国内外信息安全标准化情况概要

中国科学院研究生院 信息安全国家重点实验室
全国信息安全技术标准化委员会 WG7

赵战生

2011年9月22日西宁
2011年11月3日 重庆

概要

- 1.信息安全标准化工作的重要性
- 2.需要什么标准
- 3.我国和国际标准化组织的工作组布局
- 4.国内外信息安全标准的主要成果
  - 4.1 密码应用标准
  - 4.2 保密标准
  - 4.3 信息安全技术产品标准
  - 4.4 信息安全评估标准
  - 4.5 信息系统安全标准
  - 4.6 信息安全管理标准

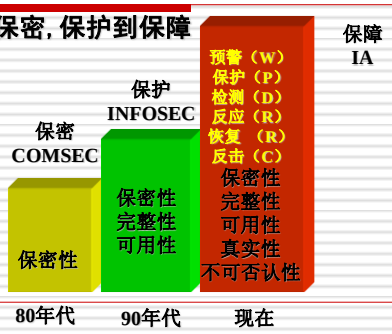
1.信息安全标准化工作的重要性

- 曲维枝同志指出：

没有信息安全的信息化是危险的信息化；没有完善的信息安全标准，信息化建设中的产品、系统、工程就不能实现安全的互联、互通、互操作，就不能形成我国自主的信息安全产业，就不能构造出一个自主可控的信息安全保障体系，就难以保证国家信息安全和国家利益。

2.需要什么标准

- 从保密，保护到保障



到底信息安全保障应该包括那些方面？！

- 一个宗旨:保障信息化带来的利益最大化(应用服务安全)
- 两个对象:
  - 信息
  - 信息系统
- 三个安全保障能力来源
  - 技术
  - 管理
  - 人

- 四个层面
  - 局域计算环境
  - 边界和外部连接
  - 基础设施
  - 信息内容

- 五个信息状态
  - 产生
  - 存储
  - 处理
  - 传输
  - 消亡

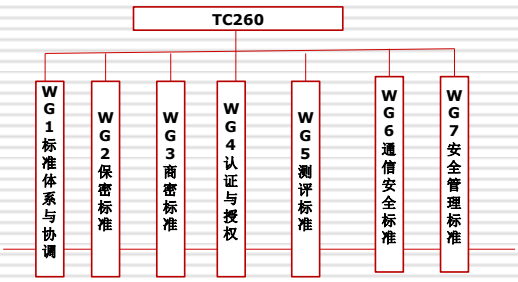
- 六个信息保障的环节
  - 预警（W）
  - 保护（P）
  - 检测（D）
  - 响应（R）
  - 恢复（R）
  - 反击（C）

- 七个安全属性
  - 保密性
  - 完整性
  - 可用性
  - 可认证性
  - 不可否认性
  - 可控性
  - 可追究性

- 我国信息安全保障工作的基本制度性安排
  - 信息安全等级保护
  - 涉密信息系统的信息安全保障管理
  - 密码技术的研究、开发、应用、管理
  - 信息安全保障工作中的产品、服务认证认可
  - 信息安全中内容安全监管

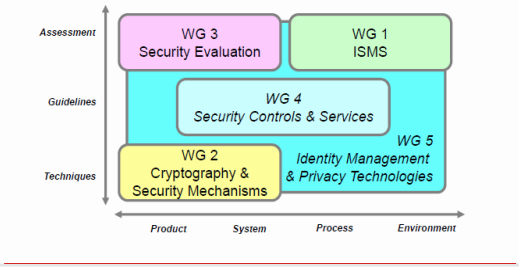
3.我国和国际标准化组织的工作组布局

TC260工作组布局



ISO/IEC JTC1 SC27 信息安全标准化工作内容

- WG1：信息安全管理体系
- WG2：密码学与安全机制
- WG3：安全评价准则
- WG4：安全控制与服务
- WG5：身份管理与隐私保护技术



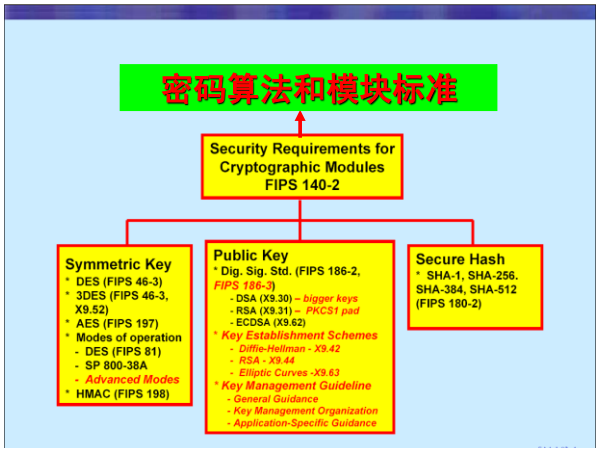
4.国内外信息安全标准的主要成果

我国信息安全标准成果概要

- 我国国家信息安全标准自**1995**年开始制定，至**2002**年共制定标准**19**项，全部由国际标准直接转化而来。主要内容是有关密码及评估的标准。在这**19**项中，**2004**年后已有**12**项进行了修订。
- 自安标委**2004**年成立以来至目前我国实际现存正式信息安全标准**87**项。送审及征求意见标准**20**余项。
- 这些标准中，既包括技术标准，如产品和系统（网络）标准，亦包括管理标准，如风险管理标准等，覆盖了当前信息安全主要需求领域。

4.1 密码应用标准

- 密码算法的标准化工作，美国进行的最为有序、深化。在其国家安全局（**NSA**)的支持、帮助、监控下，民用密码标准由其商务部(**DOC**）下属的国家技术标准研究所（**NIST**）负责制定。
- 从上世纪颁布的国家数据加密标准（**DES**），到为本世纪需要遴选出来的先进的加密标准（**AES**）；从**RSA**到**ECC**，以及密码模块的安全要求，他们有了全局部署。

