做好准备迎接信息安全管理体系标准27001新版本

Be Ready and Prepared for the New Edition of ISO/IEC 27001

王新杰

Wang Xinjie

2013.07.14

OWASP 中国

The Open Web Application Security Project

(ISC)²®

自我介绍
About Me

OWASP 中国
The Open Web Application Security Project

- **王新杰**

(ISC)² 中国顾问，北京时代新威信息技术有限公司总经理。自1999年至今在信息安全行业从业十多年。主要工作领域为信息安全管理体系、信息安全审计和信息安全教育培训。同时也担任：

- 中国信息安全测评中心CISP-Auditor培训教师
- 中国合格评定国家认可委员会（CNAS）信息安全专业和IT服务专业评审员
- 全国信息安全标准化技术委员会（TC260/WG7）成员
- 信息安全国际标准化组织ISMS工作组（ISO/IEC JTC1/SC27/WG1）专家
- 亚洲信息安全论坛（RAISE Forum）成员

联系方式:

(ISC)² Authorized China Agency

地址：北京市海淀区知春路甲48号盈都大厦C座2单元17B
电话：010-58731396
邮箱：wxinjie@isc2.org
网址：www.isc2.org

(ISC)²®

OWASP 中国
The Open Web Application Security Project

2500年前的信息安全意识

An Information Security Awareness 2500 Years Ago

孔子 Confucius (B.C.551－B.C.479)

子曰: 几事不密则害成。

Confucius said: “It would cause harm if you do not keep the sensitive things secret”.

《易经・系辞》

《The Book of Changes · Xici 》

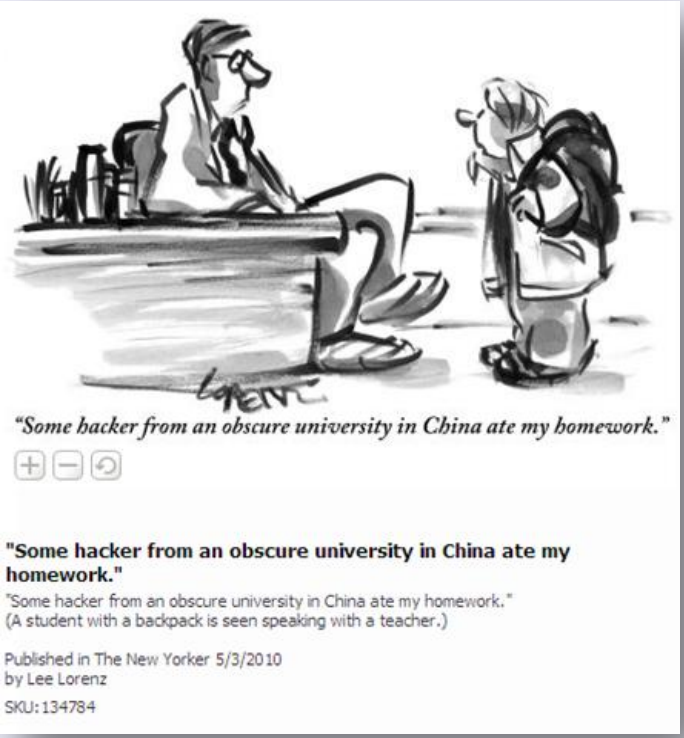
(ISC)²

引子

OWASP 中国
The Open Web Application Security Project

2010年发生的故事：美国一个小学生的作业让黑客吃了

A Story in 2010：An US Pupil's Homework Was Eaten by A Hacker



"来自中国一个不知名大学的黑客把我的家庭作业给吃了"

