如何开发和实施 ISMS

How to Develop and Implement an ISMS

—ISO/IEC27001实施

王新杰

北京知识安全工程中心

自我介绍

王新杰

- 2000年开始ISMS相关工作，目前主要从事：
  - ☑ ISMS认证咨询
  - ☑ 国家注册ISMS审核员培训
- 国家注册ISMS审核员培训教师
- 中国合格评定国家认可委员会信息安全专业委员会委员
- 联系：13311575049 wangxinjie@sina.com

缩略语介绍

ISMS

- Information Security Management System-ISMS
  信息安全管理体系
- 基于国际标准ISO/IEC27001：信息安全管理体系要求
- 是综合信息安全管理和技术手段，保障组织信息安全的一种方法
- ISMS是管理体系（MS）家族的一个成员

主要议题

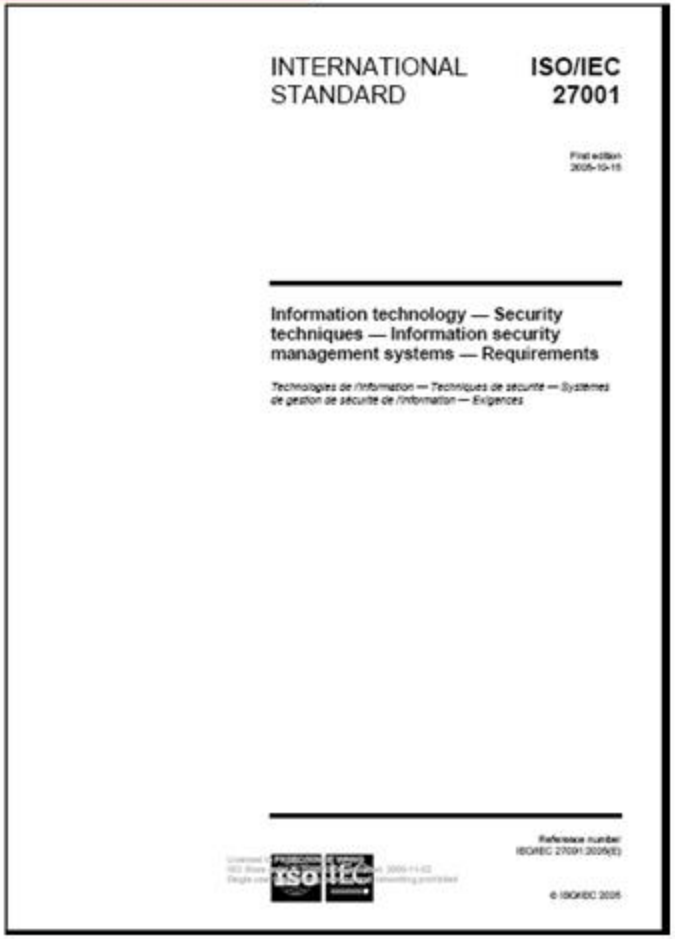
1. 从ISMS标准说起
2. 为什么需要ISMS
3. 全球ISMS认证现状
4. 开发和实施ISMS
5. 遇到的问题

1. 从ISMS标准说起

- 已经发布的ISMS标准和ISMS标准族
  - ISO/IEC27001:2005
  - ISO/IEC27002:2005
  - ISMS标准族：27000系列

1. 从ISMS标准说起

- **ISO/IEC27001:2005**



INTERNATIONAL STANDARD

ISO/IEC 27001

First edition
2005-10-15

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2005(E)

© ISO/IEC 2005

1. 从ISMS标准说起

ISO/IEC27001:2005

- ISO/IEC27001:2005的名称

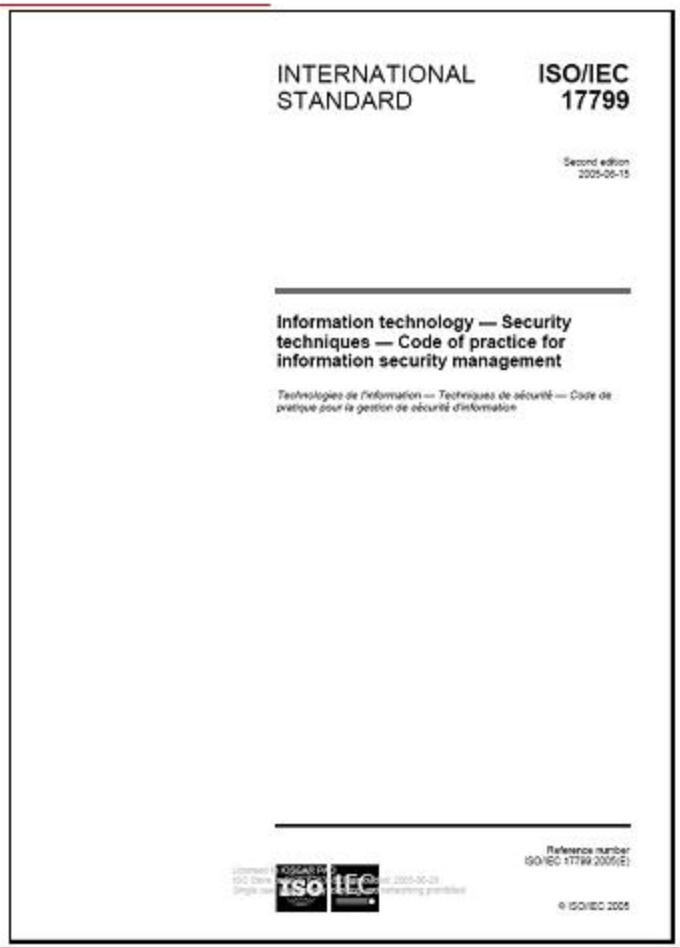
  Information technology- Security techniques-Information security management systems-requirements

  信息技术-安全技术-信息安全管理体系-要求

- 该标准用于：为建立、实施、运行、监视、评审、保持和改进信息安全管理体系提供模型，并规定了要求。
- 该标准适用于：所有类型的组织（例如，商业企业、政府机构、非赢利组织）。
- 是建立和实施ISMS的依据，是ISMS认证的依据。