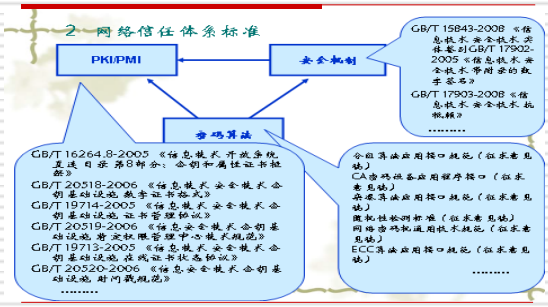


目前我国有关密码应用的标准

GB/T 17964-2008	《信息安全技术 分组密码算法的工作模式》
GB/T 15843.1-2008	《信息技术 安全技术 实体鉴别 第1部分:概述》
GB/T 15843.2-2008	《信息技术 安全技术 实体鉴别 第2部分:采用对称加密算法的机制》
GB/T 15843.3-2008	《信息技术 安全技术 实体鉴别 第3部分:采用数字签名技术的机制》
GB/T 15843.4-2008	《信息技术 安全技术 实体鉴别 第4部分:采用密码校验函数的机制》
GB/T 15843.5-2005	《信息技术 安全技术 实体鉴别 第5部分:使用零知识技术的机制》
GB/T 15852.1-2008	《信息技术 安全技术 消息鉴别码 第1部分:采用分组密码的机制》
GB/T 17903.1-2008	《信息技术安全技术 抗抵赖 第1部分:概述》
GB/T 17903.2-2008	《信息技术安全技术 抗抵赖 第2部分:采用对称技术的机制》
GB/T 17903.3-2008	《信息技术安全技术 抗抵赖 第3部分:采用非对称技术的机制》

GB/T 19717-2005	《基于多用途互联网邮件扩展（MIME）的安全报文交换》
GB/T 19771-2005	《信息技术 安全技术 公钥基础设施 PKI组件最小互操作规范》
GB/T 19713-2005	《信息技术安全技术 公钥基础设施在线证书状态协议》
GB/T 19714-2005	《信息技术安全技术 公钥基础设施证书管理协议》
GB/T 20518-2006	《信息安全技术公钥基础设施数字证书格式》
GB/T 17902.2-2005	《信息技术 安全技术 带附录的数字签名 第2部分：基于身份的机制》
GB/T 17902.3-2005	《信息技术 安全技术 带附录的数字签名 第3部分：基于证书的机制》
GB/T 20520-2006	《信息安全技术公钥基础设施时间戳规范》
GB/T 20519-2006	《信息安全技术公钥基础设施特定权限管理中心技术规范》

GB/T 21054-2007	《信息安全技术 公钥基础设施 PKI系统安全等级保护评估准则》
GB/T 21053-2007	《信息安全技术 公钥基础设施 PKI系统安全等级保护技术要求》
GB/T 25057-2010	《信息安全技术 公钥基础设施 电子签名卡应用接口基本要求》
GB/T 25059-2010	《信息安全技术 公钥基础设施简易在线证书状态协议》
GB/T 25060-2010	《信息安全技术 公钥基础设施 X.509数字证书应用接口规范》
GB/T 25061-2010	《信息安全技术 公钥基础设施 XML数字签名语法与处理规范》
GB/T 25065-2010	《信息安全技术 公钥基础设施 签名生成应用程序的安全要求》
GB/T 25056－2010	《信息系统安全技术 证书认证系统密码及其相关安全技术规范》
GB/T 25055－2010	《信息安全技术公钥基础设施安全支撑平台技术框架》
GB/T 25064－2010	《信息安全技术公钥基础设施电子签名格式规范》



4.2 保密标准

- 我国的保密标准均由国家保密局（**WG2**）负责制定。至今已经完成**30**项相关标准。他们是：

1. **BMB1-1994**《电话机电磁泄漏发射限值和测试方法》
2. **BMB2-1998**《使用现场的信息设备电磁泄漏发射检查测试方法和安全判据》
3. **BMB3-1999**《处理涉密信息的电磁屏蔽室的技术要求和测试方法》
4. **BMB4-2000**《电磁干扰器技术要求和测试方法》

5. **BMB5-2000**《涉密信息设备使用现场的电磁泄漏发射防护要求》
6. **BMB6-2001**《密码设备电磁泄漏发射限值》
7. **BMB7-2001**《密码设备电磁泄漏发射测试方法（总则）》
8. **BMB7.1-2001**《电话密码机电磁泄漏发射测试方法》
9. **BMB8-2004**《国家保密局电磁泄漏发射防护产品检测实验室认可要求》
10. **BMB10-2004**《涉及国家秘密的计算机网络安全隔离设备的技术要求和测试方法》

11. **BMB11-2004**《涉及国家秘密的计算机信息系统防火墙安全技术要求》
12. **BMB12-2004**《涉及国家秘密的计算机信息系统漏洞扫描产品技术要求》
13. **BMB13-2004**《涉及国家秘密的计算机信息系统入侵检测产品技术要求》
14. **BMB14-2004**《涉及国家秘密的信息系统安全保密测评实验室要求》
15. **BMB15-2004**《涉及国家秘密的信息系统安全审计产品技术要求》

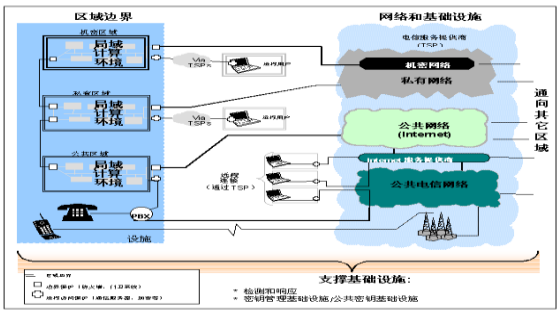
16. BMB16-2004《涉及国家秘密的信息系统安全隔离与信息交换产品技术要求》
17. BMB17-2006《涉及国家秘密的信息系统分级保护技术要求》（部分代替BMZ1－2000）
18. BMB18-2006《涉及国家秘密的信息系统工程监理规范》
19. BMB19-2006《电磁泄漏发射屏蔽机柜技术要求和测试方法》
20. GGBB1-1999《信息设备电磁泄漏发射限值》
21. GGBB2-1999《信息设备电磁泄漏发射测试方法》

