2021年软考-高项

信息系统项目管理师

论文写作专题

-12安全管理#论文写作思路

讲师:朱建军（江山老师）

信息安全*历年考题子题目要求

1、2012年下半年考题

请以“论构建信息系统安全策略问题，分别从以下三个方面进行论述”：

1、概要叙述你参与管理过的信息系统项目（项目的背景、项目规模、发起单位、目的、项目内容、组织结构、项目周期、交付的产品、项目安全需求等）

2、围绕以下两方面，结合项目实际论述构建信息系统安全策略的基本内容

（1）构建信息安全策略的核心内容

（2）构建信息安全策略的设计原则

3、请结合论文中所提到的信息系统项目，**简要论述项目中涉及的几种具体的安全策略**。并指出其中可以进一步改进之处。

【江山老师点评】对于本题的写作，江山老师认为此题有一定的难度。

如果非要写，请把安全管理相关内容学习下，针对问题2和3作答。此题不需要掌握。

信息安全*历年考题子题目要求

2、2017年下半年考题

请以“信息系统项目的安全管理”为题，分别从以下三个方面进行论述：

1、概要叙述你参与过的或者你所在组织开展过的信息系统相关项目的基本情况（项目背景、规模、目的、项目内容、组织结构、项目周期、支付成果等），并说明你在其中承担的工作。

2、结合项目实际，论述你对项目安全管理的认识，可以包括但不限于以下几个方面。

(1)信息安全管理的主要工作内容。

(2)信息安全管理中可以使用的工具、技术和方法等。

(3)信息安全管理工作内容、使用的工具、技术和方法如何在项目管理的各方面（如人力资源管理、文档管理、沟通管理、采购管理）得到体现。

3、请结合论文中所提到的信息系统项目，**介绍你是如何进行安全管理的，包括具体做法和经验教训。**

【江山老师点评】写这个题目的考生应该很少的，当然，这也是我们平时不需要掌握的内容

信息安全*历年考题子题目要求

3、2019年上半年考题

试题一论信息系统项目的风险管理与安全管理

项目风险是一种不确定的事件和条件，一旦发生，对项目目标产生某种正面或负面的影响。信息系统安全策略是指针对信息系统的安全风险进行有效的识别和评估后，所采取的各种措施和手段，以及建立的各种管理制度和规章等。

请以“论信息系统项目的风险管理与安全管理”为题，分别从以下三个方面进行论述：

1、概要叙述你参与管理过的信息系统项目（项目的背景、项目规模、发起单位、目的、项目内容、组织结构、项目周期、交付的成果等），并说明你在其中承担的工作。

2、结合项目管理实际情况并围绕以下要点论述你对信息系统项目风险管理和安全管理的认识。

（1）项目风险管理和安全管理的联系区别。

（2）项目风险管理的主要过程和方法。

（3）请解释适度安全、木桶效应这两个常见的安全管理中的概念，并说明安全与应用之间的关系。

3 请结合论文中所提到的信息系统项目，**介绍在该项目中是如何进行风险管理和安全管理的（可叙述具体做法），并总结你的心得体会。**

适度安全的观点:怎样才是适度安全，需要运用风险评估的方法才能得出结论。风险评估围绕威胁、资产、脆弱性、安全措施展开分析。在评估时不仅要考虑现有环境，还要考虑近期和远期发展变化趋势。同时，还要评估控制风险所需的安全代价。在此基础上对风险和代价进行均衡，才能确定相应的安全策略。安全风险和安全代价两者之间的关系，可用图表示。

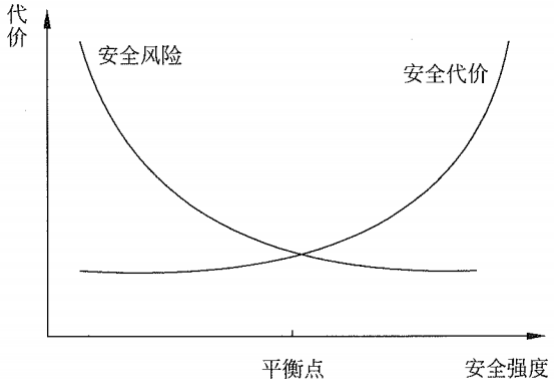

图 22-1　安全风险和安全代价之间关系

从图中不难看出，**安全代价低，显然安全风险肯定很大；反之，安全风险要降得很低，安全的代价也就很大。这个代价不光指资金投入，包括系统性能下降、效率低下等引出的“代价”。一个好的信息安全保障系统的标志就是有效控制两者的“平衡点”，既能保证安全风险的有效控制，又使安全的代价可以接受。这个平衡点对于不同行业、不同单位、不同时间点都不一样，需要实现“动态”控制。三种不同架构的信息安全保障系统和网络信息安全的等级保护等的理念和建设方案，都是适度安全的观点的体现。**

