# 电信网安全保障能力评价模型与方法浅析

近年来，在国家信息化战略的指引下，越来越多的企业核心数据承载在网络环境中，IT 网络环境下的信息安全问题成为信息管理者关注的问重点，如何构建信息安全保障体系，同时如何建立一套科学有效的评价标准，考量系统的 IT 保障体系建设能力水平，一直是学术界和企业共同关注的焦点。

作为国内最大的固网电信运营商来说，随着中国电信全业务运营战略的推进，IT 系统（即 CTG-MBOSS 系统，由管理支撑系统 MSS，业务支撑系统 BSS，运营支撑系统 OSS 和企业数据架构 EDA 组成） 已经成为电信生产环节中不可或缺的一部分，IT 系统的安全问题也日趋重要。

中国电信 IT 安全保障体系以 CTG-MBOSS 信息化架构为基础，是支撑企业 IT 安全建设和管理的基础架构，整个体系以 IT 安全战略为指导，将组织、策略、运行、技术等安全各方面要素结合起来，通过安全管理制度的逐一落实，安全防护措施的统一部署，循序渐进的构建一个科学全面的信息安全保障体系。体系建设和实施路线遵循“管技结合、预防为主、注重长效、循序渐进”十六字方针，按照“职责明晰、预防为主、有效识别；主动防御、及时响应、集中管控；体系完善、流程通畅、全员参与” 的路线向“可管、可控、可信”三个阶段能力目标演进，最终实现可信赖的 IT 安全运营环境愿景，整体安全保障体系框架如图 1 所示。


图 1　中国电信 IT 安全保障体系框架图

其中，安全策略体系总述了中国电信 IT 安全的总体方针政策、演进策略、标准和指南、以及各类实施细则组成。

安全组织体系定义了保障 IT 安全策略有效执行需要的角色和职责，为安全策略能够贯彻实施的组织保障的保证，从职能上分为决策、管理和执行类别。

安全运行体系从 IT 系统生命周期和安全风险管控流程出发，从开发、建设、维护、响应和核查五个阶段提出安全风险管控的要点，明确了不同阶段安全防护的具体要求，涵盖了风险管理、系统开发建设、运行维护、事件响应、安全监控和安全检查等内容。

技术体系是实现 IT 安全保障体系的重要手段，从物理安全、网络安全、系统安全、应用安全、数据安全和终端安全六个方面实现安全检测与识别、安全防护、安全审计与恢复三大保障能力。

## 2　安全能力成熟度模型

为了保证电信网 IT 安全保障体系建设有序推进并完成建设目标，需要一套合理的评价模型和方法对安全保障体系建设成效进行公正有效的考量和评价。而且该模型和方法要能够适应复杂的实际建设情况，能够包含量化评估的方法、模型和流程，是一个全面科学的、可量化的考评体系。

当前国内外关于信息安全评估的标准和考评方法形成了几种流派，其中国标 GB-T2027 对安全建设能力成熟度评价做了基本的定义，描述了 5 个级别的安全保障能力定义，分别为：未实施级；基本执行级；计划和跟踪级；充分定义级；量化控制级；持续改进级等五个级别，上述 5 个能力级别对能力特征进行了充分的定义，但没有给出具体的操作细则。

在结合了国家标准和电信实际现状后，结合其他行业最佳实践和中国电信实际情况，从考核指标量化入手，围绕五级能力成熟度模型，形成一个可持续改进的 IT 安全保障体系能力成熟度模型和评价方法，模型从 IT 安全规划建设、运作、技术保障、管理措施等几个方面因素入手，建立一种普遍适应的评价准则，对安全能力建设做出评价，指导企业开展安全建设工作。

### 2.1　考量指标

评估 IT 安全保障体系能力成熟度通过上述安全保障体系策略、组织、运行和技术四个层次来进行，每一个层次包含不同的内容，对应着不同的标准和考核指标。在每一个层次中，有关键指标，围绕关键指标，有相应的具体流程和活动，能力评估就是根据这些关键指标和相应流程合活动的情况合状态来进行的。在 IT 安全保障体系能力成熟度模型中，会有对每个层次的不同级别的关键指标、标准流程的详细定义和描述，同时会有能力不足的措施说明等。