22. BMZ1-2000《涉及国家秘密的计算机信息系统保密技术要求》（已被BMB17－2006和BMB20－2007代替）
23. BMZ2-2001《涉及国家秘密的计算机信息系统安全保密方案设计指南》（已被BMB23－2008代替）
24. BMZ3-2001《涉及国家秘密的计算机信息系统安全保密测评指南》（已被BMB22－2007代替）
25. BMB9.1-2007《保密会议移动通信干扰器技术要求和测试方法》
26. BMB9.2-2007《保密会议移动通信干扰器安装使用指南》

27. BMB20-2007《涉及国家秘密的信息系统分级保护管理规范》（部分代替BMZ1－2000）
28. BMB21-2007《涉及国家秘密的载体销毁与信息消除安全保密要求》
29. BMB22-2007《涉及国家秘密的信息系统分级保护测评指南》（代替BMZ3－2001）
30. BMB23-2008《涉及国家秘密的信息系统分级保护方案设计指南》（代替BMZ2－2001）

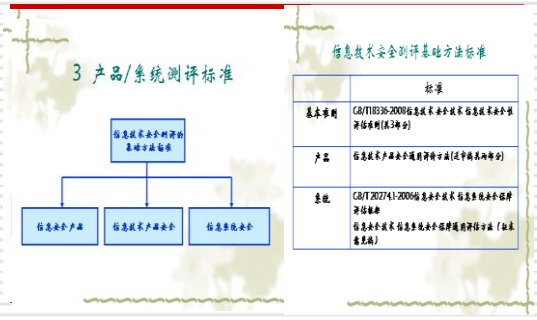
4.3信息安全技术产品标准

-信息保障技术框架关注的领域



信息安全技术产品标准
-根据技术保障框架形成保护要求（IATF）

保卫网络和基础设施	保卫边界和外部连接	保卫局域计算环境	支撑性基础设施		系统轮廓
交换机和路由器	防火墙	操作系统	PKI/KMI	检测和响应	多国信息共享
无线	VPN	生物识别技术	证书管理	IDS	
	外部设备	单级WEB	密钥恢复		
	远程访问	令牌	第四级PKI目录		
	多域解决方案	移动代码			
	移动代码	消息安全			
	门卫	数据库			

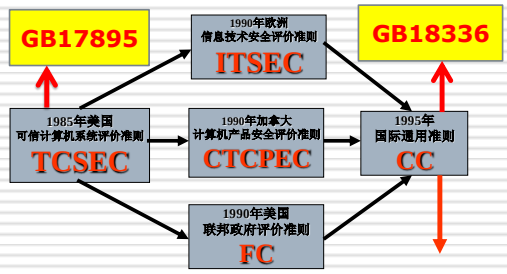


4.4 信息安全评估标准

- 安全评估标准的发展经历了漫长的时间
- 最具影响的是上世纪80年代，美国国防部推出的可信计算机安全评价准则（TCSEC）。
- 该标准（俗称橘皮书）基于贝尔.拉巴杜拉模型的“禁止上读下写”原则，用访问控制机制（自主型访问控制，强制型访问控制），针对计算机的保密性需求，把计算机的可信级别分成四类七个等级。
- 橘皮书随后又补充了针对网络、数据库等安全需求，发展成彩虹系列。
- 我国至今唯一的信息安全强制标准GB 17859就是参考橘皮书制定的。 GB 17859根据我们的产业能力，将信息安全产品分成五个等级。

- 上世纪九十年代，欧洲四国（英、法、德、荷）参照TCSEC，补充了完整性、可用性需求，提出了信息技术安全评价准则（ITSEC）。
- 上世纪九十年代中，六国七方（美（NIST，DOD）加、英、法、德、荷）和ISO共同推出通用评价准则（CC for ITSEC）。成为ISO不断发展的ISO/IEC 15408。
- 我国参考ISO/IEC15408颁布了推荐性标准GB/T18336

信息安全产品测评发展历史



GB/17859-1999	《计算机信息系统 安全保护等级划分准则》
GB/T 20271-2006	《信息安全技术 信息系统通用安全技术要求》
GB/T 20282-2006	《信息安全技术 信息系统安全工程管理要求》

TCSEC安全级化分表

类别	级别	名称	主要特征
A	A1	验证设计	形式化的最高级描述和验证，形式化的隐蔽通道分析，非形式化的代码对应证明
B	B3	安全区域	存取监控，高抗渗透能力
	B2	结构化保护	形式化模型/隐通道约束、面向安全的体系结构，较好的抗渗透能力
	B1	标识的安全保护	强制存取控制、安全标识
C	C2	受控制的存取控制	单独的可查性、广泛的审计跟踪
	C1	自主安全保护	自主存取控制
D	D	低级保护	相当于无安全功能的个人微机

TCSEC 安全策略实施及评估

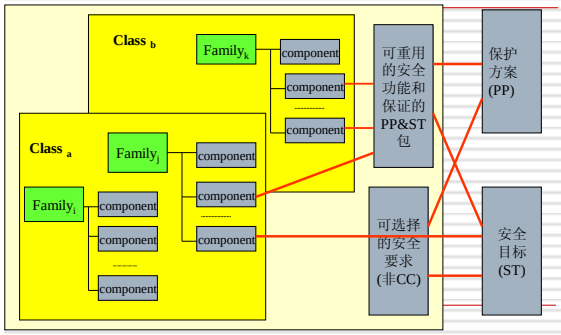
方面	评估标准	C1	C2	B1	B2	B3	A1
安全策略	自主访问控制	P		O			O
	目标重用		P		O	O	
	标识			P		O	O
	标识完整性			P	O		
	被标识信息输出			P			
	多层设备输出			P			
	单层设备输出			P			
	标记人可读输出			P			
	强制访问控制			P	O		
	目标敏感标识			P	O		
	设备标识			P	O		
可说明性	确认和授权	P	O	O			
	审计跟踪		P			O	O
	可信路径				P	O	

TCSEC 安全策略实施及评估

方面	评估标准	C1	C2	B1	B2	B3	A1
安全保证	系统体系	H	I	I	I	I	I
	系统完整性	H					
	安全测试	H		I	I	I	I
	设计说明和确认	H		I	I	I	I
	隐通道分析				H	I	I
	可信装置管理				H	I	
	配置管理				H		I
	可信恢复					H	
	可信分发						H
文档	安全特性用户指南	H					
	可信装置手册	H	I	I	I	I	I
	测试文件	H		I			I
	设计文件	H	I		I	I	I