(ISC)²®

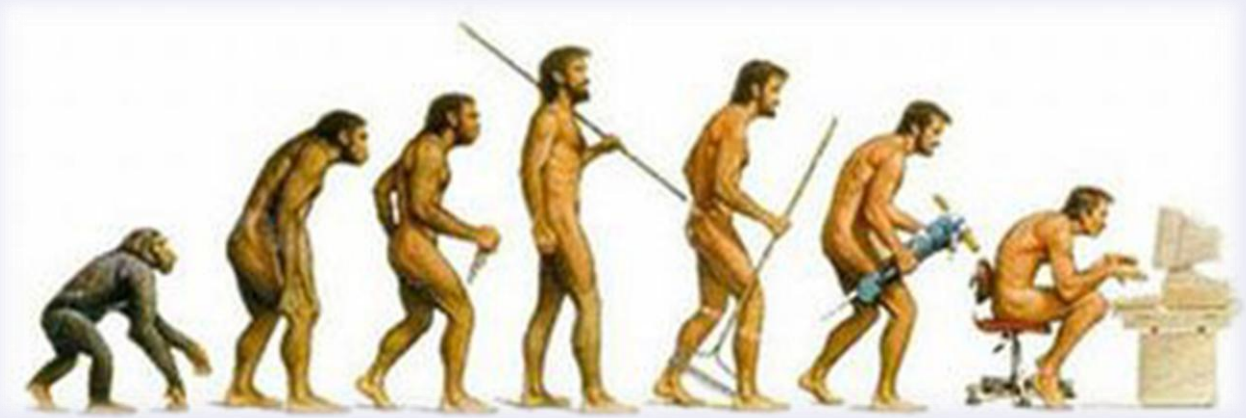
引子

OWASP 中国
The Open Web Application Security Project

这一切，都源于生产工具的变化

我们已经离不开的生产工具：

- 电脑
- 网络



(ISC)²

主要内容

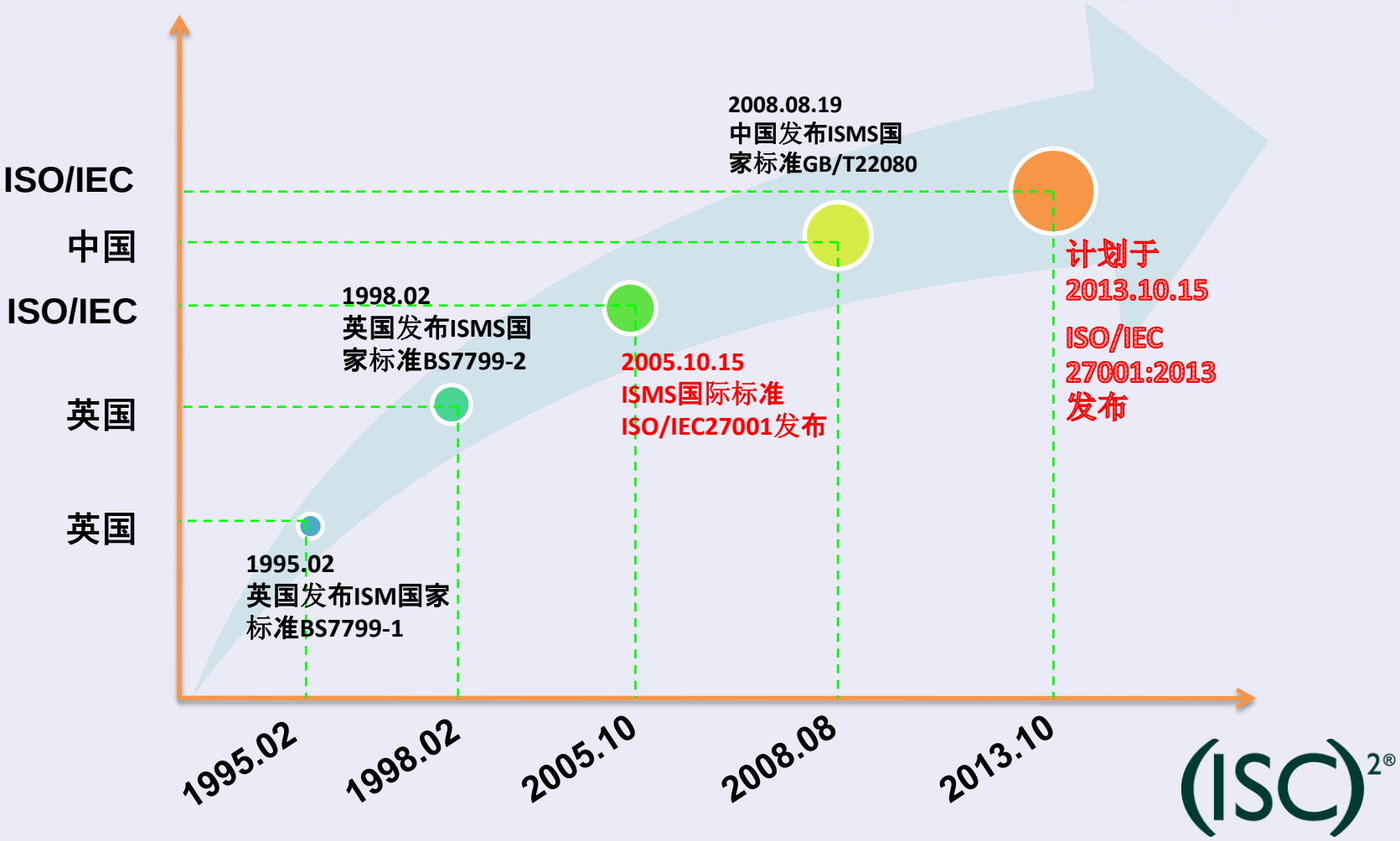
OWASP 中国
The Open Web Application Security Project