1. 从ISMS标准说起

- **ISO/IEC27002:2005**



INTERNATIONAL STANDARD

ISO/IEC 17799

Second edition
2005-06-15

Information technology — Security techniques — Code of practice for information security management

Technologies de l'information — Techniques de sécurité — Code de pratique pour la gestion de sécurité d'information

Reference number
ISO/IEC 17799:2005(E)

1. 从ISMS标准说起

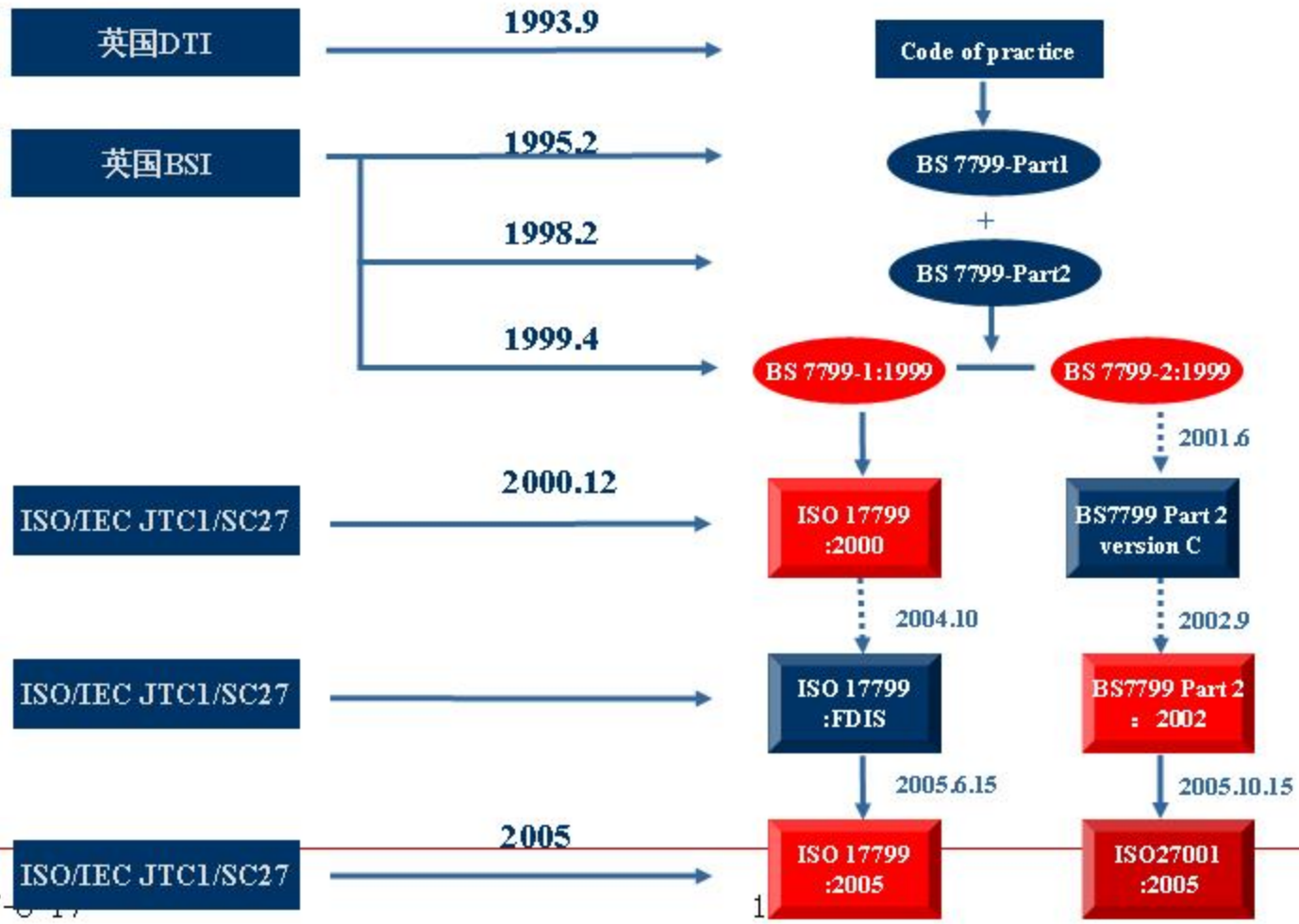
- **ISO/IEC27002:2005**
  - ISO/IEC27002:2005
    Information technology- Security techniques-Code of practice for information security management
    信息技术-安全技术-信息安全管理实用规则
  - 该标准给出了一个组织启动、实施、保持和改进信息安全管理的指南和一般原则，可作为建立组织的安全准则和有效安全管理实践的实用指南。
  - 该标准是ISO/IEC27001: 2005附录A的实施指南。

1. 从ISMS标准说起

- 正在制定中的ISMS族标准

序号	ISMS标准序号	标准名称	当前状态（2007.6）
1	ISO/IEC27000	ISMS 概述和词汇	委员会草案（CD）第2版
2	ISO/IEC27003	ISMS 实施指南	工作组草案（WD）第4版
3	ISO/IEC27004	ISM 测量	委员会草案（CD）第2版
4	ISO/IEC27005	ISMS 风险管理	最终委员会草案（FCD）第2版
5	ISO/IEC27007	ISMS 审核指南	新项目（NWI）