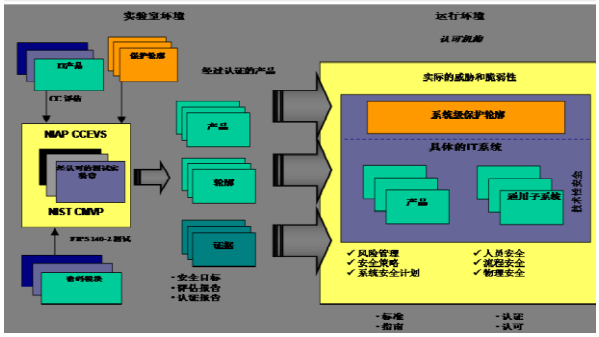
GB/T18336.1-2008	《信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型》
GB/T18336.2-2008	《信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求》
GB/T18336.3-2008	《信息技术 安全技术 信息技术安全性评估准则 第3部分： 安全保证要求》
GB/T 20283-2006	《信息安全技术 保护轮廓和安全目标的产生指南》

安全要求的组织结构



4.5 信息系统安全标准

产品不等同与系统



英国提出的IAMM

	过程	第一级 初始 业务和法律要求的IA危机意识	第二级 已建立 IA过程已制度化	第三级 业务启用 IA 过程在业务关键领域中实施	第四级 定量管理 公司例外项的数目实施IA进程已知并被报告	第五级 优化 良好的IA过程已集成为正常业务的一部分
在部门文化中嵌入信息风险管理	领导与治理					
	意识、培训、教育					
	信息风险管理					
实施IA测度的实践典范	贯穿生存周期的测度					
	保证信息共享					
有效的符合	合规性					

德国BSI制定的IT 基线保护标准

- 层模型和建模
  - IT基础保障建模
  - 基础层分配模式
- 模块（81）
  - B1一般方面（16）
  - B2基础设施（12）
  - B3 IT系统（服务器10，客户端10，网络组件3，其他6）
  - B4网络（7）
  - B5应用（17）

- 威胁目录（**483**）
  - G1不可抗力（19）
  - G2组织的缺点（147）
  - G3人为故障（98）
  - G4技术故障（73）
  - G5蓄意的行为（146）

- 措施目录（**1219**）
  - M1基础设施（73）
  - M2组织（443）
  - M3人员（69）
  - M4硬件和软件（345）
  - M5通讯（152）
  - M6应急准备（137）

系统安全建设和安全管理

- 美国联邦下信息安全管理法（**FISMA**）的实施
  - 第一阶段：标准和准则的制定
    2003-2008年
  - 第二阶段：组织认证计划
    2007-2010年
  - 第三阶段：安全工具验证计划
    原定**2008-2009**年，现在纳入第二阶段和使用现有的**IT**产品测试，评价和审定程序

- 遵守**NIST**的标准与指南的要求
  按照**FISMA**的规定，商务部长应以**NIST**开发的指导方针为基础标准，规定准联邦信息系统的标准和指南。为提高联邦信息系统的操作和安全效率，部长须视需要作出标准的强制性和约束力。标准规定应包括信息安全标准提供最低限度的信息安全要求和在联邦信息和信息系统安全的其他方面需要的改进。

- 与**FISMA**相一致的联邦信息处理标准（**FIPS**）是经商务部长的批准由并的**NIST**发行。 **FIPS**对联邦机构是强制性的，遵守这些**FISMA**规定的标准的对联邦机构具有约束力，因此，各机构不得放弃其使用。

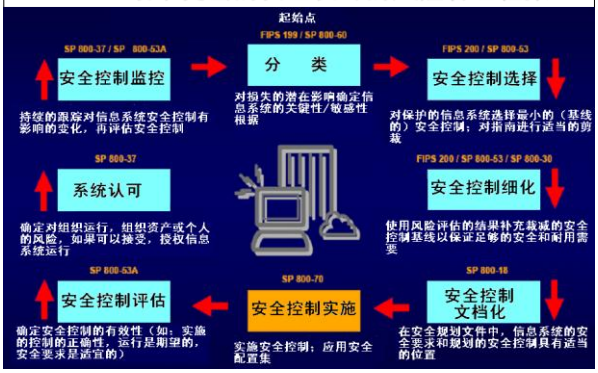
- 特别出版物（SP）是作为建议和指南文本由NIST发行。除了国家安全计划和系统，其他联邦各机构必须在联邦信息处理标准中遵循NIST的这些特别出版物规定的要求。FIPS 200要求使用特别出版物800-53的修订。此外，OMB（行政预算管理局）的政策（包括OMB对FISMA的报告和机构隐私管理）规定，除了国家安全方案和系统，其他联邦机构必须遵循某些具体NIST的特别出版物。

- 其它与安全有关的出版物，包括跨部门的报告（NISTIRs）和信息技术实验室（ITL）公告，提供了技术和NIST的其他有关活动信息。这些出版物只有在由OMB说明后是强制性的规定。
- 对于NIST安全标准和指南遵循的既定时间表由OBM在其政策、指示、或备忘录中确定（例如，FISMA年度报告指南）。

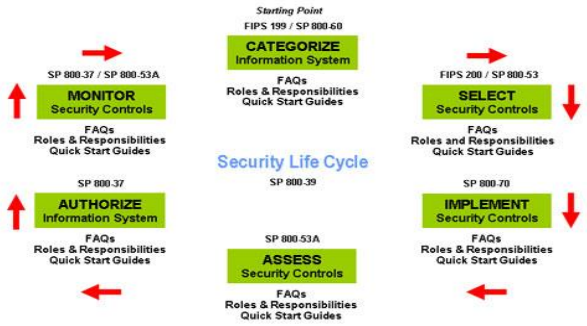
NIST为第一阶段制定的标准与指南

- FIPS 199：美国联邦信息和信息系统安全分类标准
- FIPS 200：联邦信息和信息系统的最低安全要求
- SP 800-18：开发联邦信息系统和组织的安全计划指南
- SP 800-30：版本1，实施风险评估指南
- SP 800-37：版本1，对联邦信息系统运用风险管理框架指南：安全生命周期方法
- SP800-39：业务范围的风险管理：组织，任务和信息系统的视图
- SP800-53：版本3，推荐的联邦信息系统和组织的安全控制
- SP 800 - 53A：版本1，联邦信息系统和组织安全控制评估指南
- SP800-59：确定一个信息系统作为国家安全系统的指南
- SP800-60：修订1，信息和信息系统安全分类映射类型指南
- SP 800 -XX: 信息系统安全工程指南
- SP 800 - yy：软件应用安全指南

