# **《信息安全体系的“术”》**

# **——标准主线与关联性**

## **前言**

所谓“术”，就是一种知识，一种经验。而信息安全体系的“术”，顾名思义，就是信息安全体系中的相关知识和经验。相关从业人员应该掌握信息安全体系的哪些知识，以及各个知识之间的关系呢？

《信息安全体系的“道”》

一般认为信息安全是加密/解密、安全协议、漏洞挖掘、渗透测试等具体技术。实际上，信息安全涉及管理、治理、人员、技术等多个维度，是一门非常宽泛的综合性交叉学科。正因为这个学科的宽度和广度均十分夸张，只要精通其中的一个维度，就足以在业界立足。但是，从多个维度去了解和学习信息安全，可以帮助我们更好地把握知识的脉络，从更体系化的层次去看待信息安全。

信息安全体系的“术”包括：

* 信息安全体系包含哪些领域？
* 这些领域相互之间有何关系？
* 信息安全术语和标准有哪些？
* 这些标准体现的知识有哪些？

本文暂时不涉及的内容是：

* “互联网时代”面临的信息安全新体系。
* 具体安全技术，如漏洞挖掘、渗透测试。

## **从信息安全的标准出发，把握信息安全体系**

一个核心问题：什么是信息安全？

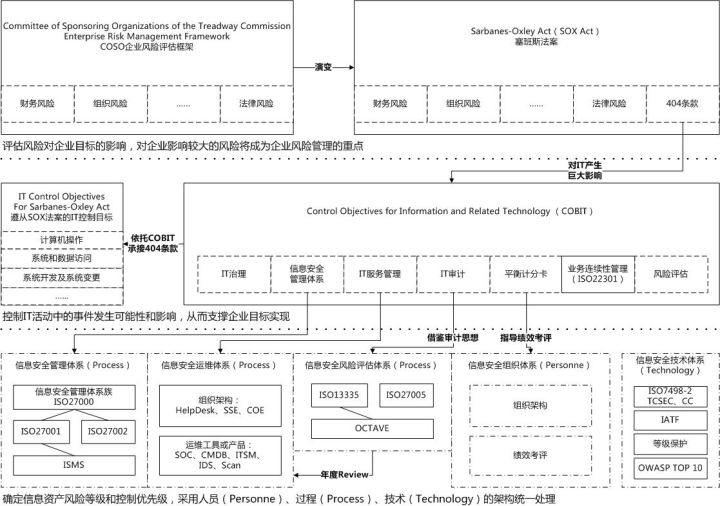
* 做理论的人会说，信息安全就是密码学、安全协议、隐私保护；做技术的人会说，信息安全就是漏洞挖掘、渗透测试；
* 做体系的人会说，信息安全就是行业标准，管理体系。

信息安全包含了上述各个方面：有技术层面、管理层面、人员层面等。实际上，各个相关标准或多或少都会提到“安全”或者“信息安全”这类关键词。在深入信息安全具体知识之前，了解信息安全体系的最好方法就是从标准出发。我们首先考察标准的诞生及其生命周期，通过剖析标准的演化过程，形成信息安全体系。

在给出信息安全相关标准的演化过程之前，我们首先要强调3个关键点。在讲解标准演化过程之时，我们也会不断强调这3点。在实际应用这些标准的时候，也需把握住这3个核心点，从而正确理解和使用标准：

* 标准与标准之间是相互渗透和包含的。任何一个好的标准经过不断地完善、改良、更新后，都会形成体系和框架，并且在其生命周期中逐渐与其他标准进行融合。（注：标准也是业界最佳实践的沉淀，能够代表大多数行业内的应用实践。同样的，标准也是针对业界常遇到的问题的，统一解决方案的参考内容，是应用科学方案的实践总结，是经验快速复制的有力手段。）
* 标准不是绝对的，是可以修改的。标准自身也承认其可修改性，并允许在应用过程中对标准本身进行添加、裁剪和修改。这种修改可能是标准自身的版本更新，也可能是企业根据实际需求对标准进行修改。
* 标准可以互相借鉴和映射。我们可以把标准和法律进行类比。在以《宪法》为代表的法律中，一般并不指明具体的量刑依据和处罚措施，而是通过《刑法》等细节法律法规，或具体案件的解释来执行法律。信息安全中的标准也是这样的。一般来说，具体的应用流程为：标准-->管理制度和流程-->技术要求-->解决方案-->产品和具体技术实现。