- 27001的来龙去脉
- 27001的新变化
- 新版27001中的信息安全人力资源要求

(ISC)²

27001的来龙去脉

OWASP 中国
The Open Web Application Security Project



(ISC)²

27001家族

27001 ISMS要求

- 27000 基础和术语
- 27002 实用规则
- 27003 ISMS实施指南
- 27004 控制措施测量
- 27005 风险管理
- 27013 与20000整合实施

支持标准和指南

- 27006 认可要求
- 27007 ISMS审核指南
- 27008 控制措施审核员指南

认证要求和指南

- 27009 认证认可服务
- 27010 部门和组织间通信
- 27011 电信
- 27014 信息安全治理
- 27015 金融服务
- 27016 信息安全经济
- 27017 云服务安全
- 27018 云服务数据保护

行业要求和指南

- 27031
- 27032
- 27033
- 27034
- 27035
- 27036
- 27037
- 27038
- 27039
- 27040
- 27041
- 27042
- 27043
- 27044

控制指南

2703x-4x

标准序号	标准名称
27031	业务连续性中的ICT就绪指南 Guidelines for ICT readiness for business continuity
27032	网际安全指南 Guidelines for cybersecurity
27033	安全评估测试准则 Security evaluation, testing and specification
27034	应用安全 Application security
27035	信息安全事件管理 Information security incident management
27036	供应链信息安全 Information security for supplier relationships
27037	数字证据的识别、手机、获取和保护指南 Guidelines for identification, collection, acquisition and preservation of digital evidence
27038	数字编辑规范 Specification for digital redaction
27039	入侵检测和防范系统的选择、部署和操作 Selection, deployment and operations of intrusion detection and prevention systems
27040	存储安全 Storage security
27041	确保适当和充分的事件调查方法指南 Guidance on assuring suitability and adequacy of incident investigation methods
27042	数字证据分析和解释指南 Guidelines for analysis and interpretation of digital evidence
27043	事件调查原则和流程 Incident investigation principles and processes
27044	安全信息和事件管理指南 Guidelines for Security Information and Event Management

(ISC)²®

ISO/IEC JTC1/SC27

OWASP 中国
The Open Web Application Security Project

工作组	分工范围
WG 1	信息安全管理体系 Information security management systems
WG 2	密码和安全机制 Cryptography and security mechanisms
WG 3	安全评估测试准则 Security evaluation, testing and specification
WG 4	安全控制措施和服务 Security controls and services
WG 5	标识管理和隐私保护技术 Identity management and privacy technologies