1. 从ISMS标准说起

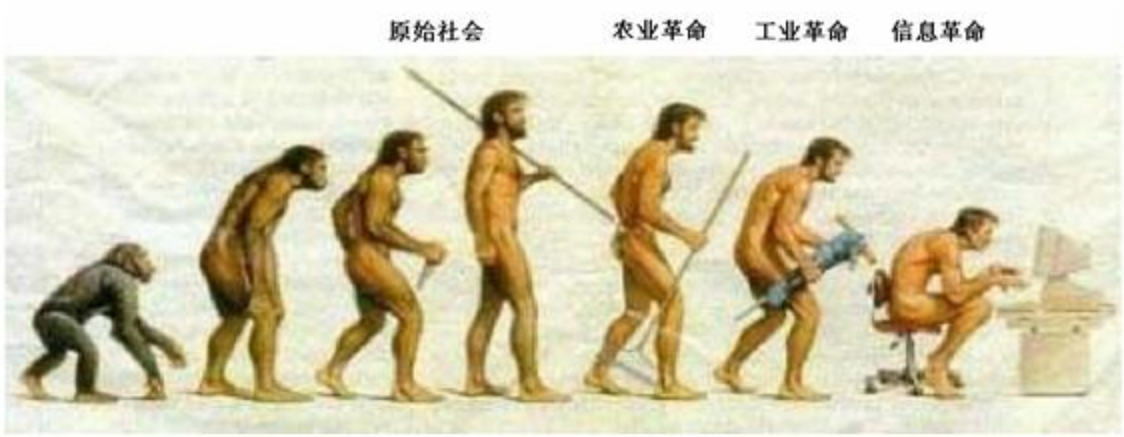


ISMS标准的由来

主要议题

1. 从ISMS标准说起
2. 为什么需要ISMS
3. 全球ISMS认证现状
4. 开发和实施ISMS
5. 遇到的问题

2. 为什么需要ISMS



- 生产工具的发展
- 信息安全就是生产安全

2. 为什么需要ISMS

组织有价值的信息在哪里？

解决信息安全问题的方案

- 产品导向型
- 需求导向型

ISMS是需求导向型的解决信息安全问题的方案。

2. 为什么需要ISMS

Prof. Basie von Solms

Head of the Academy for Information Technology, University of Johannesburg

- **information security – the third wave**
  - technical wave
  - management wave
  - institutional wave
- **2006年3月，又提出：**
  - corporate governance

主要议题

1. 从ISMS标准说起
2. 为什么需要ISMS
3. **全球ISMS认证现状**
4. 开发和实施ISMS
5. 遇到的问题

3. 全球ISMS的现状

- 每年成倍增长的全球ISMS认证证书

3. 全球ISMS的现状

Japan	2148*	Turkey	11	Oman	2
UK	313	Spain	10	Pakistan	2
India	288	Philippines	9	Slovak Republic	2
Taiwan	121	Saudi Arabia	9	South Africa	2
Germany	70	Sweden	8	Sri Lanka	2
Hungary	50	UAE	8	Armenia	1
Korea	50	Iceland	7	Bulgaria	1
USA	49	Kuwait	6	Egypt	1
China	48	Russian Federation	6	Gibraltar	1
Australia	44	Greece	5	Lebanon	1
Italy	43	Bahrain	4	Lithuania	1
Netherlands	31	Indonesia	4	Luxemburg	1
Hong Kong	28	Slovenia	4	Macedonia	1
Czech Republic	25	Thailand	4	Moldova	1
Singapore	25	Argentina	3	Morocco	1
Malaysia	20	Canada	3	New Zealand	1
Ireland	17	France	3	Peru	1
Brazil	16	Isle of Man	3	Qatar	1
Poland	16	Macau	3	Ukraine	1
Austria	14	Romania	3	Uruguay	1
Finland	14	Belgium	2	Vietnam	1
Norway	14	Colombia	2	Yugoslavia	1
Mexico	12	Croatia	2	Relative Total	3664
Switzerland	11	Denmark	2	Absolute Total	3653*

2007.5.31
全球ISMS
证书

3. 全球ISMS的现状

ISMS在中国

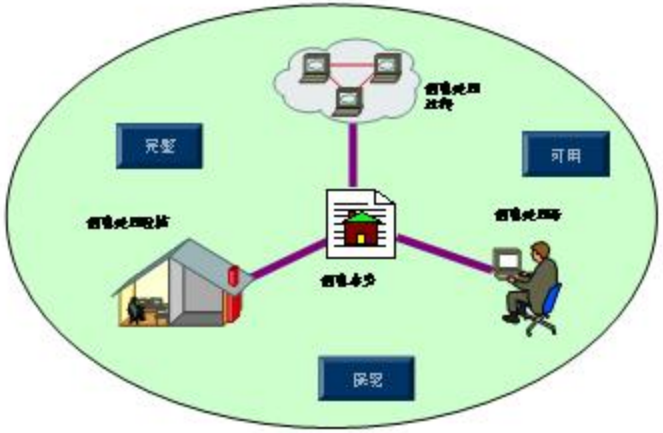
- 2000年前后，ISMS开始被中国用户认识；
- 2002年4月，政策主管部门开始ISMS认证认可制度的研究；
- 2002年11月，信安标委WG7开始研究和制定ISMS国家标准；
- 2005年6月15日，我国发布第一个ISMS国家标准“GB/T19716-2005信息安全管理实用规则”，该标准修改采用ISO/IEC17799:2000；
- 2005年8月，认监委批准北京知识安全工程中心和上海质量教育培训中心为ISMS认证培训机构；
- 2006年3月，国信办在5个单位开展ISMS标准应用试点工作：国家税务总局、证监会、北京、上海、武钢；
- 2006年4月，认监委批准4家ISMS试点认证机构：信产部4所、华夏认证中心、上海认证中心、赛宝认证中心；
- 2007年4月，中国向国际标准化组织ISO/IEC JTC1/SC27提出ISMS审核标准提案

