1. 信息安全度量的定义

1.1 什么是度量

在物理和数学领域，度量的定义为“用拓扑空间的二值函数，给出空间中任意两点之间距离的值，或者是用于分析的距离的近似值。”我们可以认为，“几乎任何量化问题空间并得出值的情况，都可能看作是度量”。传统的企业管理领域有一条准则——不能测量的东西就不能管理；这条准则也同样适用于信息安全管理领域。

1.2 什么是信息安全度量

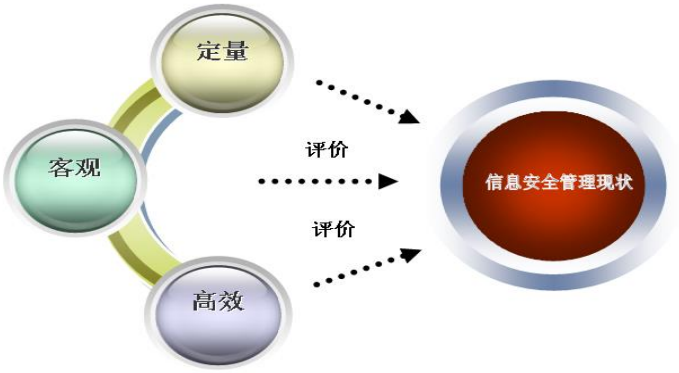
行业的实践经验表明，企业在完成了网络安全架构和安全管理建设的基础建设之后，常常会遇上安全管理落地难、检查难的问题。安全内控度量则是针对此问题的解决方案。

信息安全内控度量可以理解为在企业内部信息安全管理中通过采用系统的、量化的、有效的手段对信息安全管理的现状进行测量和评价，从而发现潜在的安全控制弱点，切实推动安全管理规范的落地，持续提升组织的信息安全管理水平。

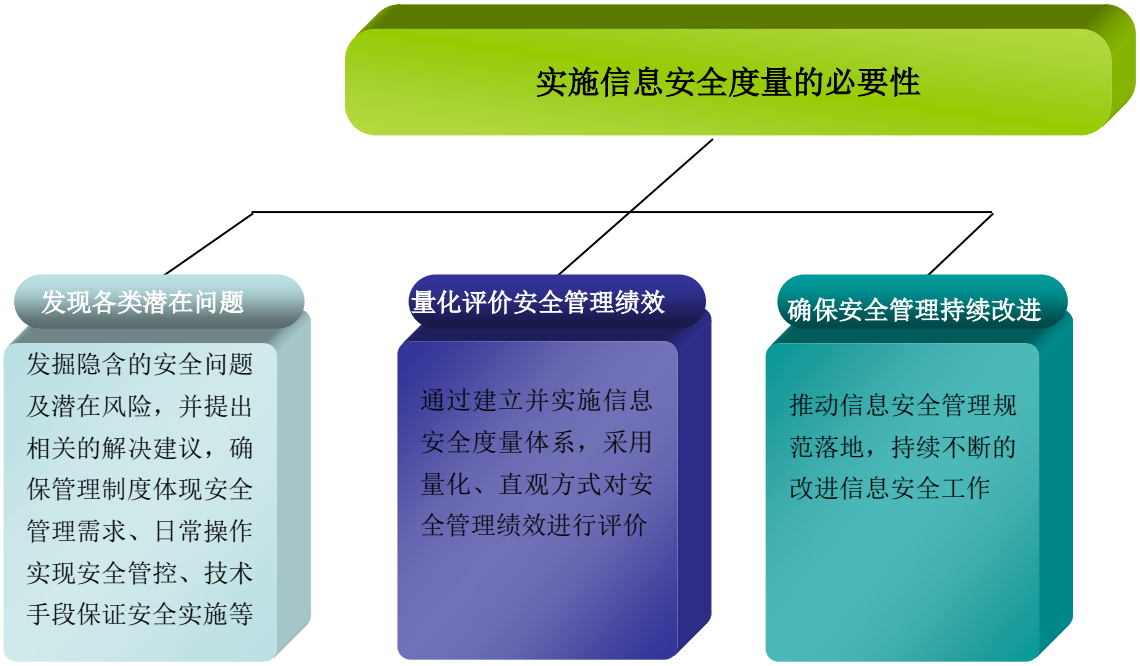
2. 信息安全度量体系建设意义

2.1 度量的优势

以往对信息安全管理情况的评价大多采用定性评价，定性评价的优点在于能够对无法量化的制度建设、流程控制、日常操作等方面进行一个较为客观的评价，但定性评价的缺点也很明显，由于无法对评价结果进行量化，只能人为的对评价结果进行大致分级，这就有可能因为评价者自身的不足影响评价的客观性和准确性。信息安全内控度量正是要解决这种问题，通过大量可量化的、具有代表性的指标对信息安全管理情况进行量化的分析和评价。