(ISC)²®

ISO/IEC JTC1/SC27/WG1专家

主要内容

OWASP 中国
The Open Web Application Security Project

- 27001的来龙去脉
- **27001的新变化**
- 新版27001中的信息安全人力资源要求

(ISC)²

27001修订背景

OWASP 中国
The Open Web Application Security Project

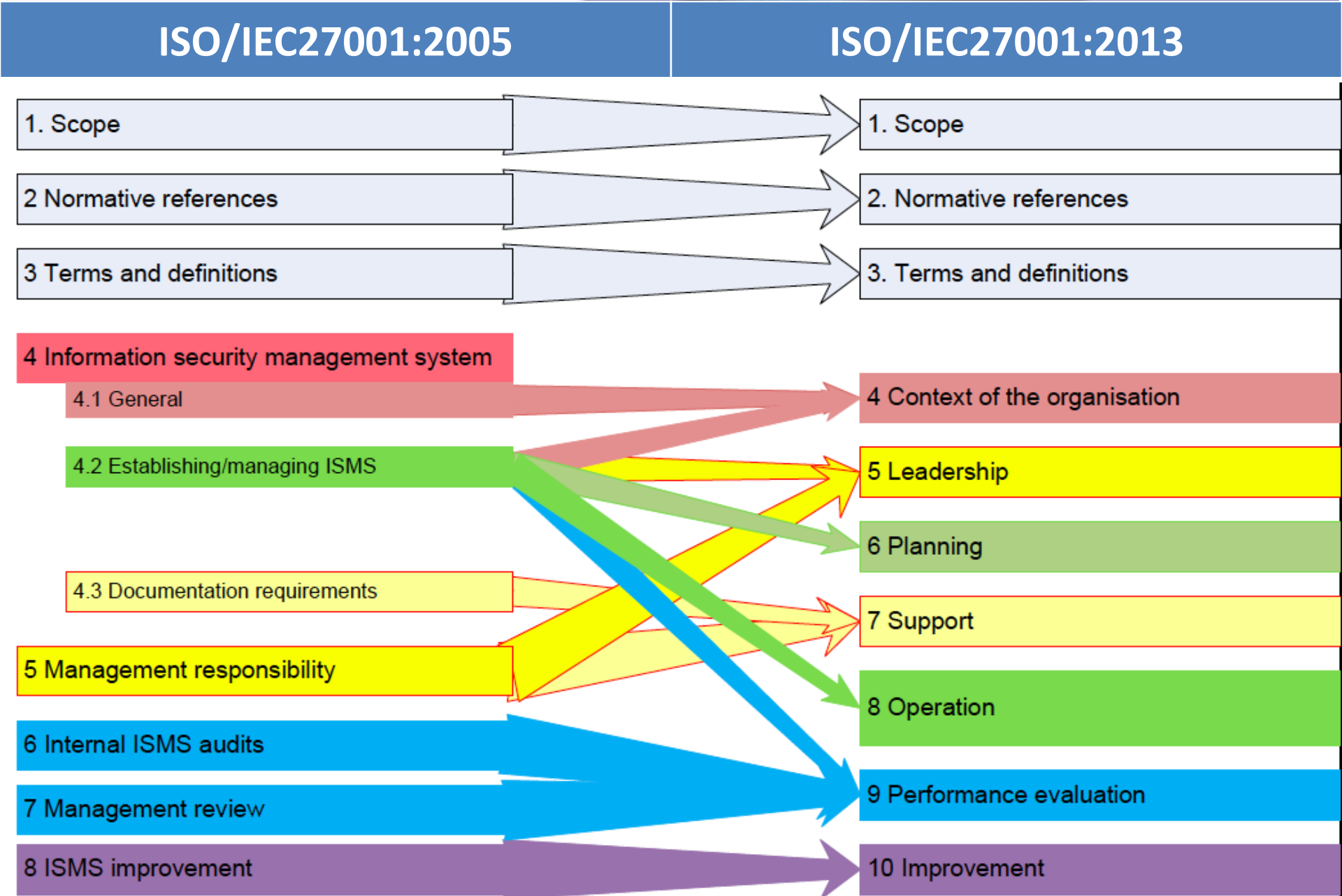
- ISO国际标准修订周期为5年，2009年SC27/WG1启动27001修订；
- ISO/TMB/JTCG MSS整合项目，将目前现行的管理体系（MS）标准，如ISO9000，ISO14000，ISO22000，ISO28000等，进行整合，统一结构，同一文本；
- 2010年，SC27/WG1决定采用MSS的统一结构和同一文本，修订27001；
- 2013年4月，在法国Sophia Antipolis的ETSI举行的SC27/WG1第46届全体会议上通过决议，将27001的FDIS提交JTC1，进行为期2个月的投票，如投票通过，计划于2013年10月发布新版本。