主要议题

1. 从ISMS标准说起
2. 为什么需要ISMS
3. 全球ISMS认证现状
4. **开发和实施ISMS**
5. 遇到的问题

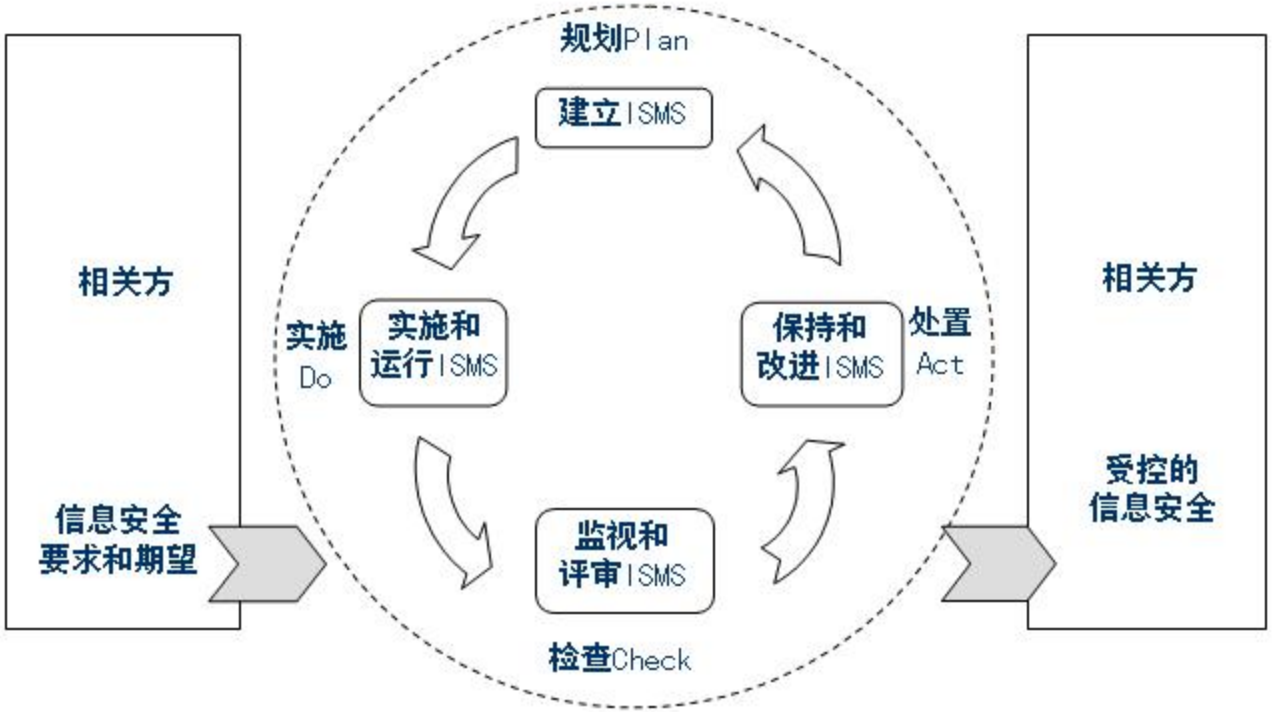
4. 开发和实施ISMS

- **ISO/IEC27001:2005的要求**
- 开发和实施**ISMS**



4. 开发和实施ISMS

- ISO/IEC27001:2005的要求



4. 开发和实施ISMS

- **ISO/IEC27001:2005的要求**

PDCA各阶段	内容	对应标准条款
P–规划 **建立**ISMS	建立与管理风险和改进信息安全有关的ISMS方针、目标、过程和程序，以提供与组织整体方针和目标相一致的结果。	4.1 4.2.1 4.3 5
D–实施 **实施和运行**ISMS	实施和运行ISMS方针、控制措施、过程和程序。	4.2.2
C–检查 **监视和评审**ISMS	对照ISMS方针、目标和实践经验，评估并在适当时，测量过程的执行情况，并将结果报告管理者以供评审。	4.2.3 6 7
A–处置 **保持和改进**ISMS	基于ISMS内部审核和管理评审的结果或者其他相关信息，采取纠正和预防措施，以持续改进ISMS。	4.2.4 8

ISO/IEC27001的要求

- P：建立ISMS
  - 4.1 总要求

    文件化的ISMS
  - 4.2.1 建立ISMS

    a) 范围
    b) 方针
    c) ~ h) 风险评估和管理
    i) 管理者授权实施和运行ISMS
    j) 适用声明
  - 4.3 文件要求
  - 5 管理职责

ISO/IEC27001的要求

- P：建立ISMS 之4.3 文件要求 – 文件的作用
  - 是指导组织有关信息安全工作方面的内部“法规”--使工作有章可循。
  - 是组织实际工作的标准。ISMS文件是根据ISMS标准和组织需要“量身定做”的实际工作的标准。对一般员工来说，在其实际工作中，可以不过问ISMS标准(ISO/IEC 27001:2005)，但必须按照ISMS文件的要求执行工作。
  - 是控制措施（controls）的重要部分。
  - 提供客观证据--为满足相关方要求，以及持续改进提供依据。
  - 提供适宜的内部培训的依据。
  - 提供ISMS审核（包括内审和外审）的依据，文件审核、现场审核。

ISO/IEC27001的要求

- P：建立ISMS 之4.3 文件要求

4.3.1 总则－必需的ISMS文件包括：

序号	文件名称	标准条款	说明
1	ISMS方针和目标	4.3.1 a)	可合并，一般是《信息安全方针》。
2	ISMS范围	4.3.1 b)	
3	风险评估方法的描述	4.3.1 d)	可编制《风险评估程序》，其运行结果产生《风险评估报告》。
4	风险评估报告	4.3.1 e)	
5	风险处理计划	4.3.1 f)	可编制《风险处理程序》，其运行结果产生《风险处理计划》。
6	文件控制程序	4.3.2	
7	记录控制程序	4.3.3	
8	内部审核程序	6	
9	纠正措施程序	8.2	通常合并在一起，称为《纠正和预防措施程序》。
10	预防措施程序	8.3	
11	适用声明	4.3.1 j)	
12	管理评审程序	7.1	在标准中，并没有称为“管理评审程序”，但作为管理体系，一般都要有。

