* P2：

信息安全测评不是从事神秘的hacker工作

* P3:

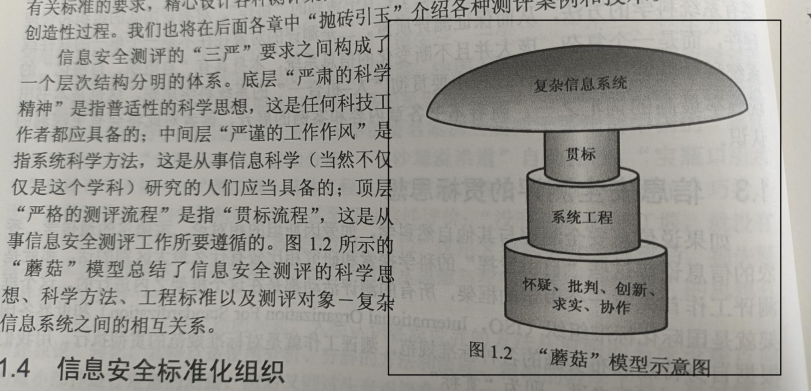
”怀疑，批判，创新，求实，协作”是一名科学工作者必须具备的科学素养，同样也是指导我们进行信息系统安全测评的基本精神与思想

* P5：

如果说**信息安全测评与其他自然科学**，如爱因斯坦的相对论、孟德尔的遗传学、香农的信息论等这些“自由发挥”的科学探索和研究相比较有什么**最大区别**的话，那就测评工作首先有一个限定的框架，所有的测评活动都是在这个框架之内进行的。这个架就是国际化标准组织(ISO, International Organization For Standardization) 和世界各国根据自身特点颁布实施的各种标准规范。**测评工作就是对标准规范的贯彻执行，用我这行的“行话”来讲，即为“贯标”。**

* P6：

信息安全测评的“三严”要求之间构成了一个层次结构分明的体系。底层“**严肃的科学精神**”是指普适性的科学思想，这是任何科技工作者都应具备的;中间层“**严谨的工作作风**”是指系统科学方法，这是从事信息科学(当然不仅仅是这个学科)研究的人们应当具备的;顶层思林贯帕“**严格的测评流程**”是指“贯标流程”，这是从事信息安全测评工作所要遵循的。



* P8：

成立于2001年的**全国信息安全标准化技术委员会（CITS）**负责全国信息安全技术领域以及与ISO/IEC JTC1 相对应的标准化工作

* P13：

此项工作由美国国防部牵头组织实施，历时十余年，于1985年12月正式公布，名为“可信计算机系统评价准则”（**TCSEC**,Trusted Computer System Evaluation Criteria）,也就是俗称的**“橙皮书”：全球计算机系统安全评估的第一个正式标准，具有划时代意义**。

* P15：

西方划级：**与我国划级的区别**

**(1)基础，**。

**(2)粒度，**。

**(3)费效比，**

我国划级：

按计算机信息系统遭受破坏后给**个人、机构、社会和国家**带来的不同影响程度，将信

系统安全等级划分为 5 个不同的安全级别。5个级别分别是什么？

* P17：

安全域是将一个大型信息系统中具有某种相似性的子系统“聚集”在一起。目前，中国划分安全域的方法归纳起来大致有资产价值相似性安全域、业务应用相似性安全域、安全需求相似性安全域和安全威胁相似性安全域4 种。

资产价值相似性安全域(security zones with similar information assets)，指同一

安全区域内的信息资产应具有相近的资产价值。

例如，一个信息系统的数据中心往往是该系统最重要的子系统之一，各类数据服务

器具有类似的资产价值，可以将它们划入同一个安全域。

**业务应用相似性安全域(security zones with similar business applications)，指**

**同一安全区域内信息系统的业务应用或系统功能相似。**

例如，一个银行的各个支行，其信息系统的业务应用均非常相似，也可以将其划入

同一个(纵向广域) 安全域。

安全需求相似性安全域 (security zones with similar security requirements)，指

同一安全区域内的信息资产应具有相似的机密性要求、完整性要求和可用性要求

例如，国家重要政府部门的办公系统，在安全需求方面具有相似性，也可以将其划

个(横向广域) 安全域。

安全威胁相似性安全域(security zones with similar security threats)，指同一安

全区域内的信息资产应处在相似的风险环境中，面临相似的威胁。

例如，各个企事业单位的门户网站均面临来自 Intermet 的安全威胁，可以将其划入

个独立的安全域。

* P18：

信息安全测评 (testing and assessment of information security)，指测评人员在系统工程思想的指导下，遵照国家有关标准、规范和流程，通过设计各种测评案例，对一个信息系统的安全性能和功能进行“标准符合性”论证的过程。