信息安全领域相关的主线标准通过用一个总体框架图来描述概念、标准之间的联系。目的是讲清楚各个标准和其引出“术”之间的关系。整个框架图分为上、中、下三个层次。第一层为企业内部风险控制；第二层为信息技术（Information Technology，IT）风险控制、第三层则是信息安全体系。这三个层次从上到下依次细化，最终落实到信息安全的管理和风险控制上。



## **第一层：企业风险评估**

一个企业在运行和发展过程中要面临很多的风险。所以，各个企业的CEO真不是躺着挣钱，企业时时刻刻都面临着巨大的风险。比如：

* 财务风险。企业高层为伪造财务指标，指示财务人员对营业额、利润等进行虚假性处理。
* 组织风险。董事会没有监管机制来监管总经理是否正确执行了所赋予的职责，导致总经理可以直接利用个人权利以公谋私，对企业造成伤害。例如，郑州亚细亚商场在1990-1995年是一家非常成功的零售连锁集团。然而，由于其内部控制薄弱，存在组织风险，最终成为亚细亚集团倒闭的一个主要原因。
* 法律风险。指企业运行时可能违反法律法规而造成的损失。比如由于“嘀嘀打车”的商标已被一家杭州公司注册，如果继续使用这一商标的话，会引发法律风险。因此，才有现在的“滴滴打车”，这并不是错别字。
* IT风险。当企业规模变大后，企业的IT化会成为一种必然。然而，IT化在给企业带来运行、管理便利的时候，也会引入风险。别有用心的财务人员可能会利用财务IT系统的逻辑处理等漏洞，直接修改财务金额或者指标，从而引发风险。

如何去精确定位企业的各种风险，并对这些风险进行控制呢？这实际上是全球任何一家企业都面临的一个严峻问题。企业内部风险控制有一个权威标准，是由Committee of Sponsoring Organizations of the Treadway Commission（COSO，美国反虚假财务报告委员会下属的发起人委员会）推出的，因此我们把这个权威标准也叫作COSO企业风险评估框架（Committee of Sponsoring Organizations of the Treadway Commission）。至此，企业可以根据这个框架准确地定位企业的风险，从而进行有效的规避。

COSO企业评估框架很不错，企业可以用它来正确定位和识别风险，并采取相应的措施改进。但是，COSO企业评估框架只能被动地定位和识别风险，无法高维度地打击风险。

这里面还有个小故事。安然公司倒闭的原因是财务问题。而负责安然公司财务审计的公司是当时世界著名5大审计所之一的安达信公司，这个公司在财务审计时，恶意销毁了审计档案。由于此事件的揭露，安达信公司最终也走向了倒闭。世界著名的5大审计所，就变为了现在的4大审计所了。安达信公司后来转型成为了现在业内著名的IT咨询公司埃森哲。

（Sarbanes-Oxley Act）2001年，美国最大的能源公司之一安然公司，突然申请破产保护。此后，上市公司和证券市场丑闻不断。2002年6月，世界通信公司会计丑闻事件，使得投资者对资本市场的信心遭受了巨大的打击。这些事件暴露出公司和证券监管的诸多问题。为了解决此类问题，美国国会于2002年7月25日正式通过《Sarbanes-Oxley Act》，即《塞班斯-奥克斯利法案》（简称《SOX法案》），在公司治理、会计职业监管、证券市场监督等方面做出了许多新的规定。

《SOX法案》的亮点之一，就是提出了对公司高层主管及白领犯罪的刑事责任。至此，企业风险的责任追溯中增加了刑事责任，加强了企业风险管理的能力。

SOX法案同样规定了财务风险、组织风险、法律风险等。COSO中的风险基本都能与SOX法案中找到对应。

SOX法案对于后来的信息安全风险管理起到了两个重要的借鉴作用。

追溯刑事责任。SOX增加的刑事责任追溯启迪了信息安全风险管理与刑事责任的关联。因此，在面临黑产等计算机相关攻击时，政府会出台相应的法律，规定了针对计算机犯罪的相关刑事责任。

404条款。这一条款指出了IT的相关要求。而这个要求，就与IT和信息安全产生了关系，促使了后面相关标准的诞生。

（Sarbanes-Oxley Act）第8至第11章主要是提高对公司高层主管及白领犯罪的刑事责任：

* 针对安达信毁审计档案事件，制订法规，销毁审计档案最高可判10年监禁，在联邦调查及破产事件中销毁档案最高可判20年监禁；
* 强化公司高管层对财务报告的责任，公司高管须对财务报告的真实性宣誓，提供不实财务报告将获10年或20年的刑事责任。