ISO/IEC27001的要求

- P：建立ISMS 之4.3 文件要求

4.3.2 文件控制

a) 批准

b) 评审、更新并再批准;

c) 修订状态得到标识;

d) 在使用处可获得适用文件;

e) 清晰、易于识别;

f) 对需要的人员可用，传输、贮存和最终销毁;

g) 外来文件标识;

h) 分发控制;

i) 防止作废文件的非预期使用;

j) 作废文件的标识。

ISO/IEC27001的要求

- P：建立ISMS 之4.3 文件要求

4.3.3记录控制

a) 建立并保持，以提供证据。

b) 保护和控制。应考虑相关法律法规要求和合同义务。

c) 清晰、易于识别和检索。

d) 记录的标识、贮存、保护、检索、保存期限和处置所需的控制措施应形成文件并实施。

e) 记录的详略程度应通过管理过程确定。

f) 应保留4.2中列出的过程执行记录和所有发生的与ISMS有关的安全事故的记录。

ISO/IEC27001的要求

- P：建立ISMS 之5 管理职责 5.1 管理承诺－管理者应：
  - a) 制定ISMS方针；
  - b) 确保ISMS目标和计划得以制定；
  - c) 建立信息安全的角色和职责；
  - d) 向组织传达满足信息安全目标、符合信息安全方针、履行法律责任和持续改进的重要性；
  - e) 提供足够资源，以建立、实施、运行、监视、评审、保持和改进ISMS（见5.2.1）；
  - f) 决定接受风险的准则和风险的可接受级别；
  - g) 确保ISMS内部审核的执行（见第6章）；
  - h) 实施ISMS的管理评审（见第7章）。

ISO/IEC27001的要求

- P：建立ISMS 之5管理职责 5.2 资源管理

  5.2.1 资源提供

  应确定并提供信息安全工作所需的资源－人、财、物

  5.2.1 培训、意识和能力

  ① 确保所有分配有ISMS职责的人员具有执行所要求任务的能力

  ② 确保所有相关人员意识到其信息安全活动的适当性和重要性，以及如何为达到ISMS目标做出贡献。

ISO/IEC27001的要求

PDCA各阶段	内容	对应标准条款
P－规划 建立ISMS	建立与管理风险和改进信息安全有关的ISMS方针、目标、过程和程序，以提供与组织整体方针和目标相一致的结果。	4.1 4.2.1 4.3 5
D－实施 实施和运行ISMS	实施和运行ISMS方针、控制措施、过程和程序。	4.2.2
C－检查 监视和评审ISMS	对照ISMS方针、目标和实践经验，评估并在适当时，测量过程的执行情况，并将结果报告管理者以供评审。	4.2.3 6 7
A－处置 保持和改进ISMS	基于ISMS内部审核和管理评审的结果或者其他相关信息，采取纠正和预防措施，以持续改进ISMS。	4.2.4 8

ISO/IEC27001的要求

- D：实施和运行ISMS　之4.2.2

a) 制定风险处理计划（见第5章）。

b) 实施风险处理计划。

c) 实施4.2.1 g）中所选择的控制措施。

d) 测量所选择的控制措施或控制措施集的有效性（见4.2.3c)）。

e) 实施培训和意识教育计划（见5.2.2）。

f) 管理ISMS的运行。

g) 管理ISMS的资源（见5.2）。

h) 事件和事故响应（见4.2.3 a））。

ISO/IEC27001的要求

PDCA各阶段	内容	对应标准条款
P－规划 建立ISMS	建立与管理风险和改进信息安全有关的ISMS方针、目标、过程和程序，以提供与组织整体方针和目标相一致的结果。	4.1 4.2.1 4.3 5
D－实施 实施和运行ISMS	实施和运行ISMS方针、控制措施、过程和程序。	4.2.2
C－检查 监视和评审ISMS	对照ISMS方针、目标和实践经验，评估并在适当时，测量过程的执行情况，并将结果报告管理者以供评审。	4.2.3 6 7
A－处置 保持和改进ISMS	基于ISMS内部审核和管理评审的结果或者其他相关信息，采取纠正和预防措施，以持续改进ISMS。	4.2.4 8

ISO/IEC27001的要求

- C：监视和评审ISMS 之4.2.3

a) 执行监视和评审程序和其它控制措施。
b) ISMS有效性的定期评审。
c) 测量控制措施的有效性以验证安全要求是否被满足。
d) 按照计划的时间间隔进行风险评估的评审。
e) 按计划的时间间隔，对ISMS进行内部审核（见第6章）。
f) 定期对ISMS进行管理评审。
g) 考虑监视和评审活动的结果，以更新安全计划。
h) 记录可能影响ISMS的有效性或执行情况的措施和事件（见4.3.3）。

ISO/IEC27001的要求

- C：监视和评审ISMS 之 6 内部ISMS审核 术语介绍

  - **审核 audit**
    为获得审核证据并对其进行客观的评价，以确定满足审核准则的程度所进行的系统的、独立的并形成文件的过程。
  - **内部审核 internal audit**
    有时称为第一方审核，用于内部目的的，由组织自己或以组织名义进行，可作为组织自我合格声明的基础。
  - **审核员 aditor**
    有能力实施审核的人员。
  - **审核方案 audit programme**
    针对特定时间段所策划，并具有特定目的的一组(一次或多次)审核。

ISO/IEC27001的要求

- C：监视和评审ISMS 之6 内部ISMS审核 术语介绍

  - 符合（合格） conformity
    满足要求。
  - 不符合（不合格） nonconformity
    未满足要求。
  - 验证 verification
    通过提供客观证据对规定要求已得到满足的认定。
  - 要求 requirement
    明示的、通常隐含的或必须履行的需求或期望

ISO/IEC27001的要求

- C：监视和评审ISMS　之6 内部ISMS审核

① 按照计划的时间间隔进行内部ISMS审核。

② 审核方案。

③ 审核的客观和公正，审核员不应审核自己的工作。

④ 内审程序中的职责和要求。

⑤ 受审核区域的管理者应消除不符合及其原因，并跟踪验证。

⑥ ISO19011:2002 给出了审核指南。

ISO/IEC27001的要求

- C：监视和评审ISMS 之7 ISMS的管理评审 术语介绍

  - 评审 review
    为确定主题事项达到规定目标的适宜性、充分性和有效性所进行的活动。也可包括确定效率。
    如管理评审、设计和开发评审、顾客要求评审等。