IT 安全保障体系能力水平，包括四大体系的能力成熟度因素：

（1）策略体系：安全策略相关的企业安全战略、安全滚动规划、安全建设资金投入、安全资源保障的健全程度。

（2）组织体系：安全组织和人员配置程度，安全组织的运作和执行效能，全员安全素质水平，对人员的安全管理水平。

（3）运作体系：围绕 IT 系统生命周期，从设计、建设和运维几个层面执行安全管控的规范化和标准化程度，安全管理的成熟度和水平。

（4）技术体系：针对安全技术保障措施和防护手段的建设完善程度。

评估能力成熟度主要依据目前的能力状态是否达到规定的要求而进行划分，能力不达标则能力成熟度低，反之则高。因此，评估模型对 IT 安全保障体系能力成熟度划分等级进行分值评估，在每个层次的能力成熟度模型中有详细的关键指标，还有详细的标准流程和活动指标，再根据指标的等级和关键程度可以设置权重，最后再计算总分。最后，针对所有的关键指标或者所有的标准指标的累计分数整个 IT 安全保障体系能力成熟度进行总分评定，成熟度评估具体执行中将采取调查、调研、访谈、效果跟踪等方法进行。

2.2　计算方法

（1）体系成效考量计算方法

IT 安全保障体系的建设成效= 安全策略体系水平*α +安全组织体系水平*β +安全运作体系水平*γ +安全技术保障措施建设水平*δ 。

α 、β 、γ 、δ 分别表示 IT 安全策略体系、安全组织体系水平、安全运作体系水平和安全技术保障措施建设水平的重要性赋值所占的权重，其中 α ≥0，β ≥0，γ ≥0，δ ≥0 且 α +β +γ +δ =1。

（2）体系水平成熟度计算方法

安全策略体系水平=α 1*策略指标项 1+α 2*策略指标项 2+α 3*策略指标项 3+α 4*策略指标项 4+… …。

其中，α 1、α 2、α 3、α 4 等分别为各个指标项的加权因子，　=1，安全策略指标项分值和权重因子数值由细则另行定义。

其余三个能力指标安全组织体系水平、安全运作体系水平和安全技术保障措施建设水平成熟度计算方案以此类推。

（3）体系成效考量评价矩阵

针对 IT 安全保障体系建设成效，建立 IT 安全保障体系成熟度衡量标准和指标，具体如表 1 所示。

3　安全能力评估实践

在以上安全能力成熟度模型基础上，通过建立一套可操作的能力达标评价标准-安全基线（Security BaseLine），考量 IT 安全保障体系建设成效，实现保障体系水平真正可量化评价。中国电信 IT 安全基线考评方法描述了 CTG-MBOSS 系统最基本的安全要求，通过安全基线考核指标，实现对企业各 IT 系统安全建设成效和管理水平的动态管理，促进 IT 安全管理能力提升。

中国电信 IT 安全基线达标标准，从管理和技术两个维度对如何考察安全建设能力给出了详细的达标评比办法，将安全能力分为 C 级、B 级、A 级。分为组织架构管理、人员安全管理、运维安全管理、应用安全、主机安全、网络安全、审计安全管理七大项。一个完整的安全基线保障体系应该是将安全管理和安全技术手段相结合，通过各种安全管理制度、安全组织机构和安全运维制度等方面的建设，并在网络层、主机层、应用层采取各种安全技术手段建立多层保护的深度防御保障体系。从安全基线可操作性的角度出发，在安全管理层面应将组织架构管理要求、人员安全管理要求和运维安全管理要求等三部分作为 IT 系统安全的基线考评要求，在安全技术层面应将应用安全要求、主机安全要求、网络安全要求和安全审计要求等 4 部分作为 IT 系统安全的基线考评要求，通过建立健全 IT 系统管理与技术防护体系，逐步提升 IT 系统整体安全防护能力。IT 安全基线评分标准如图 2 所示。