NIST最早提出的认证认可的风险管理框架



目前版本的SP 800-37 对风险管理框架进行的改进



美国NISTSP800-39提升风险管理理念

- 2011年3月1日，NIST发布了 Special Publication 《Managing Information Security Risk *Organization, Mission, and Information System View*》最终版本
- 该出版物被称为在**FISMA**要求下进行联邦信息系统风险管理的“旗舰性文件”

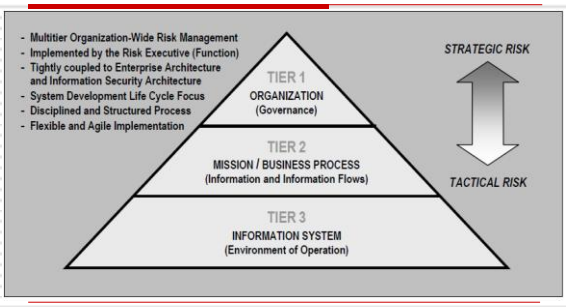
- 文件提出风险管理的通行过程是：
  - 框定风险（**FRAMING RISK**）
  - 评估风险（**ASSESSING RISK**）
  - 响应风险（**RESPONDING TO RISK**）
  - 监视风险（**MONITORING RISK**）

- 文件提出了阶梯形风险管理的概念
- 三个阶梯依次是：
  - 阶梯**1**：从组织的视野
  - 阶梯**2**：从使命/业务处理的视野
  - 阶梯**3**：从信息系统的视野

风险管理框架的特点

- 创立近实时的风险管理的概念，并通过实施强有力的连续监测过程推动信息系统的授权；
- 鼓励使用自动化操作来向高级领导人提供必要的信息，产生成本效益，以关注组织的信息系统支持的核心任务和业务职能进行基于风险的决策；
- 将信息安全结合到业务安全体系结构和系统开发的生命周期；
- 规定强调安全控制的选择、实施、评估、监测和信息系统的授权；
- 在信息系统一级结合风险管理的过程，在组织一级行使风险管理的责任；
- 为组织的信息系统安全控制的部署建立责任制和问责制，并使这些制度得到传承。

递升的风险管理方法



NIST Special Publication 800-53
Revision 3为联邦信息系统和组织推荐的案控制（共207项）
Recommended Security Controls for Federal Information Systems and Organizations ***August 2009***
INCLUDES UPDATES AS OF 05-01-2010

序	类	族	可选控制措施数目
1	管理	规划	6
2		风险评估	5
3		系统和服务获得	14
4		安全评估和授权	7
5		程序管理	11
6	技术	访问控制	22
7		标示与鉴别	8
8		系统和通信保护	34
9		审计和责任追究	14
10	运营	意识与培训	6
11		配置管理	9
12		人员安全	8
13		物理和环境保护	19
14		媒体保护	6
15		系统和信息完整性	13
16		应急计划	10
17		事件响应	8
18		维护	6

可选控制项示例表-访问控制

控制号	-	优先	控制基准		
			低	中	高
	访问控制				
AC-1	访问控制策略及规程	P1	AC-1	AC-1	AC-1
AC-2	账户管理	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	强制访问	P1	AC-3	AC-3	AC-3
AC-4	信息流强制	P1	不选	AC-4	AC-4
AC-5	分权划职	P1	不选	AC-5	AC-5
AC-6	最小特权	P1	不选	AC-6 (1) (2)	AC-6 (1) (2)
AC-7	不成功的注册尝试	P2	AC-7	AC-7	AC-7
AC-8	系统用户通知单	P1	AC-8	AC-8	AC-8
AC-9	以前登录（访问）通知单	P0	不选	不选	不选
AC-10	并发会话控制	P3	不选	不选	AC-10
AC-11	会话锁定	P3	不选	AC-11	AC-11
AC-12	会话终止 (隐含:成为SC-10的一部分)	—	—	—	—
AC-13	监督与检查—访问控制 (隐含:成为AC-2, AU-6的一部分)	—	—	—	—
AC-14	不附带鉴别与认证情况下允许的行动	P1	AC-14	AC-14 (1)	AC-14 (1)
AC-15	自动标记(隐含:作为 AC-16的一部分)	—	—	—	—
AC-16	安全属性	P0	不选	不选	不选
AC-17	远程访问	P1	AC-17	AC-17 (1) (2) (3) (4) (5) (10)	AC-17 (1) (2) (3) (4) (5) (6) (10)
AC-18	无线接入限制 (隐含:作为AC-17的一部分)	—	—	—	—
AC-19	移动终端的访问控制	P1	AC-19	AC-19 (1) (2) (3)	AC-19 (1) (2) (3)
AC-20	外部信息系统的用户	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	基于协作和信息共享的用户	P0	不选	不选	不选
AC-22	可理解的内容	P3	AC-22	AC-22	AC-22

NIST Special Publication 800-53A Revision 1

评估联邦信息系统和组织中的安全控制

构建有效的安全评估计划

Guide for Assessing the Security Controls in Federal Information Systems and Organizations *Building Effective Security Assessment Plans* ***May 2010***

- 在系统开发生命周期中进行评估
- 进行安全控制评估的战略
- 建设一支有效的保证案例
- 评估程序
- 准备安全控制评估
- 开发安全评估计划
- 进行安全控制评估
- 分析安全评估报告结果
- 附录**A**参考.
- 附录**B**词汇
- 附录**C**缩略语
- 附录**D**评估方法的描述
- 附录**E**渗透测试
- 附录**F**评定程序目录
- 附录**G**安全评估报告
- 附录**H**评审个案.