ISO/IEC27001的要求

- C：监视和评审ISMS 之 7 ISMS的管理评审

  7.1 总则

  ① 按照计划的时间间隔进行管理评审，至少一年一次。

  ② 包括评估ISMS改进的机会和变更的需要。

  ③ 包括信息安全方针和信息安全目标。

  ④ 评审报告和评审记录。

ISO/IEC27001的要求

- C：监视和评审ISMS　之7 ISMS的管理评审

  7.2 评审输入

  a) ISMS审核和评审的结果;

  b) 相关方的反馈;

  c) 组织用于改进ISMS执行情况和有效性的技术、产品或程序;

  d) 预防和纠正措施的状况;

  e) 以往风险评估没有充分强调的脆弱点或威胁;

  f) 有效性测量的结果;

  g) 以往管理评审的跟踪措施;

  h) 可能影响ISMS的任何变更;

  i) 改进的建议。

ISO/IEC27001的要求

- C：监视和评审ISMS 之 7 ISMS的管理评审

  7.3 评审输出

  a) ISMS有效性的改进;

  b) 风险评估和风险处理计划的更新;

  c) 必要时修改影响信息安全的程序，以响应内部或外部可能影响ISMS的事件;

  d) 资源需求;

  e) 正在被测量的控制措施的有效性的改进。

ISO/IEC27001的要求

PDCA各阶段	内容	对应标准条款
P－规划 建立ISMS	建立与管理风险和改进信息安全有关的ISMS方针、目标、过程和程序，以提供与组织整体方针和目标相一致的结果。	4.1 4.2.1 4.3 5
D－实施 实施和运行ISMS	实施和运行ISMS方针、控制措施、过程和程序。	4.2.2
C－检查 监视和评审ISMS	对照ISMS方针、目标和实践经验，评估并在适当时，测量过程的执行情况，并将结果报告管理者以供评审。	4.2.3 6 7
A－处置 保持和改进ISMS	基于ISMS内部审核和管理评审的结果或者其他相关信息，采取纠正和预防措施，以持续改进ISMS。	4.2.4 8

ISO/IEC27001的要求

- A：保持和改进ISMS 之 4.2.4

  组织应经常：

  a) 实施已识别的ISMS改进措施。

  b) 依照8.2和8.3采取合适的纠正和预防措施。从其它组织和组织自身的安全经验中吸取教训。

  c) 向所有相关方沟通措施和改进措施，其详细程度应与环境相适应，需要时，商定如何进行。

  d) 确保改进达到了预期目标。

ISO/IEC27001的要求

- A：保持和改进ISMS 之 8 ISMS改进 术语介绍

  - 持续改进 continual improvement
    增强满足要求的能力的循环活动。
  - 预防措施 preventive action
    为消除潜在不符合或其他潜在不期望情况的原因所采取的措施。
  - 纠正措施 corrective action
    为消除已发现的不符合或其他不期望情况的原因所采取的措施。
  - 纠正 corrective
    为消除已发现的不符合所采取的措施。

ISO/IEC27001的要求

- A：保持和改进ISMS 之 8 ISMS改进

8.1 持续改进

组织应通过使用信息安全方针、安全目标、审核结果、监视事件的分析、纠正和预防措施以及管理评审（见第7章），持续改进ISMS的有效性。

ISO/IEC27001的要求

- A：保持和改进ISMS 之 8 ISMS改进

8.2 纠正措施

① 应采取措施消除与ISMS要求不符合的原因，以防止再发生。

② 纠正措施程序应规定以下要求：

a) 识别不符合；

b) 确定不符合的原因；

c) 评价确保不符合不再发生的措施需求；

d) 确定和实施所需要的纠正措施；

e) 记录所采取措施的结果（见4.3.3）；

f) 评审所采取的纠正措施。

ISO/IEC27001的要求

- A：保持和改进ISMS 之 8 ISMS改进

8.3 预防措施

① 应确定措施，以消除潜在不符合的原因，防止其发生。

② 预防措施程序应规定以下要求：

a) 识别潜在的不符合及其原因；

b) 评价防止不符合发生的措施需求；

c) 确定和实施所需要的预防措施；

d) 记录所采取措施的结果（见4.3.3）；

e) 评审所采取的预防措施。

③ 应识别变化的风险，并识别针对重大变化的风险的预防措施的要求。

④ 预防措施的优先级要根据风险评估的结果确定。

⑤ 预防不符合的措施通常比纠正措施更节约成本。

ISO/IEC27001的要求

PDCA各阶段	内容	对应标准条款
P-规划 建立ISMS	建立与管理风险和改进信息安全有关的ISMS方针、目标、过程和程序，以提供与组织整体方针和目标相一致的结果。	4.1 4.2.1 4.3 5
D-实施 实施和运行ISMS	实施和运行ISMS方针、控制措施、过程和程序。	4.2.2
C-检查 监视和评审ISMS	对照ISMS方针、目标和实践经验，评估并在适当时，测量过程的执行情况，并将结果报告管理者以供评审。	4.2.3 6 7
A-处置 保持和改进ISMS	基于ISMS内部审核和管理评审的结果或者其他相关信息，采取纠正和预防措施，以持续改进ISMS。	4.2.4 8

ISO/IEC27001的要求

- ISO/IEC27001:2005 附录A的要求

章节	控制措施域	控制目标	控制措施
A.5	安全方针	1	2
A.6	信息安全组织	2	11
A.7	资产管理	2	5
A.8	人力资源安全	3	9
A.9	物理和环境安全	2	13
A.10	通信和操作管理	10	32
A.11	访问控制	7	25
A.12	信息系统获取、开发和维护	6	16
A.13	信息安全事故管理	2	5
A.14	业务连续性管理	1	5
A.15	符合性	3	10
合计		39	133

4. 开发和实施ISMS

- 开发和实施ISMS
  - 正确理解ISMS
  - 建立信息安全管理机构
  - 识别ISMS文件要求
  - 执行风险评估和处理
  - 遵循标准规定的ISMS运行过程-PDCA