## **第二层：IT风险评估**

SOX法案的404条款指出了IT技术审计的相关要求。然而，这个要求实在是太简单，以至于人们没办法落实这个要求。这个要求有多简单呢？请看404条款中，a(1)和a(2)两句话，这两句话就是与IT相关的要求。

写的倒是挺高大上的，但这也太高大上了，没办法落地实施吧？实际上，在SOX法案出台以后，业内也在寻找一个可以落地执行的相关标准。最终，业内终于找到了这个标准，就是IT风险中最为经典的框架：COBIT框架。

a(1)：强调公司管理层建立和维护内部控制系统及相应控制程序充分有效的责任；

a(2)：发行人管理层最近财政年度末对内部控制体系及控制程序有效性的评价；

COBIT框架非常经典，可以说，IT风险中可能遇到的所有问题的风险处置问题，在COBIT中都能找到相应的答案。

2012年，ISACA已经推出了COBIT 5版本。但是，COBIT 4是学习COBIT很好的一个框架。如果想学习COBIT的话，建议先学习COBIT 4版本。这是因为，COBIT 4版本的逻辑非常清晰，而COBIT 5在COBIT 4的基础上进一步进行了融合。如果直接学习COBIT 5的话，会缺少很多必要的背景知识和基础。

业界找到COBIT框架之后，都开始使用COBIT作为SOX法案IT风险方面的承接框架。然而，虽然所有的具体标准都从COBIT中裁剪得到，但是各方对于问题的理解和对COBIT的裁剪方法都有所不同，没有形成统一的标准。后来，ISACA作为COBIT的推出方，专门裁剪、定制出了一个适合SOX法案的IT风险控制框架，这就是《IT Control Objectives for Sarbanes-Oxley》，即《遵从塞班斯法案的IT控制目标》。这一框架中，增加了我们熟知的变更控制、计算机病毒防治等多种具有IT特色的风险控制项。

（COBIT）COBIT的全称为Control Objectives for Information & related Technology。它是一系列关于IT管理最佳实践（框架）的集合，由美国信息系统审计与控制协会（Information Systems Audit and Control Association，ISACA）和IT治理委员会（IT Governance）于1992年创建。

COBIT作为IT风险控制框架，用来控制IT活动有可能影响企业目标的潜在事件可能性及其影响程度。实际上，企业在执行任何决策和行动之前，都需要对风险进行识别，这就是前面说到的企业风险内部控制，如财务风险、组织风险等。当企业的目标依托于IT目标，由IT目标支撑时，就需要对IT进行风险识别。COBIT就是用来对IT相关项进行风险识别的框架，如IT环境有无风险，IT决策架构有无风险，IT服务有无风险，信息安全有无风险等。注意，我们常见的信息安全属于IT风险中的一类。业内有些人也会混淆这两个概念，把IT风险和信息安全风险混在了一起，这是不准确的。

COBIT中指出了IT中的多种风险和管理方法：IT治理、信息安全管理体系、IT服务管理、IT审计、平衡计分卡、业务连续性管理、风险评估等等。而信息安全管理体系最终得到展开，映射到第三层。接下来，我们在第二层谈一谈除信息安全管理体系之外的几个重要的管理体系。