(ISC)²

27001结构变化


27001:2005与2013
结构对比
27001:2005
0 引言
1 范围
2 规范性引用文件
3 术语和定义
4 信息安全管理体系
5 管理职责
6 ISMS内部审核
7 ISMS的管理评审
8 改进ISMS
附录 A
附录 B
附录 C
参考文献
27001:2013
0 引言
1 范围
2 规范性引用文件
3 术语和定义
4 组织环境
5 领导
6 策划
7 支持
8 运行
9 绩效评价
10 改进

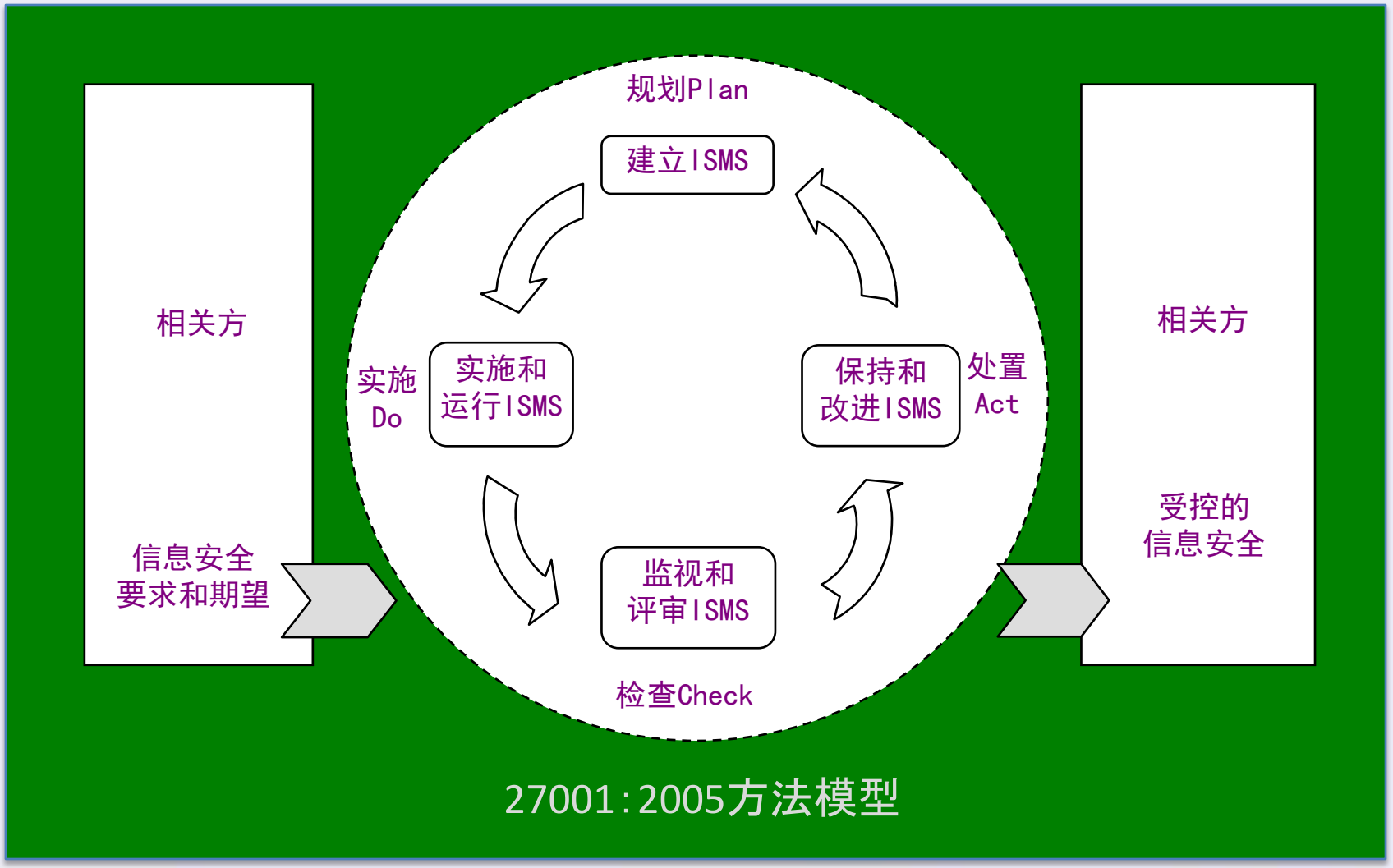
27001内容变化


ISO/IEC27001:2005
ISO/IEC27001:2013
1. Scope
2 Normative references
3 Terms and definitions
4 Information security management system
4.1 General