评估方法：

- 评估方法：检查，访谈，测试
- 检查评价对象：
  - 说明书（例如：政策，计划，程序，系统要求，设计）
  - 机制（例如：功能硬件实现，软件，固件）
  - 活动（例如：系统操作，管理，演练）
- 访谈评价对象：个人或群体。
- 测试评价对象：
  - 机制（如硬件，软件，固件）
  - 活动（例如，系统操作、管理、演练）

技术管理并重，追求自动化

- 美国推动信息安全自动化计划
  - 一个计划：ISAP

    《**Information Security Automation Program**》**Version 1.0 Beta, Last Revised 5/22/2007**

    是一个美国政府多个机构发起的使技术安全操作能够自动化标准化的计划
- 目标：**Automating Vulnerability Management, Security Measurement, and Compliance**

- 一个方法：SCAP

《Security Content Automation Protocol》
Version 1.0 Beta Last Revised 5/22/2007

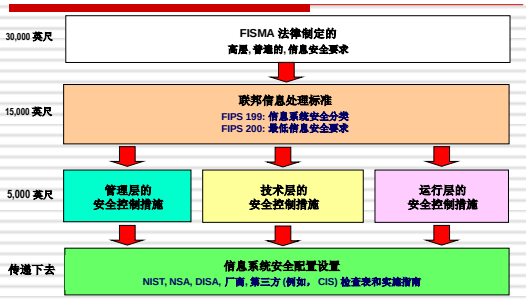
是为使用明确的标准使漏洞管理、度量以及政策符合性评价（如FISMA)自动化的一种方法

- 一个要求：FDCC

《Federal Desktop Core Configuration 》

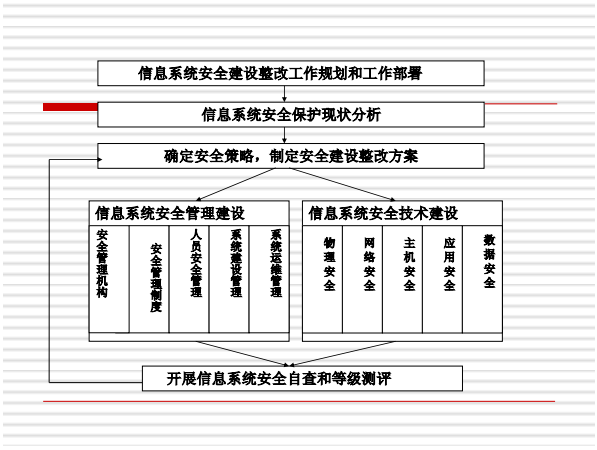
- 2007年3月20日美国电子政务和信息技术办公室官员（Administrator, Office of E-Government and Information Technology）Karen Evans对首席信息官发布里了《使用通用安全配置管理安全风险》（Managing Security Risk By Using Common Security Configurations）的备忘录

要干什么
FISMA 合规模型



我国信息系统安全等级保护的工作要求

- 五个规定动作
  - 定级
  - 备案
  - 安全建设整改
  - 等级测评
  - 检查



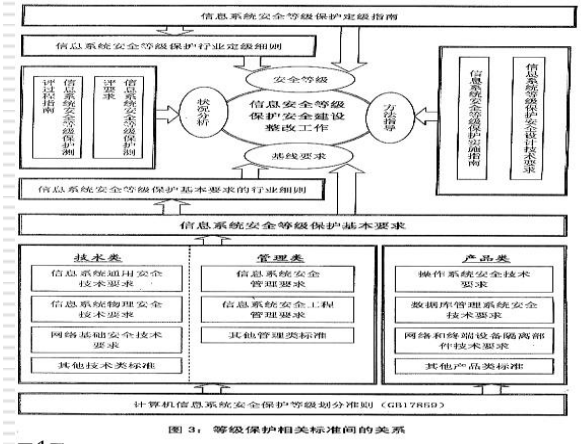
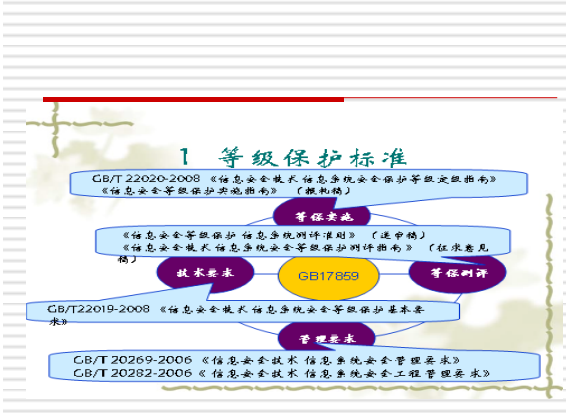


图 3： 等级保护相关标准间的关系



控制系统安全挑战

安全论题	信息技术	控制系统
反病毒和移动代码对策	普遍且广泛使用	不普遍且部署困难
支持技术的寿命	3-5年	多达20年
外包	普遍且广泛使用	很少使用（只有厂商）
补丁的应用	定期/按时	缓慢（限于厂商）
变更管理	定期/按时	基于遗产-不适合现代安全性
关键内容的时效	延误通常可接受	对于安全是关键的
可用性	延误通常可接受	24 x 7 x 365 x 永远
安全意识	私人领域和公共领域均良好	就网络安全而言通常贫乏
安全测试与审计	严格按时间表并强制	偶然为断供测试/为事件建立审计
物理安全	可靠	非常好,但通常偏远且无人值守

什么是SCADA

- SCADA(数据监控和采集系统)和分布式的控制系统 (DCS) 是计算机的控制系统，支持电力、 石油和天然气等高效生产和分配的。如果未受保护的它们可能产生灾难性的中断，对我们重要的国家基础设施的网络容易受到恶意攻击。

SCADA的特点

- 支持社会经济发展
- 关乎国家安全与社会稳定
- 涉及传统安全与信息安全

SCADA的特点

- 支持社会经济发展
- 关乎国家安全与社会稳定
- 涉及传统安全与信息安全

有关SCADA的标准

- NIST System Protection Profile - Industrial Control Systems, April 2004
- NIST - Field Device Protection Profile For SCADA Systems In Medium Robustness Environments, Version 0.71, May 2006
- NIST Special Publication 800-53 Revision 2, Recommended Security Controls for Federal Information Systems, December 2007, (Appendix I addresses Industrial Control Systems)
- NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, FINAL PUBLIC DRAFT, September 2008