2.2 安全度量的必要性



2.3 度量和审计的差异与关联

比较项	审计	度量
发起方	内部 / 外部	内部
关注重点	合规性	包括但不限于合规性
活动持续时间	阶段	周期 / 持续
评价方式	定性为主	定量为主
产出物	审计报告	安全管理绩效

3. 实施方法论和依据

3.1 信息安全内控度量体系理论支持

任何体系的构建都需要相应的标准及理论支持，信息安全度量作为评价信息安全管理的重要手段之一也不例外，国际上已经有了一些较为成熟的体系及标准为度量体系的建设提供支持，Cobit 和 ISO27004 就是最为典型的两个。作为 IT 治理框架，Cobit 提供了一个 IT 管理框架以及配套的支撑工具集，这些都是为了帮助管理者通过 IT 过程管理 IT 资源实现 IT

目标满足业务需求。Cobit 建立了一个包含 7 个业务需求、20 个业务目标、28 个 IT 目标、34 个 IT 过程、100 多个控制管理目标的 IT 管理框架，通过控制度、度量、标准三个纬度来度量 IT 过程能力。ISO27004 作为 ISO27000 系列中的一个重要组成部分，对信息安全度量目标、度量项、度量过程、度量值乃至度量实施都给出了指引。

3.2 内控度量的 PDCA

PDCA 就是业界公认的信息安全管理方法论，遵循计划（Plan）、实施（Do）、检查（Check）、改进（Action）相结合的闭环机制，可以有效的为各类安全管理活动提供支持。如下图所示，采用 PDCA 的循环机制，通过度量体系设计、度量实施、度量结果分析、输出、度量改进这四大环节，可以建立持续改进的信息安全管理机制。

3.3 安言的 PROC 方法论

作为信息安全咨询提供者，安言咨询在以 ISO27001 认证为代表的信息安全管理体系建设方面经历了长期的实践，积累了丰富的经验。在帮助企业建立符合自身需求的信息安全内控度量体系上，安言咨询的方法论体现为 PROC 过程模型，这个过程模型是对经典的 PDCA 管理模式的具体实现，更具有针对性和可实施性。

PROC（Preparation，Realization，Operation，Certification）模型如下图所示。

PROC 模式将整个信息安全内控度量体系建设项目划分成四个大的阶段，每个阶段又包含相应的工作子项，每项工作均具有前后关联，只要能够按照规划顺利开展各阶段工作，最终就能建立起有效的信息安全内控度量体系，实现信息安全管理工作的客观、量化、有效评价。各阶段具体工作如下：

- **准备阶段（Preparation）**：在准备阶段，项目小组要对信息安全内控度量体系的实施做好预备工作，明确度量体系实施范围，提供相关资源，建立总体的安全管理方针，进行现状调研，了解并分析信息安全现状，明确风险问题和由此带来的具体需求。这
- **实现阶段（Realization）**：在实现阶段，项目小组要组织相关资源，依据前期现状调研和现状分析结果开展度量体系设计和实现工作，为好计划，同时编写、测试、修订并完善内控度量体系运行所需各类文件。
- **运行阶段（Operation）**：信息安全内控度量体系建立起来之后，要通过一定时间的试运行来检验其有效性和可操作性性。在此阶段，应该培训专门人员，建立起内部度量机制，通过例行检查、专项检查等各类检查活动，来检查已建立的度量体系是否符合企业评估自身安全管理的要求。
- **验证阶段（Certification）**：经过一定时间运行，内控度量体系达到一个稳定的状态，各项文档和记录已经建立完备，此时，可以提请进行项目验收。

3.4 信息安全内控度量体系设计依据

度量体系的设计需要参考企业内部和外部管理要求，行业标准、法律法规、监管机构发文等都可以作为参考，一般包含以下三类文件：

- 内部安全制度：企业内部发布的各类安全管理制度
- 国内法律法规及监管机构要求：各类国家标准（GB50174-2000、等级保护等）、《银行业金融机构信息科技风险管理指引》等
- 国际标准、行业最佳实践：ISO27001、ISO27002、ISO 27004、Cobit、ITIL 等