* **IT服务管理。**IT服务管理可以认为就是信息技术基础架构库（Information Technology Infrastructure Library，ITIL）。IT服务管理的目的是让公司的内部员工方便、舒适地使用IT服务。举个例子，HelpDesk，即桌面运维。为了让内部员工感受好这个服务，IT服务管理会明确出服务目录，如提供操作系统重装服务、硬件维修服务、数据备份服务等；明确出服务等级协议（Service Level Agreement，SLA）承诺，如首次电话接通率95%，首次服务故障解决率80%等）；明确出问题管理，如公司标配软件和个人常用软件冲突时，采用常用软件库来规避。当然，IT服务管理还包括更大层面的运维管理，如变更管理、容量管理等。
* **IT审计。**IT审计要使用一定的审计方法，帮助企业在各个维度进行风险识别时，能够应用审计的架构和理念，帮助企业规避此类风险。比如，IT服务管理中变更管理引发了风险。而IT审计就通过审计方法，具体告知企业变更管理的哪些方面做的不够。这里要注意的是，IT审计和风险评估有一点区别。风险评估依据经验，没有固定的标准；而IT审计由于是由财务审计脱胎而来，因此其具有严格的标准，希望通过逻辑化的、可重复实现的电子证据来证明现状与标准之间的差距。在进行IT审计时，需要按照标准和实际情况进行一一比对，依托可复现的证据具体定位风险和问题。
* **平衡计分卡。**在执行相关规定和措施时，很重要的一点就是确认这些规定和措施是否能够正确、有效地执行。而监督执行所使用的方法一般就是平衡计分卡，换个大家都熟悉的词就是绩效考核。平衡计分卡是比财务审核更加优化、更加领先的一种考核方式。以前，衡量企业或个人的方式很简单：财务。只要企业财务好，收入高，大家的绩效考评就都会高；反之，财务情况不好，收入低，那么大家的绩效考评就都不高。与之相比，平衡计分卡提出，考核项不仅仅取决于财务考核，还应该有20%-30%来自于其他地方，如团队能力建设、流程优化、客户服务等。从各个维度对员工进行综合评估，这样才可以使绩效反应出更加准确的信息，更有利于组织的长期发展。
* **业务连续性管理。**业务连续性指企业有应对风险、自动调整和快速反应的能力，以保证企业业务的连续运转。我们熟知的信息安全，可以防止黑客入侵、防止数据被恶意删改等，可以降低风险。但是，企业不可避免地面临自然灾害等非人为因素的影响，导致不可预估的后果。规避此类风险，就需要依靠业务连续性了。举例来说，911事件发生时，位于美国纽约世贸双子星大楼的国际金融服务公司摩根斯坦利的核心机房也被炸毁了。但是，1天过后，摩根斯坦利的服务业务得到了恢复，重新面对全球开放。这是因为摩根斯坦利遵从了业务连续性管理，花费资金构建了同城、甚至异地的容灾机房。业务连续性管理现在可以与ISO22301标准划等号了。ISO22301给出的是业务连续性框架，规定了很多管理要求，如定期演练、容灾团队建设、容灾机房建设等等。实施ISO22301，还需要应用具体的技术实现。比如，为了提高业务连续性，网络公司的主数据中心通过核心路由器、核心交换机、高速冗余光纤，通过上百兆异地异步传输，实现了异地容灾机制。这就是ISO22301和具体技术相互依托、相互指导的例子。
* **风险评估。**一方面是IT风险评估，另一方面也包括信息安全风险评估。

COBIT之所以堪称经典，是因为COBIT基本上覆盖了业内的所有IT风险。举个简单的例子，我们来看一看中国银监会颁发的《商业银行科技管理风险指引》这一监管性文件（商业银行信息科技风险管理指引）。这一监管性文件主要规定了商业银行所面临的信息科技风险。下面是此文件的目录：

因此，可以 依据COBIT框架，根据不同的场景制定不同的规范。只要处于IT层面的风险控制和管理，基本可以确定脱离不了COBIT框架。可以这么说，熟用COBIT，走遍业内都不怕！

第一章 总则

第二章 信息科技治理 //对应COBIT的IT治理

第三章 信息科技风险管理 //对应COBIT的风险评估

第四章 信息安全 //对应COBIT信息安全管理体系中的信息安全

第五章 信息系统开发、测试和维护 //对应COBIT信息安全管理体系中的安全软件开发流程

第六章 信息科技运行 //对应COBIT的IT服务管理

第七章 业务连续性管理 //对应COBIT的业务连续性管理

第八章 外包 //对应COBIT信息安全管理体系中的外包风险控制

第九章 内部审计 //对应COBIT中部分提到了审计

第十章 外部审计 //对应COBIT中部分提到了审计

第十一章 附则

**注意，唯一的例外是互联网场景。在互联网场景中，需要其它的框架进行衔接。在这里不涉及互联网环境的信息安全体系。**

## **第三层：信息安全体系**

讲完COBIT，我们落到第三层：信息安全体系。信息安全体系进一步细分，会有很多相关的标准和框架。我们一般认为，要首先确定信息资产风险等级和控制优先级。

**1、信息安全风险评估体系**

在COBIT里面已经提到了IT风险评估，但在第三层中又单独提到了信息安全风险评估，是否有些多余？实际上并不是这样。风险评估最能体现标准与标准之间相互借鉴、相互包容的特点。风险评估是一个逐渐借鉴和向其他标准融合的过程。在最初，业内遵循ISO13335的风险评估方式，即：风险值=资产\*威胁\*脆弱性。后来，在企业内部风险控制层面就不提这种风险评估方式了，而是提出：风险值=影响\*发生可能性。随后，ISO27005也开始提出类似的观点。任何标准如果想做到使用方便、影响力大，则在版本更替和扩充的时候，都会逐渐形成大的标准，达到四通八达，与其他标准互相映射的状态。因此，标准与标准之间会逐渐形成大融合。

