《信息安全管理》知识点串讲

一、信息安全管理基础

1. 管理的概念：组织、协调、控制的活动，核心**过程的管理**控制。
2. 管理对象和组成：包括人员在内的相关资产；组成包括人员、目标、规则和运行。
3. 管理体系概念：**完备性**、**逻辑性**的管理措施的集合，遵守“木桶原理”。
4. 信息安全管理体系：

1）根据 **ISO/IEC 27001** 所制定的体系，为狭义的体系。

2）广义信息安全管理体系：泛指一切与信息安全管理有关的措施的集合。

5. 信息安全管理的作用，包括不限于这些作用：

1）促进**业务目标**的实现；2）管理与组织整体**的融合**；3）**预防**、阻止和减少事件发生的作用；4）技术和管理的结合；5）**对内**和**对外**的作用。

6. 信息安全管理的成功要素：包括不限于的要素 1）反应**业务目标**；2）**文化**的一致性；3）领导层**实质性的支持**；4）领导对**风险管理**的理解；5）**科学的测量**体系；6）持续的**教育和培训**。

二、信息安全风险管理

1. 风险管理的概念：**识别**和**处置**风险的过程，是预防的措施。风险四要素是资产、威胁、脆弱性、安全措施。
2. 风险管理参考的方法：

1）**COSO** 风险控制框架：**战略**、**运营**、**报告和合规性**风险管理，具体包括组件。

2）ISO**31000** 的风险管理标准（国际标准工作参考），适用范围非常的广泛。

3）**ITIL** 信息技术服务（信息安全风险管理）：**服务战略**、**服务设计**、**服务转化**、**服务运营**、**服务改进**等五个阶段来实施。

4）**COBIT** 风险控制：通过 **IT 活动**风险控制支持 **IT 过程和 IT 目标，进一步支持业务目标（商业目标）**的实现。

3. 基于 **GB/Z 24364:2009** 的风险管理指南（**考试重点**）

1）四阶段：

— **背景建立**：风险管理准备、系统调查、系统分析、安全分析。

— **风险评估**：风险评估**准备**、风险要素识别（**资产**、**威胁**、**脆弱性**、**安全措施**）、风险分析、风险报告。

— **风险处理**：**降低**风险、**规避**风险、**转移**风险、**接受**风险。

— **批准监督**：对风险管理的认可；风险管理过程风险的控制。

2）两过程：

— **监控审查**：对风险管理过程的**偏差**、**变化**、**延误**进行**控制和纠正**。

— **沟通咨询**：提高风险管理的**质量**和效果的交流和沟通工作。

三、27001 信息安全管理体系（PDCA）

1.管理的方法：PDCA 过程的方法。

2.体系的四个阶段的内容：

3.体系文档的管理

1）规划和使用文档管理结构：3 层或 4 层结构，其中高层包括方阵、策略、手册；最底层包括文件表格、记录、表单等。

2）对文档要进行全生命周期的管理。

四、ISO/IEC 27002:2013 信息安全管理控制措施

1. 安全策略

1）制定策略：由领导批准和发布，代表宏观的要求和导向，高级别策略为方针。

2）策略评审：新制定、修订等需要进行评审，保证适宜性、充分性和有效性。

2. 安全组织

1）内部组织：角色分配、职责分离、与政府的联系、与利益方的联系、项目中的信息安全管理。

2）移动设备和远程办公：设备的安全，远程办公。

3. 人力资源安全

1）任用前：安全审查、岗位的定义。

2）任用中：职责管理、安全教育培训、纪律处理。

3）任用终止或变化：权限回收、信息保密等要求。

4. 资产安全

1）**资产**清单：设备资产的清单、责任人、可接受的使用、归还。

2）**信息**分类：数据资产的分类指南、信息标记、信息处理。

3）**介质**管理：移动介质管理、介质处置、介质传输的安全。

5. **操作安全**：核心为一切的操作均需要制定和执行相应的操作程序。

6. 供应商管理

1）供应商合作方针、信息安全问题的协议。

2）供应商的审查、供应商的服务变更管理。

7. **符合性管理**：安全管理要符合**政策、法律、法规、标准、知识产权、隐私保护、审计、技术审核**等要求。

8. 访问控制（结合参考访问控制知识）

9. 密码技术管理（结合参考密码学知识）

10. 物理和环境安全（结合参考物理环境安全）

11. 通信安全（结合参考网络通信安全）

12. 事件安全管理（详细参考《业务连续性管理》）

13.业务连续性管理（详细参考《业务连续性管理》）
14.系统获取开发和维护（结合参考安全工程过程）

五、信息安全管理测量

1. 重要性：衡量安全有效性的必须的，闭环的关键方法。
2. 测量方法：**ISO/IEC 27004** 的管理测量的标准（对象-过程-措施-目标）。
3. 测量过程：测量职责分配等准备-制定测量方案-测量的实施-测量分析与报告-测量的改进。

温馨提示：为了减少学习的负担和聚焦核心，知识点总结写的是关键的精要的要点，并非是知识点的全文，请一定进一步结合官方的教材进行扩充补充、理解和掌握全面，以免产生以偏概全的问题。

（END）