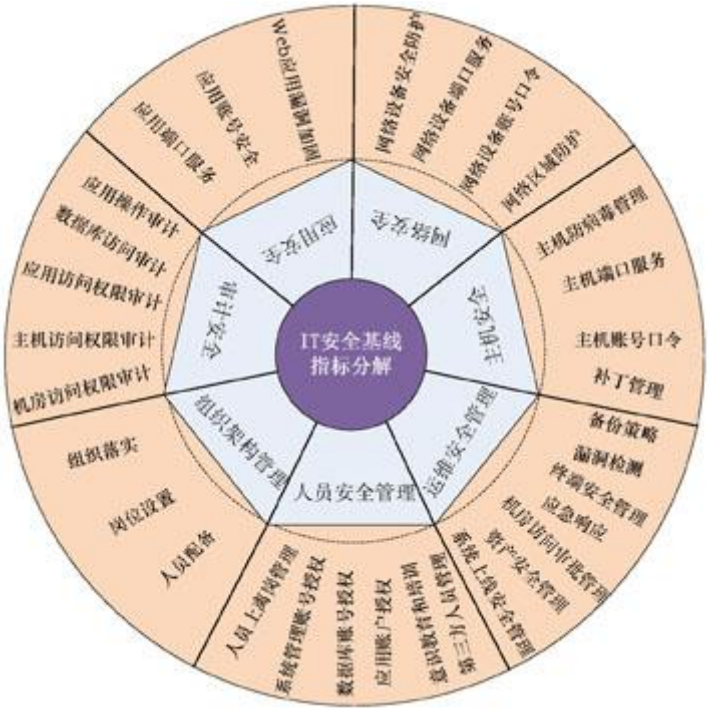

图 2　IT 安全基线指标分解示例图

在实际操作中，IT 安全基线达标测评采取打分的方式进行量化操作，对每一个检测项打分，属于判断结果为“是”或“否”的检测项，结果为“是”则评 1 分，为“否”则评 0 分。根据各项总分数对 IT 系统的安全评测结果分别进行等级化评定，IT 安全基线能力基线视图和判定方法如图 3 所示。

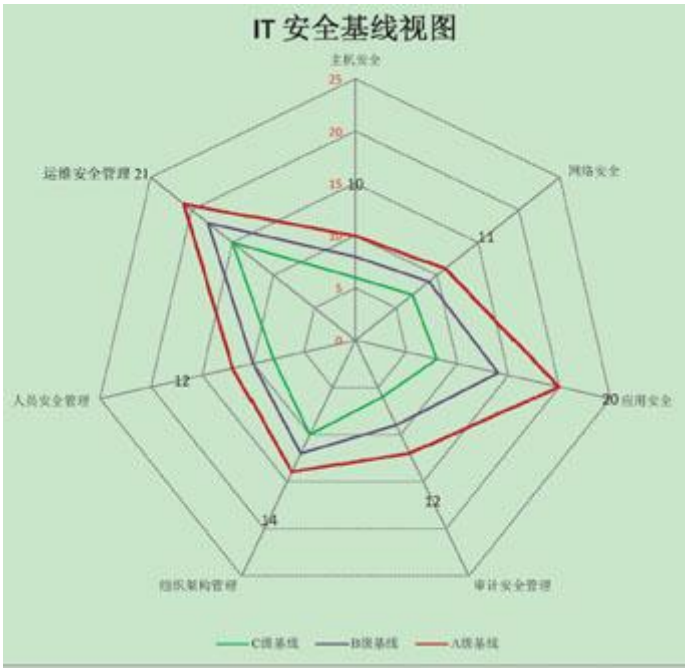


图 3　IT 安全基线达标考核示例图

图 3 中的连线为 IT 安全达标能力的基本水平线，也真正体现了能力“基线”的真正意义。

## 4　结束语

综上所述，本文在 IT 安全保障体系模型框架基础上，阐述了一个可持续改进的 IT 安全保障体系能力成熟度模型，从 IT 安全规划建设、运作、技术保障、管理措施等几个方面因素入手，找出一套合理的评价方法对安全保障体系建设成效进行公正有效的考量和评价，给出了一个具有普遍性的具体可操作的安全基线达标实践方法，可指导企业开展 IT 安全建设能力评价工作。