① 正确理解ISMS

- 正确理解ISMS
- 分析ISMS的要素
- 正确的ISMS设计与开发思路

在SINOCOM实施ISMS动员大会上的一个比喻：ISMS就是一台“机器”！

② 建立ISMS管理机构

- 什么是ISMS管理机构
- 为什么需要管理机构
- 管理者承诺

③ 识别ISMS文件要求

- 文件的作用
- ISMS文件的类型
- 文件的创建
- 文件的基本要求
- ISMS文件与QMS文件的比较

④ 执行风险评估和处理

- 必须的活动
- 产生两个文件：风险评估报告和风险处理计划
- 主要过程：**4.2.1中c)~h)**

c) 确定风险评估方法

d) 识别风险

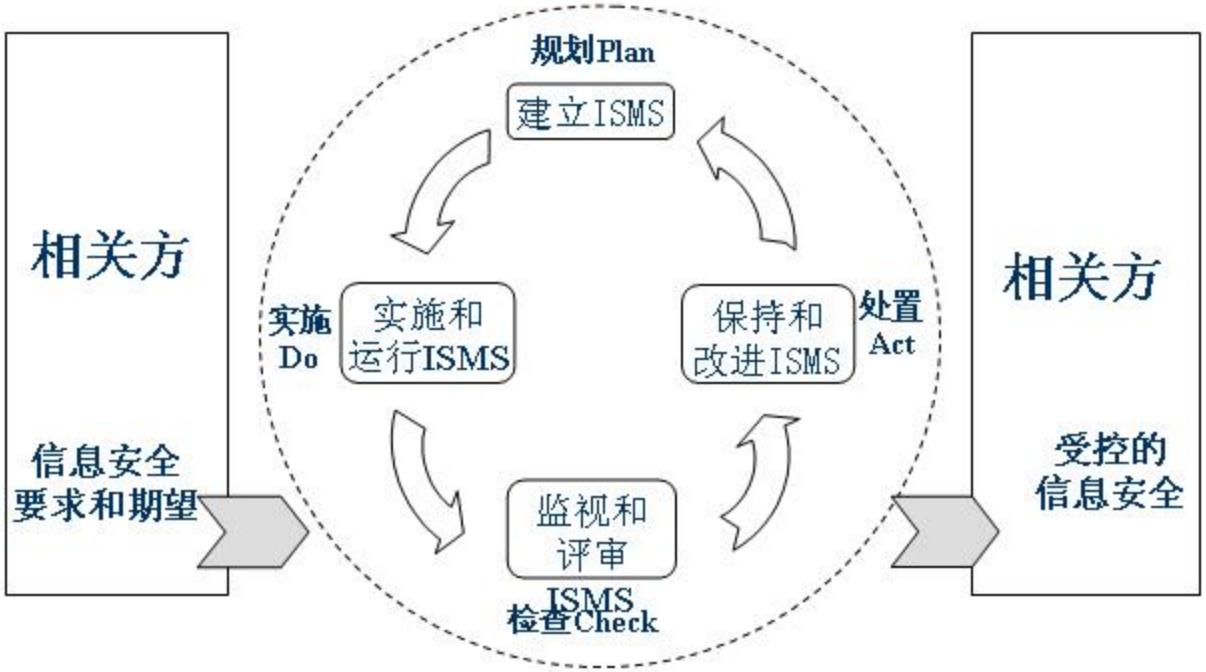
e) 分析和评价风险

f) 识别和评价风险处理的可选措施

g) 为处理风险选择控制目标和控制措施

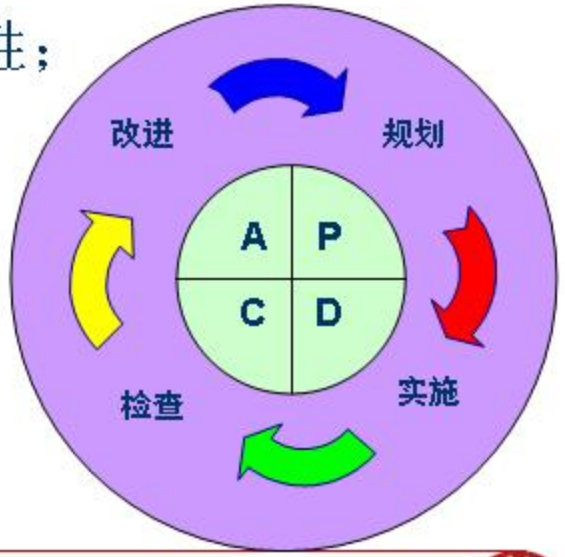
h) 获得管理者对建议的残余风险的批准

⑤ 遵循标准规定的ISMS运行过程－PDCA



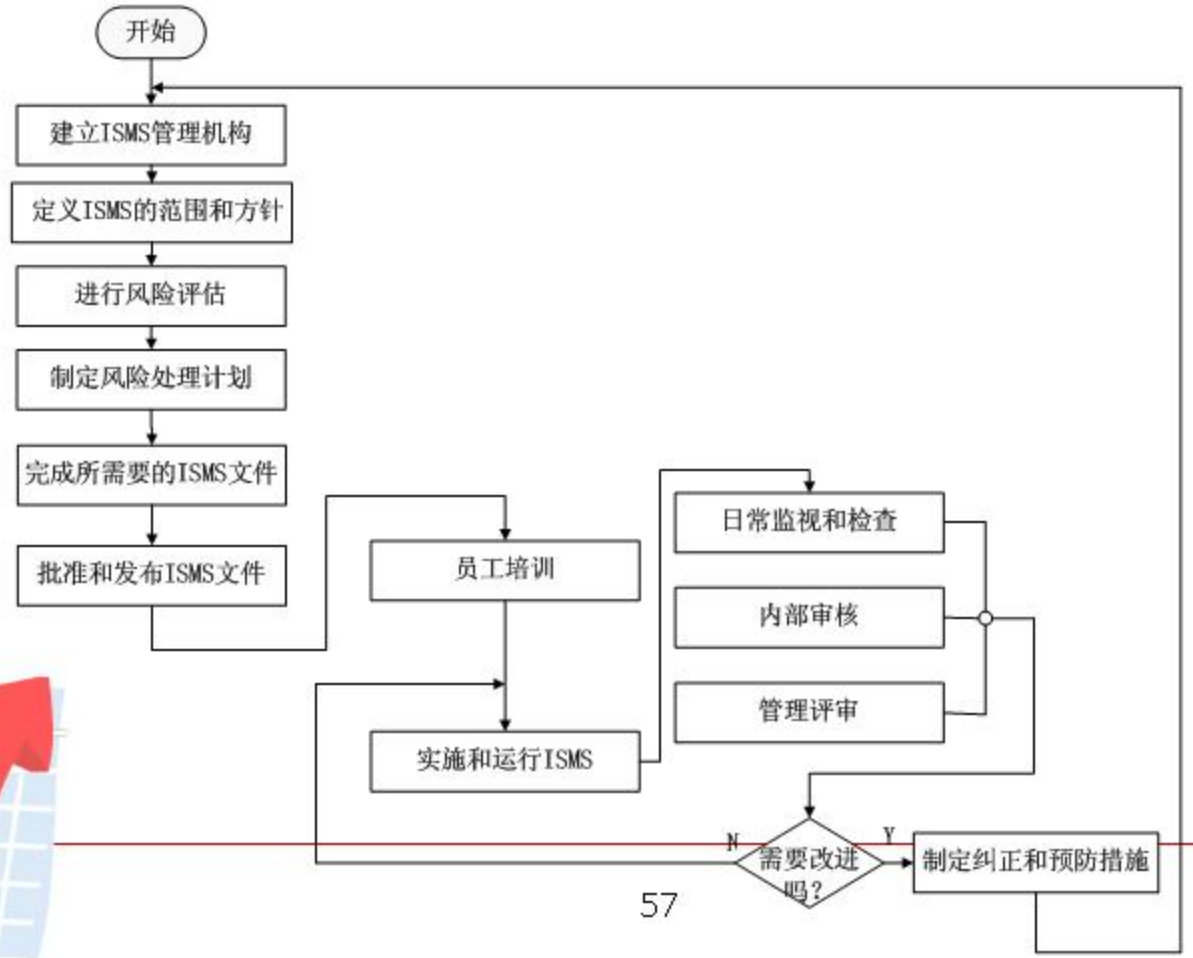
ISMS开发和实施

- 应用于**ISMS**的**PDCA**模型，可以概括为：
  1）规定应该做什么并形成ISMS文件；
  2）做ISMS文件已规定的事情；
  3）评审你所做的事情的符合性和有效性；
  4）通过预防和纠正措施，持续改进。



基于PDCA的ISMS的实际建设流程

P- Plan计划　　D-Do实施　　C-Check检查　　A-Act改进



PKSEC之ISO/IEC27001认证咨询方案

- 方案A：体系符合性实施指导
- 方案B：控制措施有效性部署指导
- 方案C：控制措施部署实施

主要议题

1. 为什么需要ISMS
2. ISMS标准
3. 全球ISMS的现状
4. 开发和实施ISMS
5. **遇到的问题**

5. 遇到的问题

Q1: 区分两种不同的“信息安全管理”

Q2: 认识“技术”和“管理”的辨证关系

Q3: 理解ISMS与等级保护、风险评估的关系

Q4: 实施ISMS要有耐心

Q1-区分两种不同的“信息安全管理”

举例 / 项目	举例1：海淀区政府发文，要求行政机关和事业单位建立和实施ISMS	举例2：海淀区政府根据自身需要决定建立和实施ISMS
性质	行政（政府）行为	组织自身事务
依据	行政许可法	组织自身业务需要和规章制度
主体	行政机关	组织
目的	行政管理	组织自身的业务管理
方法	法规、文件	组织自己决定

Q2-认识“技术”和“管理”的辨证关系

- 完全“技术”
- 完全“管理”
- 三分技术，七分管理？
- **ISMS**并非仅仅管理！

Q3-理解ISMS与等级保护、风险评估的关系

