认为是安全的威胁和影响的性质信息和系统的漏洞是不断发展和变化

尽管如此，如美国国会研究服务等组织记录了有用的指导和损失与安全事件的统计数据[CRS04]。他们声称：

网络攻击对股票价格影响的调查显示，确定的目标公司遭受的攻击之后几天损失 1%至 5%。对于一般的纽约证券交易所上市的公司中，价格下跌的幅度转换成美元之后，股东损失在 50 亿美元和 200 亿美元之间。

安全带来的影响往往是无形的

虽然有形的安全事件可以测量（在限期内恢复和重建丧失生产力和工作人员系统的时间），无形的影响可能更严重。无形的影响包括对组织的信任关系的影响、

损害其声誉、经济以及社会的信心，导致从已公开报告的违约损失。

在其固有的性质，安全性有时被描述为一个支持网络和组织新兴的属性。鉴于安全的许多层面，制定安全难以轻易确定具体的方向。一个组织的安全状况往往取决于人、流程和技术的互动与交叉。随着组织和基础网络设施在响应不断变化的风险环境的变化，一个实体的安全状态也将改变。

部署的最佳做法和措施不一致

许多组织都无法达到的安全性的有效部署，普遍接受的做法是他们解决已经出现的问题，并试图跟上伴随的安全风险的变化和增长。其结果是，建立一个 ESP 可能是一项特别艰巨的任务。

幸运的是有一些被广泛接受的安全最佳实践和标准。国际标准化组织（ISO）的 ISO 17799[ISO05A]和 ISO 27001[ISO05B]一路领先。美国国家标准与技术研究所相继出台了一系列世界级的标准和信息安全指南，适用于公共和私营部门实体。

专业技术协会发展的最佳实践，已被全球范围内的行业和政府采纳。一个很好的例子是由信息系统审计和控制协会开发的控制目标“信息及相关技术框架”（COBIT） [ITGI05B]。越来越多的准则和清单，例如为互联网安全中心创建确定大多数专业人员认为可以接受的做法。[Allen 06d]

毫无疑问，在安全的情况下组织今天面临的是一部分没有重视这些实践和标准。很多报告给 CERT[7] 的漏洞证明这种差距的存在，其中有许多已知的解决方案尚未实施。实施稳健的做法和安全标准可以显著促进正确部署组织安全状态作为 ESP。这就是说，并不是每一个实践和标准适用于每一个组织。领导者需要确保实践的选择和实施直接支持业务目标。

建立和维持安全文化的困难

实现特定的安全状态并不能保证它可以持续。安全不是一个一次性项目的开始和结束，这是一个持续的过程。它需要不断改进，监测，测量，并执行（即“做”）[Allen 06e, ISO 05b]。持续改进需要关注和投资，在核算和经济可行的情况下安全投资往往以牺牲其他需求来优先考虑的事项。

由于安全是困难的，往往令人讨厌因此大多数人和组织不愿应对。解决安全不仅仅是一个战术，技术能力是难以克服的障碍因素。作为一个网络社区，有没有完美的解决方案，有效的安全保障，措施和基准可能根据不同行业，不同公司有所不同。这种局面难以改善没有显著报告事件增加的成本/损失来估算可能发生的损失，在已经发生的过程中没有采取降低风险的指标。这些指标是类似保险公司精算数据，它提供了一个损失评估的统计的基础[Gerdes 05]。

此外，安全保障常常被看作是有负面的影响，如增加了成本、降低了应用程序、系统和网络性能和给用户带来不便（例如多种方式进行身份验证、定期更换以及很难记住）。“虽然内部审计人员往往在业务系统内识别安全漏洞，他们更严格的制度控制的建议被否决，因为在许多情况下，实现和维护这些控件的直接成本或者因为它们引入导致不受欢迎、效率低下” [Taylor 04]。董事会和高级领导应该需要正式的审计和审查安全程序，与正式的报告卡和及时采取纠正措施以结束风险。

因此，董事会和高级管理层有一项艰巨的任务创造一种安全文化意识的基调，积极遵守安全性需求。只有政策是不够的，他们必须支持自顶向下的行动转达安全在企业经营和竞争力的重要性，和安全漏洞对企业利润和声誉的影响。

高层领导积极显著的参与是最有效地通过开发和维持的 ESP 方法 [Westby 04b]。

总结

理解-克服-组织所面临的挑战，因为他们开发和维持一个 ESP 是有效的安全这一进程道路上的一部分。每一个挑战，需要组织内的众多参与者的关注。因此，面临的挑战可以被用来作为统一的工作机制，通过跨部门的安全团队能够帮助开发从业务人员像他们购买安全解决方案。

一个有效的方法管理和治理企业安全必须正视这些挑战，提供对比和效益预测并且相互抵消面临的挑战。不断提高认识，知识和理解安全成为共同的理念是必要的第一步。这包括制定包含风险和机会的安全价值观。

结论

在今天的经济，政治，科技，环境和社会环境，解决安全问题的必要性是大多数组织的一个核心。客户需要它是因为对隐私和身份盗窃事件上升的关注。商业合作伙伴，供应商和尤其是当彼此相互提供网络和信息访问时形成了需求。通过使用网络间谍活动，获得有竞争力的情报，并敲诈组织正变得越来越普遍。国内和国外的法律和法规的要求组织（以及其领导）在安全性方面需要表现出应有的谨慎。

一个组织能否充分利用新的机遇往往取决于其提供开放、 方便、可用的和安全的网络连接和服务能力。有信誉维护信息和所在的内部环境之内增强组织保持和增加市场份额的能力。

企业安全管理意味着足够的安全是一项不可或缺的业务需求。如果一个组织的管理，包括董事会的董事，高级管理人员和所有管理人员没有建立和加强业务需要的有效企业安全策略，组织的所需的安全状态将无法衔接、实现或持续。为了实现可持续发展的能力，企业必须统一企业安全领导的治理水平，采取行动强制遵守而不是如其他的组织一样缺乏权利、责任和资源。

参考本文在http://www.cert.org/governance/references.html。

注释

1 在这篇文章的大部分内容是摘录和更新先前发表的作品[Allen 05, Allen 06a, Allen 06b, Allen 06c].

2 这个指南不专门针对物理资产如以物理形式的设施，设备和信息的安全性和保护，虽然很多指引中都适用于这类资产。

3 请参阅“管理企业安全性”[Allen 05]和“安全不仅仅是一个技术问题”[Allen 06b]。

4 有些组织有CSO和CISO，分离的设备和人员的安全职责，以及IT/信息安全。随着企业意识到，但是，它们的物理设施，流程和人员的安全受到IT系统和设备的影响，反之亦然，它们整合了CISO和CSO的职责演化成一个综合CSO角色的首席风险官（CRO）的作用[ITCI 06]。本指南使用的术语CSO，实际是指包括CISO和可替代CRO的角色。另外，如果一个组织有CSO和CRO，他们都参与ESP的开发和维持，CSO带头执行安全性要求的风险管理计划，由CRO实施与监督。

5 这个建立依据和修改是在Harris的一篇文章中发现类似的陈述[Harris 06]。

6 零容忍，意味着对系统进行定期监测未经授权的更改。如果发现这种变化会立即进行调查，或备份操作配置和事后的检验进行检讨，以确保这种情况不再发生。请参阅“Prioritizing IT Controls for Effective, Measurable Security。[Kim 06]”

7 卡内基 - 梅隆大学的CERT和CERT协调中心是在美国专利和商标局注册。