- ANSI/ISA-TR99.00.02-2004, Integrating Electronic Security into the Manufacturing and Control Systems Environment, April 2004
- ANSI/ISA-TR99.00.01-2007, Security Technologies for Industrial Automation and Control Systems, January 2007
- ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts and Models, October 2007

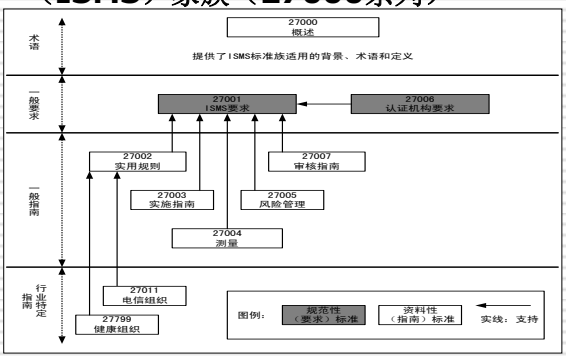
- IEEE Std 1402-2000, IEEE Guide for Electric Power Substation Physical and Electronic Security, January 2000
- IEEE Std 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities, February 2008
- IEEE P1613-2003, Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations, 2003
- IEEE P1777/D1, Draft Recommended Practice for Using Wireless Data Communications in Power System

- 还有许多国家和工业团体在关注SCADA安全问题，发布了一些相关标准

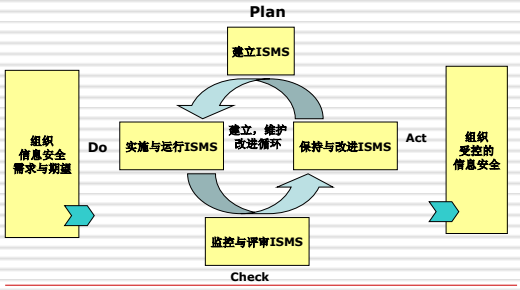
4.6 信息安全管理标准

- 27号文件要求：
  立足国情，以我为主坚持管理与技术并重
- 国际标准化组织的信息安全管理标准逐步配套，形成了信息安全管理体系（ISMS），并正在进一步与其他管理标准整合之中。

国际标准化组织信息安全管理体系标准（ISMS）家族（27000系列）



PDCA模型



信息安全管理的主要活动

1. 制定信息安全目标和实现目标的途径；
2. 建设信息安全组织机构，设置岗位、配置人员并分配职责；
3. 实施信息安全风险评估和管理；
4. 制定并实施信息安全策略；
5. 为实现信息安全目标提供资源并实施管理；
6. 信息安全的教育与培训；
7. 信息安全事故管理；
8. 信息安全的持续改进。

27002

- 名称:*IS 27002 (ISO/IEC 17799) – Code of practice for information security management*(信息安全管理实用规则)
- 来源:ISO/ICE 17799 2000改写成的ISO/IEC 17799：2005
- 内容:给出了11个安全域，39个控制目标，133个安全控制措施
- 状态:2005年已经正式发布

信息安全管理体系标准发布情况 (ISO SC27 WG1)

序号	项目号	标准名称	所处阶段
1	ISO/IEC 27000	信息安全管理体系概述和术语	已发布
2	ISO/IEC 27001	信息安全管理体系要求	已发布
3	ISO/IEC 27002	信息安全管理实用规则	已发布
4	ISO/IEC 27003	信息安全管理体系实施指南	已发布
5	ISO/IEC 27004	信息安全管理测量	已发布
6	ISO/IEC 27005	信息安全风险管理	已发布
7	ISO/IEC 27006	信息安全管理体系审核和认证结构的要求	已发布
8	ISO/IEC 27007	信息安全管理体系审核指南	CD
9	ISO/IEC 27008	关于ISMS控制措施的审核指南	WD

10	ISO/IEC 27010	用于行业间通信的信息安全管理	WD
11	ISO/IEC 27011	基于ISO/IEC 27002的电信组织的信息安全管理指南	已发布
12	ISO/IEC 27013	ISO/IEC 20000-1 and ISO/IEC 27001整合的实现指南	WD
13	ISO/IEC 27014	信息安全治理框架	WD
14	ISO/IEC 27015	用于金融和保险服务行业的信息安全管理体系	WD

信息安全服务与控制类标准发布情况 (ISO SC27 WG4)

序号	项目号	标准名称	所处阶段
1	ISO/IEC 27031	业务连续性的ICT就绪指南	CD
2	ISO/IEC 27032	网际安全指南	WD

3	ISO/IEC 27033-1	网络安全 第1部分：概述和术语	FDIS
4	ISO/IEC 27033-2	网络安全 第2部分：网络安全的设计和实施指南	CD
5	ISO/IEC 27033-3	网络安全 第3部分：涉及的网络情景-威胁、设计技术和控制主题	CD
6	ISO/IEC 27033-4	网络安全 第4部分：使用安全网关的网间通信安全保护-威胁、设计技术和控制主题	WD
7	ISO/IEC 27033-5	网络安全 第5部分：使用虚拟专用网的跨网通信安全保护-威胁、设计技术和控制主题	NP
8	ISO/IEC 27033-6	网络安全 第6部分：使用IP Convergence的跨网通信安全保护-威胁、设计技术和控制主题	NP
9	ISO/IEC 27033-7	网络安全 第7部分：使用无线和无线电的跨网通信安全保护-威胁、设计技术和控制主题	NP

10	ISO/IEC 27034-1	应用安全 第1部分：概述和术语	CD
11	ISO/IEC 27034-2	应用安全 第2部分：组织规范性框架	WD
12	ISO/IEC 27034-3	应用安全 第3部分：应用安全管理过程	NP
13	ISO/IEC 27034-4	应用安全 第4部分：应用安全验证	NP
14	ISO/IEC 27034-5	应用安全 第5部分：应用安全控制数据架构和规程	NP
15	ISO/IEC 27035	信息安全事件管理	CD
16	ISO/IEC 27036	外包安全指南	WD
17	ISO/IEC 27037	数字证据的识别、收集、获取和保存指南	WD