现在，**信息安全风险值=影响\*发生可能性**。这种关系与原先的风险值=资产\*威胁\*脆弱性有什么联系呢？实际上，影响=资产\*脆弱性；发生可能性=威胁\*脆弱性。假设我口袋里有100元钱，这100元钱就是**资产**；小偷是**威胁**；口袋开了个大口子就是**脆弱性**。

* 小偷看到了口袋里面有100元，且口袋的口子打开的很大，那么小偷就很容易偷走钱。此时，**威胁**和**脆弱性**都很大，也就是**发生可能性**很大。
* 小偷虽然在我旁边，但是他没看到我口袋里有没有钱，而且我口袋也封闭的很好。此时，**威胁**仍然存在，但**脆弱性**很小，所以**发生可能性**很小。

而**影响**是，100元与脆弱性结合起来，对我实际业务影响有多大？有的人会认为，丢了100元也无所谓，**影响**不大；有的人会认为，这几天的饭钱就靠这100元了，**影响**很大。将**影响**和**发生可能性**结合起来，就是风险值了。

通过上述方法，我们就计算得到了信息安全风险值。对于一个企业来说，想改进信息安全的话，改进点会非常多，投入是无止境的。因此，如果要对企业的信息安全实施改进，需要考虑优先级和重点。信息安全风险评估就是来确定优先级和重点的。比如一个O2O企业，它显然会面临黑客攻击的风险，但同时也面临个人隐私数据泄露的风险。通过风险评估，企业可能会认为个人隐私数据泄露的风险要大于黑客入侵的风险。因此，企业会优先改进个人隐私数据保护方法和措施。

前面已经提到了，信息安全风险评估有2个标准，一个是ISO13335，一个是ISO27005。然而，这两个都是标准，如何具体实施呢？OCTAVE是来指导企业实施信息安全风险评估的实施指南文件。

风险评估自身应该按照年度执行。但是，互联网企业的风险评估方式会有所不同，操作方式也会有所不同。在此就不展开论述了。再未来的专栏文章中，我们会详细分析适合互联网企业的信息安全体系。

确定信息资产风险等级和控制优先级后，一般采用人员管理（Personne）、过程管理（Process）、技术管理（Technology）的架构进行处理。这三大架构简称为PPT架构。一些企业，如华为，会将运维单独列为第四大方面，这并不矛盾。下面，我们按PPT这三大方面初步讲解信息安全体系。

**2、信息安全组织体系（Personne）**

在实施信息安全管理、技术和运维体系前，首先应该构建信息安全组织体系，应该具备专门的信息安全组织。然而，除了像华为、阿里等大型公司之外，中国很少有企业具备独立的信息安全组织，而是从网络部门或者运维部门划分出一个部门作为信息安全组织。这种情况下，信息安全组织的权威性会较弱，不利于实施信息安全管理、技术和运维体系。

当建立起信息安全组织后，应该协调好组织与组织、人员与人员、组织与企业高层之前的关系，同时梳理相关的资源。这不仅仅涉及到能力和技术，还涉及到相关人员的水平。在有些公司，信息安全组织具有高度的权威性，可以随意与企业高层之间面对面交流。信息安全组织下达的指令会得到严格的执行。但也有公司，信息安全组织的权威性较差，并需要承担具体的工作和任务。此时，人员考评、技术部署等都会推动的很慢。

在安全人员管理方面，应该与其他部门相同，明确人员职责、明确考评方式、进行人员背景调查、执行相应的人员控制。在实施比较好的情况下，还应该注意人员的内部控制、人员的能力提升等，应该给安全人员一个成长的空间。

**3、信息安全管理体系（Process）**

信息安全管理体系的落实就是ISO27000标准族了。相信安全从业人员都会或多或少听说过ISO27000。但是在业内，有些人会把ISO27000、ISO27001和ISO27002混淆。我在这里想强调一下：