* P19：

信息系统安全测评四个阶段：

(1)**设计阶段**:当规划、设计一个信息系统的时候，安全测评工程师应当积极参与规划设计部门的工作，根据国家有关标准，特别是根据信息系统安全等级保护标准对这个信息系统的重要性提出安全评估意见，如可以针对这个系统的重要性(即它遭受破坏后带来的影响)来事先确定它的安全等级。

(2)**建设阶段**:当这个信息系统的设计蓝图通过有关部门的评审之后，安全测评工程师应当监督该系统的建设过程是否满足国家有关标准。更为重要的是，在系统建设完成之后，应当根据国家标准对其是否达到建设目标进行测评验收。例如，一个信息系统当初设计的时候是按照第 3 级安全标准进行建设的，那么进行验收时就应该按照这个等级进行测评验收。

(3)**运行维护阶段**:经过测评验收之后，系统进入正式运行维护(简称运维)阶段。安全测评工程师将定期或不定期地对系统进行例行测评。这一阶段相对较长(如同人的生长过程)，而且往往伴随着系统内部功能的不断延伸和完善，所以需要进行常态性的测评，并且在系统发生安全事故的时候进行及时响应 (参见本书“应急响应”一章)。

(4)**废弃阶段**:当该系统确实不堪所用的时候，安全测评工程师需要对它进行最后的测评。读者可能会认为这个环节多此一举。那么请设想一下这种情况吧:一个企业至关重要的商业秘密是否需要按照特定规程进行转移或销毁?当然，这个环节对事关国家安全的重要信息系统更为重要，在信息时代，其重要性甚至不亚于对退役核导弹和核废料的处理，只不过没有那么危险而已。

* P20：

**内网**是指那些与internet（公网）之间采取了“可靠的技术隔离手段”的企事业机构专用网络，如政府内部办公网络，银行内部OA系统，企业财务信息系统等。

**外网**是指那些与internet相连（应该有一定的安全防护措施）并向外提供服务的企事业机构的专用网络，如政府对外服务系统，政府门户网站，网络银行，社保网和校园网等

* P22：

综上所述，在内网安全测评中需要注意以下3 个问题:

**(1)内网安全模型测评。**对内网及其各个子系统的安全设计方案和建设、运行维护

情况进行“符合性”测评。该项工作的重点是测评各个子系统或安全域的等级划分是否

符合国家有关标准要求和设计要求。

**(2)内网安全技术测评。**按照国家标准对内网中各种型号的安全设备、服务器、网

络设备和终端进行技术测评。

**(3)内网安全管理测评。**按照国家标准对内网的各种管理制度、管理人员和管理机

构进行测评。

* P22：

第一种是所谓的“**委托测评**”形式，由专业的信息安全测评人员组成。第二种是所谓的“**自测评**”形式，主要人员由本单位的技术人员组成(如本单位信息中心的人员)。

* P27：

制定安全测评的工作计划时，需要注意的要点

1. 测评依据。该部分主要是罗列此次测评活动中所依据的国家标准以及参照的其他相关标准

* P36：

数据安全始终是信息安全最本质最核心的部分

数据不能多也不能少--完整性

数据安全的三个属性：**完整性（integrity），保密性（confidentiality），可用性（availability）**

* P37：

国家标准中要求信息安全测评工程师使用访谈 (“闻”与“问”)、检查和测试(“望”和“切”)这三种方法进行测评。下面给出“访谈”“检查”和“测试”的定义。

* P37：

无损测试：也就是不能影响被测系统正常工作，也不能留下任何后患

* P38:

数据安全访谈调研过程主要是测评工程师与被测信息系统的各级管理人员、技术人员和数据使用人员进行**问卷式的访谈**。访谈的内容分为数据完整性、数据保密性及数据备份和恢复三大块。首先介绍国家标准中关于数据完整性、保密性和备份与恢复三个方面的访谈要求，然后通过一个**访谈问卷调查表**的形式来细化访谈内容。