4.2 Establishing/managing ISMS
4.3 Documentation requirements
5 Management responsibility
6 Internal ISMS audits
7 Management review
8 ISMS improvement
1. Scope
2. Normative references
3. Terms and definitions
4 Context of the organisation
5 Leadership
6 Planning
7 Support
8 Operation
9 Performance evaluation
10 Improvement

27001附录A内容变化

27001方法变化

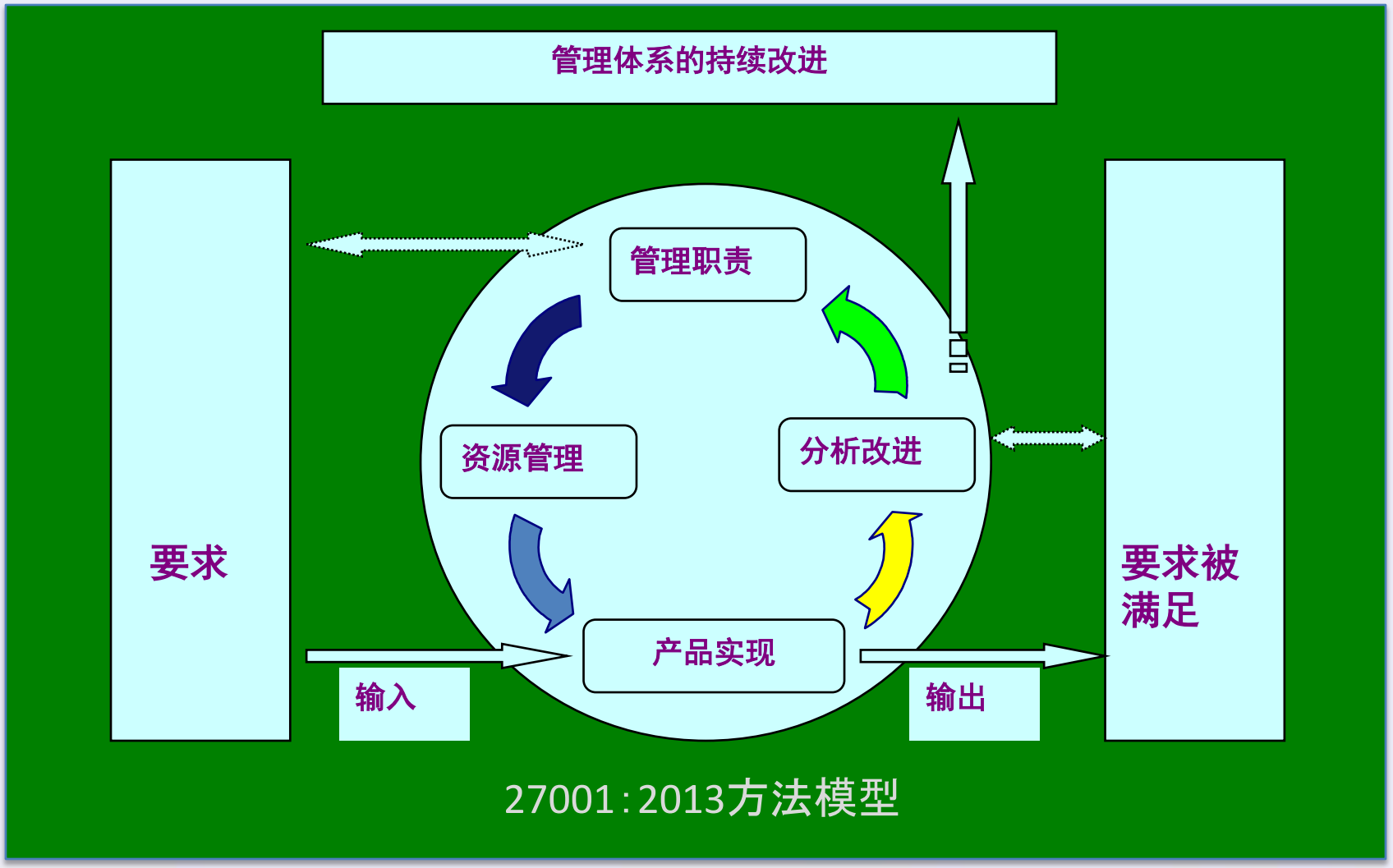
OWASP 中国
The Open Web Application Security Project