* ISO27000是一个标准族，里面包括认证、指导实施指南、度量、风险评估、通过认证机构的标准等等。
* ISO27001具体提出了对组织的信息安全管理能力进行评估，以确定其是否满足组织自身的信息安全需求。可以说，ISO27001是一种认证标准。
* ISO27002是指导实施指南。我们一般说，一家企业按照ISO27002进行了相应的建设。

ISO27000标准族作为一个成熟的信息安全管理体系标准，也具有向其他标准借鉴，与其他标准融合的特点。比如，ITIL中也提到了信息安全，其中指出：信息安全管理可以参考ISO27001。再比如，ISO27001中也提到了COBIT中的业务连续性，可以参考ISO22301进行实施。

**4、信息安全技术体系（Technology）**

新版本的ISO27002中包含了14大安全域，包括通信安全、访问控制、业务连续性、信息安全组织、物理与环境安全、人力资源安全等。我们现在有了安全管理体系，如何实施技术落地呢？举个例子，假设访问控制有如下管理要求：

* 办公区不能直接访问生产区；
* 访客区不能访问内部办公区；
* 测试区不能直接向生产区上传数据；
* 生产数据传入测试区时，应当进行脱敏处理。

规定了具体要求后，就需要进行技术改造。首先是安全域划分，根据不同的功能和不同的安全属性划分不同的区域。然后才涉及技术项目。再往后是技术测试等。因此，具体技术实际是按照管理要求落实的。

讲到技术项目，就涉及到信息安全技术体系了。由于技术实现手段很多，现在业内已经不太流行提出技术体系标准了。因此，在图中我们把技术体系单独放在最右侧。

* **ISO7498-2：**最早的技术体系标准，于1980年发布，现在基本已经不再使用了。
* **TCSEC：**大家应该听说过操作系统的安全分级，如Windows 95属于D级安全系统，Windows 98属于C级安全系统等，这就是TCSEC给出的。这个标准现在也基本不再使用。
* **CC：**通用测评准则，指出系统开发时需要满足哪些安全功能，现在还有一定的使用率。
* **IATF：**80年代美国国防局使用的标准，在2000年发布。这个标准中首先提出了安全域的划分；提出了域与域之间的控制；第一个提出了人员、流程、技术，即PPT三防一体的纵深防御理念。虽然IATF现在已经不再流行，但是它对整个信息安全界的影响还是非常深远的。
* **等级保护：**是由中国公安部、国家保密局、国家密码管理委员会办公室、国务院信息化工作办公室联合推动的中国信息安全标准，其中技术要求指导了物理安全、网络安全、主机安全、应用安全、数据安全五个层面的技术方向。
* **OWASP TOP 10：**Open Web Application Security Project（OWASP）中发布的Web 10大安全风险（[OWASP](https://link.zhihu.com/?target=https://en.wikipedia.org/wiki/OWASP" \t "https://zhuanlan.zhihu.com/p/_blank)）。这是现在比较流行的Web安全风险点，不能算是一种标准。OWASP会定期更新10大安全风险，并给出相关的标准、书籍和工具。

技术标准进一步落地就是技术方案。举个例子，信息安全管理体系要求生产区和办公区之间不能随意访问。因此，我们提出了相应的技术隔离措施和要求：使用跳转机进行跳转；跳转机本身具有审计功能；审计达到50天；可以审计图形化操作和命令化操作，等等；随后，需要针对技术要求提出相应的解决方案，由产品完成具体实现。

**5、信息安全运维体系**

除了PPT外，有的企业还会将信息安全运维体系作为独立的体系。在业内，华为公司是实现安全和运维紧密结合的杰出代表。因为华为的运维配置管理数据库（Configuration

Management Database，CMDB）信息非常准确，准确率高达98%，把安全变更、IP地址滥用、特权账号管理、安全事件等都通过CMDB实现自动化运维，这是一个非常了不起的事情。举个例子，一个服务器上线时，必须要在CMDB中执行上线流程，否则CMDB会发现没有遵守上线流程而报警，并关联绩效。按照上线流程申请后，会自动向CMDB申请IP地址，开通安全策略等安全卡点。当服务器IP地址需要改变时，也需要在CMDB中进行申请变更。审批通过后，对应的安全策略会自动调整为最新的IP地址策略。当服务器下线时，CMDB会自动化地关联删除安全策略，避免安全策略空载。可以说，华为是信息安全运维体系的业界标杆。

## **总结**

至此，标准主线与相互之间的关联性就介绍完毕了。如果上述标准可以做到融会贯通的话，那么你就能够成为信息安全体系建设方向的专家了。