* P63：

实际测评对象并非仅仅是一台冷冰冰的机器盒子，而是包括使用这台计算机的人在内的“人机合一”系统

* P63：

国家标准中把主机安全测评的数十项条款划分为“身份鉴别”，“自主访问控制”，“强制访问控制”，“安全审计”，“剩余信息保护”，“入侵防范”，“恶意代码防范”和“资源控制”8个环节

* P69：

对于第三级安全等级的主机而言，口令替换记录则应该显示出该被检主机至少**每月**进行一次口令替换

* P98：

每一台主机安全，由这些主机构成的网络不一定安全。

* P99

。网络安全测评要求中要关注的8个方面如下所述。

（1）结构安全与网段划分。热爱大海，梦想扬帆远航的读者可能知道各种舰船都有“水密舱／水密门”这样的结构，以防海水从破损的洞口涌入之后水漫金山。“结构安全与网段划分”的思想与此类似。不过这时“**既要防内又要防外**”。

（2）网络访问控制。

（3）拨号访问控制。

（4）网络安全审计。

（5）边界完整性检查。

（6）网络入侵防范。

（7）恶意代码防范。

（8）网络设备防护。

* P142

“信息高速公路”建设的基础设施——数据、主机和网络的安全测评。

* P143

应用安全的测评条款分为“身份鉴别”、“访问控制”、“安全审计”、“剩余信息保护”、“通信完整性”、“通信保密性”、“抗抵赖”、“软件容错”和“资源控制”9个环节。

（1）身份鉴别。

（2）访问控制。

（3）安全审计。

（4）剩余信息保护。

（5）通信完整性。

（6）通信保密性。

（7）**抗抵赖。**这是一个新的测评项。在法制社会中人类的“契约”活动是由具有法律效力的合同等“证据”来保障的。在虚拟空间中一样需要这种保障机制。

（8）**软件容错。**这也是一个新的测评项。“容错”是“防错”的手段之一。它要求应用软件系统具有较强的健壮性。

（9）资源控制。

* P182

在信息安全风险的定义中，“威胁”和“脆弱性”（也就是人们常说的漏洞）是相辅相成的，前者是产生风险的外因，后者是内因。对于风险的产生，两者缺一不可。

* P183

2008 年，国际标准化组织 ISO 风险管理工作组在制定相关标准的时候，在三十余个国家提出的风险定义中采纳了中国专家组提出的关于 “风险”的定义，即“风险是不确定性对目标的影响”（effect of uncertainty on objectives）。

* P183

信息安全风险（information security risk），人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件发生及其对组织造成的影响。

* P183

在信息时代，永远没有绝对的安全和零风险。人们能够做的是首先评估风险可能带来的影响，然后采用规避、转嫁和降低风险的方法，最后将风险控制在能够承受的范围之内。这就是风险评估最本质的思想。

* P184

资产（asset），即对组织具有价值的信息或资源，是安全策略保护的对象。

资产价值（asset value），即资产的重要程度或敏感程度的表征。资产价值是资产的属性，也是进行资产识别的主要内容。

* P185

资产识别是科学定级的主要依据。

* P219

威胁识别（threat recognition），指分析事故潜在起因的过程。

* P219

安全等级较高（4、5级）的核心信息系统。此时所有的资产都非常重要，需要进行安全威胁的逐一识别。例如，国家要害部门信息系统。

* P220

从可操作性的角度来讲，重点识别是风险评估工作的主要方法，符合“有所为，有所不为”的系统科学思想。

* P220

与资产识别类似，威胁识别分为威胁分类和威胁赋值两个环节。

* P222

归根结底，资产识别的结果是进行威胁识别的出发点和落脚点。

* P239

管理脆弱性有很多种，但大体上可以分为两类：一类是**结构脆弱性**，即信息安全管理体系不完备。第二类是**操作脆弱性**，“在其位不谋其政”，各种管理制度虽然完整，但并没有真正得到贯彻执行。在实际评佔过程中，一个单位往往既存在结构脆弱性，也存在操作脆弱性。

* P239

寻找、分析和度量脆弱性，是风险评估中最重要，也往往是最困难的环节。

* P240

脆弱识别分为脆弱性发现、脆弱性分类、脆弱性验证和脆弱性赋值4个环节。

* P242

（2）脆弱性的仿真验证。对于那些业务连续性很强的机构（如金融、电力等），建议测评人员选择仿真验证的方式。仿真验证还有一个好处就是可以“放开手脚”地进行各种破坏性、滲透性测试，从而尽量发现这些 CVE 对被测评单位业务的形响。