27001:2005方法模型

27001方法变化

OWASP 中国
The Open Web Application Security Project



27001:2013方法模型

主要内容

OWASP 中国
The Open Web Application Security Project

- 27001的来龙去脉
- 27001的新变化
- **新版27001中的信息安全人力资源要求**

(ISC)²

新版27001中的信息安全人力资源要求

OWASP 中国
The Open Web Application Security Project

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

确定在其管理下对其信息安全绩效有影响的人员所需的必要能力；

(ISC)²

新版27001中的信息安全人力资源要求

OWASP 中国
The Open Web Application Security Project

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

确保他们经过适当的教育、培训，或相应的经验积累具备能力；

(ISC)²

新版27001中的信息安全人力资源要求

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

如适用，应为取得这些必要能力采取行动，并评估这些行动的有效性；

新版27001中的信息安全人力资源要求

d) retain appropriate documented information as evidence of competence.

存档作为能力的证明。

CISSP®等认证是满足27001人力资源要求的最佳途径

(ISC)²®

CISSP®会员和准会员

OWASP 中国
The Open Web Application Security Project

- 具备超过4-5年的信息安全专业工作经验；
- 掌握全球认可的信息安全专业知识；
- 通过公正、严格的专业考试；
- 遵守(ISC)²职业道德规范；
- 维持认证所需的持续专业发展（CPE）学分。

(ISC)² ASSOCIATE

(ISC)²®

CISSP®认证带给您的利益

OWASP 中国
The Open Web Application Security Project

CISSP®

- 展示信息安全领域的专业应用知识；
- 脱颖而出，在业界拥有更高的声誉和竞争力；
- 享受(ISC)²会员的专享权益，扩大人际交往和增进互动交流；
- 获得更好的职业发展机会和更具竞争力的薪水；
- 满足政府和企业对信息安全认证的特定要求。

(ISC)²®

(ISC)²研讨会广告

OWASP 中国
The Open Web Application Security Project

(ISC)² The Driving Force in Security.

SecureShanghai@信息安全人才培养研讨会 （上海站）主办单位	SecureBeijing@信息安全人才培养研讨会 （北京站）主办单位
(ISC)² 上海交通大学 信息安全工程学院	(ISC)² 中国科学院高能物理研究所 Institute of High Energy Physics Chinese Academy of Sciences
时间：2013 年 7 月 31 日 （周三）	时间：2013 年 8 月 2 日 （周五）
地点：上海市华山路 1954 号上海交通大学 信息安全工程学院（徐汇校区）	地点：北京市石景山区玉泉路 19 号乙中国科学院 高能物理研究所主楼 C305 会议室
参会费用： 免费	参会费用：免费

(ISC)²

Q & A

OWASP 中国
The Open Web Application Security Project

感谢聆听，敬请斧正！

王新杰
wxinjie@isc2.org

(ISC)²