- 等级保护、**ISMS**都是保障信息安全的方法，即相对独立，又相互联系，可以联合实施，也可选择其一。
- 等级保护和**ISMS**中需要风险评估和处理过程。
- 等级保护是制度要求，**ISMS**可以支持等级保护的实施。

Q4-实施ISMS要有耐心

- 实施ISMS的组织的愿望总是“短平快”
- 人、时间、投入严重不足
- 试点经验：

  中等规模的组织（500人）

  人员：至少5人

  时间：12个月以上

  经费：60万左右（不包括申请认证的费用）

Q&A

谢谢！

附：PKSEC介绍

- 北京知识安全工程中心
  Peking Knowledge Security Engineering Center -PKSEC
- 2003年6月，吕述望教授创办，并担任主任，赵战生教授担任学术委员会主任，陈华平研究员担任总工程师。
- 定位：面向知识安全的科学研究、产品研制和咨询服务。
- 目标：建设一个知识安全创新基地；建设一个知识安全人才培训基地。

PKSEC—知识安全

- 知识安全
  - 知识安全是继计算机数据安全、网络信息安全之后的新的更高和更深层次的信息资源的安全。
  - 在信息资源中，数据是事实与数字组成的原始的素材；信息是对原始素材进行整理后形成的消息与情报；知识是对消息与情报进行理性分析与综合后形成的系统的认识与思想及清晰表述的论断。
  - 知识安全是数据安全和信息安全的扩展与延伸，又是信息资源安全一个新的发展阶段。
  - **from DCS, IS to KS**

PKSEC—业务领域

- 当前主要业务领域
  - ☑ 信息安全管理体系（ISMS）认证服务
    a) ISMS认证培训
    b) ISMS认证咨询
  - ☑ 密码技术研究与开发
    a) 密码编码
    b) 密码分析

PKSEC－在ISMS领域的优势

- PKSEC在ISMS认证服务领域的优势
  - ☑ 国家批准的全国首家ISMS认证培训机构
  - ☑ ISMS国家标准核心起草单位
  - ☑ 全国信息安全标准化技术委员会WG7、WG1、TCG成员
  - ☑ 专业信息安全科研服务机构
  - ☑ 具有7年ISMS研究和推广经验的咨询顾问团队

PKSEC－Intenet安全利用学术研讨会

- **Internet安全利用学术研讨会**
  - ☑ 1997年吕述望教授创办，2006年已经是第十五届。
  - ☑ 会议程序和学术安排按“IWMP”进行：
    a) Idea：报告学术思想
    b) Work：汇报科研工作
    c) Message：演讲最新消息
    d) Product：介绍安全产品

联络信息

王新杰

wangxinjie@pksec.com

13311575049

010-62558716，62639296