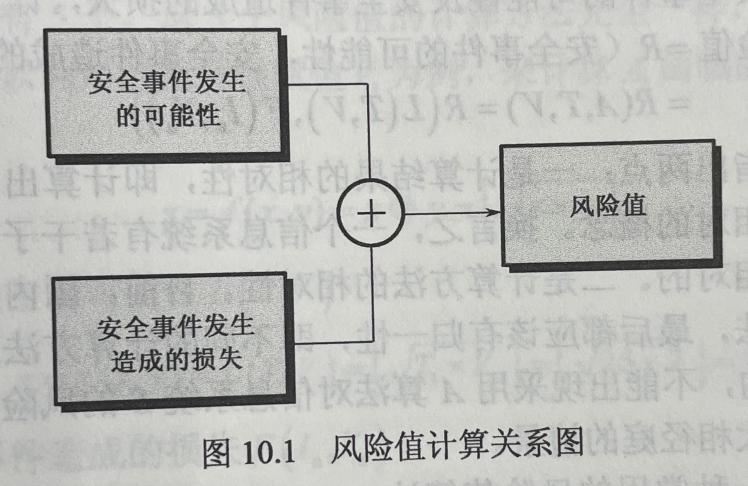
* P265

在信息安全领域（其实不仅仅是这个领域），风险分析与风险评估 (riskassessment）是两个等同的概念，经常可以互换使用。如果要说两者之间有什么“细微”的差异的话，那就是风险分析更学术化一点，如可能会给人一种更偏重分析方法研究的感觉；风险评估更工程化一点，强调整个评估过程的规范性和程序正确性。