第三版教材P610-611

木桶效应的观点:是将整个信息系统比作一个木桶，其安全水平是由构成木桶的最短的那块木板决定的。同时，**保护信息系统的各个安全要素是同等重要的，各方面要素均不容忽视。但是要强调的是，安全管理在所有要素中具有极其重要的地位。有人将安全管理的漏洞比作存在于木桶桶底的漏洞。如果安全管理有漏洞，其他安全措施即使投入再大也无济于事。**

信息安全*历年考题子题目要求

2019年上考核了安全管理是和风险管理一起，考察了风险管理和安全管理的区别联系，木桶效应；

要论述什么是风险管理？什么是安全管理？以及它们之间的联系如有些项目风险对项目的信息安全造成了威胁，也是信息安全管理的重点。反过来，科学的安全管理，可以大大加强项目的风险管理，提高项目成功的可能性，提高项目的价值。

2017年下考核了安全管理的主要内容，工具、技术和方法，如何在项目管理的各方面体现等内容。

2012年下考核主要侧重于安全策略的核心内容和设计原则。

写作思路：

总体来说，安全管理的论文写作思路其实是和项目管理十大领域是一样的，具体采用了哪些安全策略，策略的具体情况如何，策略使用的效果如何。子标题可以用人机料法环搞五个子标题，也可以以安全机制，安全服务，安全管理为子论题架构论文。

信息安全管理可考的子题目列举

1、安全管理的重要性、安全管理的方法

2、安全策略的内容、设计原则?P609-611、613-614

3、信息安全管理的主要工作内容、可以使用的工具、技术和方法等

4、请解释适度安全、木桶效应这两个常见的安全管理中的概念，并说明安全与应用之间的关系。P610-611

5、如何根据安全等级保护原则去设计系统P611

6、信息系统安全方案？P614-615

7、信息安全系统的组成？P617

8、信息安全系统工程与安全管理的关系？P624

9、访问控制？P651-656

10、如何实施安全审计？P659-660

11、您所做信息系统项目中常用的安全问题、原因、及应对措施?

历年论文子题目参考范例

1、信息安全管理的主要工作内容(2017年下)

参考要点：

1.制订信息安全方针政策
2.建立管理框架
3.建立人力资源安全管理，减少盗窃滥用误用风险
4.对组织资产进行保护，实现资产管理安全
5.进行访问控制，确保对信息，信息处理设施和业务过程访问基于业务和安全需求
6.通过加密来保护信息的保密性，真实性和完整性
7.通过物理环境安全管理，防止对组织办公场所和信息的非授权的物理访问
8.确保信息处理设施的正确和安全操作，实现运行安全
9.确保网络中信息和支持性基础设施得到保护，实现通信安全
10.确保信息系统获取，开发和使用安全
11.与供应商签订协议，确保供应商访问组织资产的合理性和安全性
12.通过流程确保安全事件得到有效处理
13.通过安全手段的实施，确保业务的持续性
14.避免违反法律法规，规章合同要求和其他安全要求

历年论文子题目参考范例

2、构建信息安全策略的核心内容(2012年下)

参考要点：

1.定方案：和供应商一起制订系统安全方案

2.定岗：使用设置专门的岗位

3.定位：明确岗位职责和职位

4.定员：明确岗位职责和职位人员

5.定目标：明确信息安全管理所要达到的目标

6.定制度：制订信息安全管理制度

7.定工作流程：制订与信息安全管理制度配套的工作流程。

总结：构建信息安全策略的核心内容就是上面的七定。

历年论文子题目参考范例

3、构建信息安全策略的设计原则(2012年下)

参考要点：

1.主要领导人负责原则：各部门一把手必须把信息安全列为其最关心的问题

2.规范定级原则：应按标准确定信息安全管理要求的相应等级

3.依法行政原则：必须保证信息系统安全行政主体合法

4.以人为本的原则：加强对使用者的安全教育，培训和管理。

5.注重效费比原则：恰当把握安全需求和资源投入之间的平衡点

6.全面防范突出重点原则：既需要全面防范又需要突出管理重点。

7.系统动态原则：从系统工程的角度实施安全管理，同时根据情况变化采取恰当的安全措施。

8.特殊安全管理原则：必须遵循安全管理的特殊原则。

历年论文子题目参考范例

4、信息安全管理如何在项目管理的各方面（如人力资源管理、文档管理、沟通管理、采购管理）得到体现(2017年下)