18	ISO/IEC TR 14516	可信第三方服务的使用和管理指南	已发布
19	ISO/IEC 15816	访问控制的安全信息对象	已发布
20	ISO/IEC 15945	支持数字签名应用的可信第三方服务规范	已发布
21	ISO/IEC 18043	入侵检测系统的选择、部署和操作	已发布
22	ISO/IEC 24762	信息和通信技术灾难恢复服务指南	已发布
23	ISO/IEC TR 29149	关于提供时间戳服务的最佳实践	WD

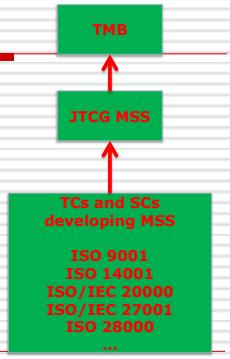
ISO/IEC 27001 的修订历程

- 2008年提出修订
- 2009年完成WD
- 2011年4月完成Ist CD
- 2011年10月将完成2nd CD
- FCD 2012?
- 预期 2013年完成IS
  (发布日期依赖于27002)

JTCG MSS and Guide 83

- TMB导则的投票
- **TMB** 根据投票结果来决策（**2011**年秋冬季）

MMS = management system standards
管理系统标准



ISO/JTC1 SC27 WG1其他新标准

- ISO/IEC 27013 (1st CD) ISO/IEC 27013 《ISO/IEC 27001和 ISO/IEC 20000-1综合实施指南》

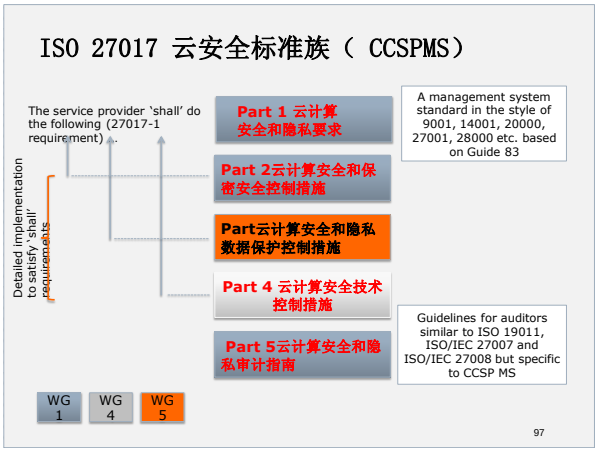
当既考虑提供服务又考虑信息资产保护时，管理体系综合实施有很多好处。这些好处可以在一个标准是否在另一个标准之前实施，或者这两个标准是否同时实施时体现出来。特别是管理和组织进程受益于标准间的相似之处和他们的共同目的。

- ISO/IEC 27016 (2nd WD) 《信息安全管理—组织经济学》

本技术报告为组织如何综合一个通用的方法将经济因素应用到信息安全管理工作提供指导、模型和实例。

ISO/JTC1 SC27 WG1 其他标准的发展

- 云计算安全和保密
  - 要求
  - 安全控制措施
  - 数据保护和保密
  - 技术
  - 审计指南
- 个人信息管理体系
  - 韩国提案
- ISMS 性能的成熟
  - 在比利时的提议



TC 260 WG7完成的管理标准

- **WG7**已完成标准22项（其中已发布**17**项，待发布**5**项）
- 标准涉及信息安全管理体系，应急管理，安全技术的控制等方面

- 管理体系类

1.GB/T 19715.1-2005 《信息技术 信息技术安全管理指南 第1部分：信息技术安全概念和模型》
2. GB/T 19715.2-2005 《信息技术 信息技术安全管理指南 第2部分：管理和规划信息技术安全》
3.GB/T 22080-2008 《信息技术 安全技术 信息安全管理体系 要求》
4.GB/T 22081-2008 《信息技术 安全技术 信息安全管理实用规则》
5.GB/T 25067–2010 《信息技术 安全技术 信息安全管理体系审核认证机构的要求》
6. GB/T 20269-2006 《信息安全技术 信息系统安全管理要求》
7. 《信息安全技术 信息系统安全管理评估要求》
8. GB/T 20282-2006 《信息安全技术 信息系统安全工程管理要求》
9.GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》
10.GB/T 24364-2009 《信息安全技术 信息安全风险管理指南》

- 应急类

1. GB/T 20988-2007 《信息安全技术 信息系统灾难恢复规范》
2. GB/T 20986-2007 《信息安全技术 信息安全事件分类分级指南》
3. GB/T 20985-2007 《信息技术 安全技术 信息安全事件管理指南》
4. GB/T 24363-2009 《信息安全技术 信息安全应急响应计划规范》

- 控制类

1. GB/T 25068.3-2010 《信息技术 安全技术 IT网络安全 第3部分：使用安全网关的网间通信安全保护》
2. GB/T 25068.4-2010 《信息技术 安全技术 IT网络安全 第4部分：远程接入的安全保护》
3. GB/T 25068.5-2010 《信息技术 安全技术 IT网络安全 第5部分：使用虚拟专用网的跨网通信安全保护》
4. GB/T 25068.5-2010 《信息技术 安全技术 IT网络安全 第5部分：使用虚拟专用网的跨网通信安全保护》
5. 《信息技术 安全技术 入侵检测系统的选择、部署和操作》
6. 《信息技术 安全技术 IT网络安全 第1部分：网络安全管理》
7. 《信息技术 安全技术 IT网络安全 第2部分：网络安全体系结构》

小结

- 胡锦涛总书记在几年中国共产党九十周年大会上指出：
  - 当前，世情、国情、党情继续发生深刻变化，我国发展中不平衡、不协调、不可持续问题突出，制约科学发展的体制机制障碍躲不开、绕不过，必须通过深化改革加以解决。
  - 实践发展永无止境，认识真理永无止境，理论创新永无止境。
  - 精神懈怠的危险，能力不足的危险，脱离群众的危险，消极腐败的危险更加尖锐地摆在全党面前

敬请各位领导指导

谢谢