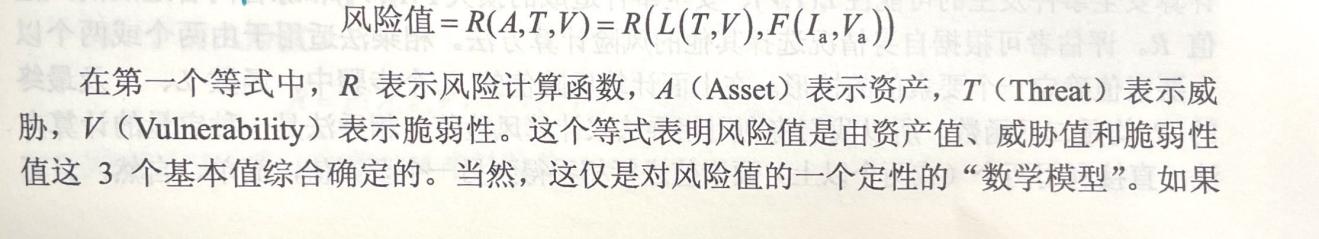
* P265

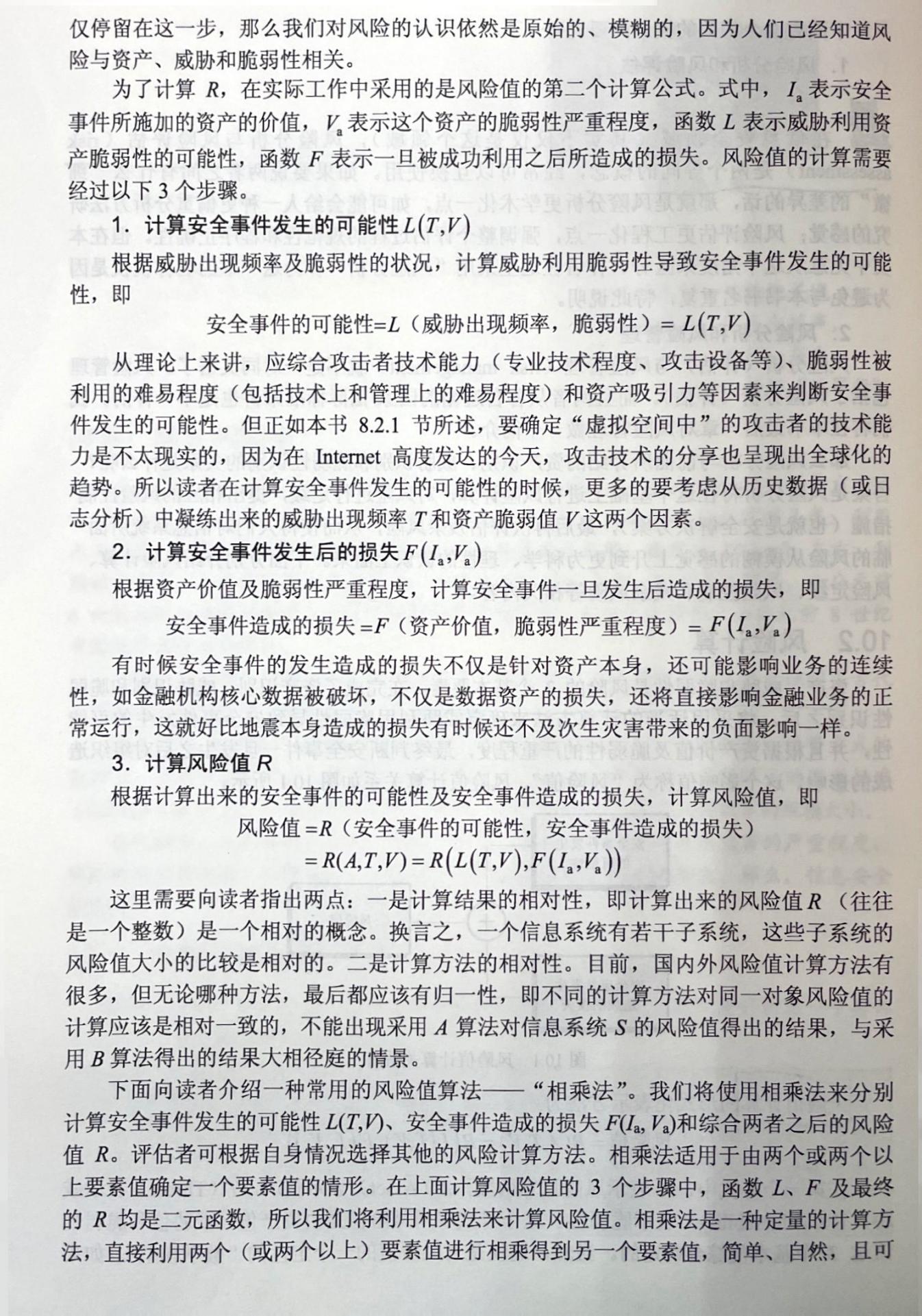
资产、威胁和脆弱性是风险的三个基本要素。

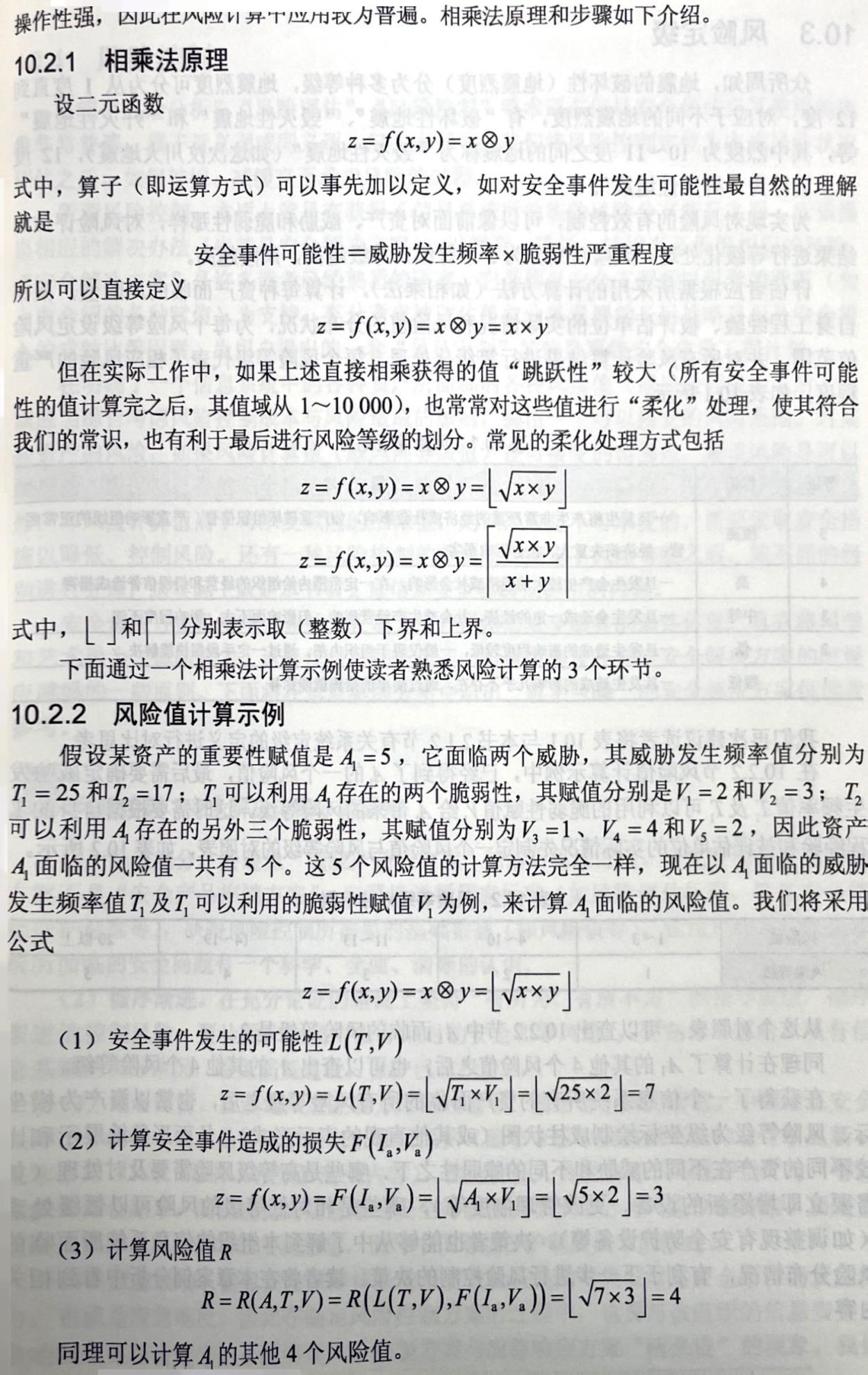
* P265



风险值计算的形式化表示方式为：







* P269

信息安全保障体系的最有效验证是面对突发信息安全事件的反应能力，也就是应急响应。因此在制定风险控制方案的过程中，也要与该组织的信息安全应急响应方案结合起来，不要出现风险控制方案与应急响应方案“两张皮”的现象。

* P270

从信息安全风险评估流程完整性的角度来讲，残余风险的评估是其中的最后一个步骤。

* P283

应急响应和风险评估是一个有机的整体。事实上，一个全流程的风险评估工作应当包括对组织的应急响应能力的评估。如果说两者之间有什么微小的差异的话，那就是风险评估注重的是组织“平时””的信息安全，是长期性的、渐变的：应急响应注重的是组织“战时”的信息安全，是短暂的、突发性的。请注意，这里没有使用“常态性”和“临时性”这一对词来区分两者之问的差异，因为我们认为无论是风险评估还是应急响应，从信息安全意识来讲，都应当是常态性的。

* P283

应急响应的基础是计划的准备，应急响应的依据是计划的编制，应急响应的核心是计划的实践。

* P284

俗话讲“计划赶不上变化”，如果不对应急响应的参与人员按照计划进行培训、演练（实战）和更新，就会落入“纸上谈兵”的境地，应急计划也就失去了存在的价值，甚至成为一个“有害无益”的计划。

* P290

应急响应的通知策略应制定信息安全事件发生后某特定人员无法联络时的备选人选方案，并在应急响应计划中明确描述。一种通用通知方法是所谓的**呼叫树**。呼叫树应包括主要的和备用的联络方法，应确定在某个人无法联系上时应采取的规程。

* P333

【ISMS 基本要求（Basic Requirements of ISMS），指组织应在其整体业务活动中，并在其所面临风险的环境下，建立、实施、运行、监视和评审 ISMS，形成文件并保持和改进其有效性文档化的ISMS。】

* P335

ISMS 要求**可比较和可重现**所选择的风险评估方法产生的结果。因此，组织的信息安全风险评估应该是一个长期、定期、可持续的工作。每一次评估所获得的结果最终汇集起来就形成了这个组织信息安全风险评估的历史记录，也常常称为基准 (benchmark）。这个基准既从历史发展的脉络反映了组织信息安全管理水平是否与时俱进，也反映了与同行业相比该组织处于什么样的位置。必要的时候（如需要进行复核复检的时候），按照同样的风险评估过程得到同样的结果。