参考要点：

1.在人力资源管理方面，我们要求凡是参与本项目的任何人员都需要经过资格审查并与公司签订保密协议；

2.在文档管理方面，初审，复审和归档由不同的人员操作；

3.在沟通管理方面，我们制定了沟通管理细则，涉及机密或影响信息安全管理方面的内容，一律不得随意外发；

4.在采购管理方面，我们严格实行供应商的准入制度和原件查验制度，与中标供应商除签署双方履约合同外，还需要签署保密协议。

总体来说，我们力求把信息安全管理与项目管理各方面结合起来，在确保安全的前提下实现了项目的成功建设。

历年论文子题目参考范例

5、信息安全管理中可以使用的工具、技术和方法等(2017年下)

参考要点：

1.在主机和操作系统安全管理规范方面，没有项目经理批准任何人不得擅自关闭或重启操作系统。
2.在网络和数据库管理方面，禁止一切非本公司人员自带电脑接入公司内部的网络。
3.在应用输入和输出管理规范方面，使用动态口令，数据传输加密和数据存储加密等相关技术。
4.在应用开发保密方面，我们要求所有参与开发和实施的人员都必须签订保密协议。
5.在应急事故管理规范方面，我们根据经常出现的一些问题开发了对应的应急预案。
6.在密码和安全设备管理规范方面，我们制定了两个人掌握数据库管理员密码的一部分，互相不透露。
7.在信息审计管理规范方面，我们制订了任何人不得以任何理由威胁或左右审计人员执行审计工作。

历年论文子题目参考范例

6、信息系统安全的威胁主要来源于哪几个方面?

参考要点:

一是对信息系统设备的威胁

二是对业务处理过程的威胁

三是对数据的威胁

7、为什么要进行安全管理?

参考要点:

1.由于信息的价值越来越高，建设的信息系统越来越多，所以大家越来越关注信息安全问题。

2.信息安全问题主要是从技术和管理的角度来确保信息的保密性，完整性，可用性，不可抵赖性。

3.信息系统的安全里管理需要多方位进行，包括物理安全管理，人员安全管理，应用系统安全管理等方面都需要构建切实可行的安全策略。

历年论文子题目参考范例

8、安全设计原则的内容有哪些

参考要点：

1. 木桶原则

对信息进行均衡全面的保护，它最大的容积取决于最短的一块木板。攻击者一般使用最容易渗透的原则，一般选择在系统最薄弱的地方进行攻击。因此充分，全面，完整的对系统的安全漏洞和安全威胁进行分析，评估和检测是设计安全系统的必要前提条件。安全机制和安全服务的设计首要目的是防止最常用的攻击手段，根本目的是提高整个系统安全最低点的安全性能。

2. 整体性原则

要求在被攻击，被破坏事件时，必须尽可能地快速恢复，减少损失。安全检测机制会检测系统的运行情况，及时发现和制止系统所受到的各种攻击。

安全恢复机制会在安全防护机制失效的情况下，进行应急处理，尽量及时地恢复信息，降低供给的破坏程度。

3. 安全性评价与平衡原则

安全体系设计要正确处理需求，风险与代价的关系，做到安全性与可用性相容，做到组织上可执行。对于信息是否安全，没有绝对评判标准和度量指标，只能取决于系统的用户需求和具体的应用环境，具体取决于系统的规模和范围，系统的性质和信息的重要程度。

4. 标准化与一致性原则

设计安全体系必须遵循一系列的标准，这样才能保证各个分系统的一致性。使整个系统安全地互联互通，共享信息。

5. 技术与管理相结合的原则

安全体系是一个复杂的系统工程，涉及人技术，操作等要素；单靠技术和单靠管理都不可能实现，因此必须将各种安全技术和运行管理机制，人员思想教育和技术培训，安全规章制度的建设相结合。

6. 统筹规划步步实施的原则

安全防护不可能一步到位，但可以在一个比较全面的安全规划下，根据实际需要，先建立基本安全体系，保证基本的必须的安全性，今后随着规模扩大和应用的增加，网络脆弱性会不断增加，需要调整或增强安全防护的力度，保证整个网络的最根本的安全需求。

7. 等级性原则

是指安全层次和安全级别。良好的信息安全系统必然是分为不同等级的，包括对信息保密程度分级，对用户操作权限分级，对网络安全程度分级，对系统实现结构的分级，从而针对不同级别的安全对象，提供全面可选的安全算法和安全体制，以满足不同需求。

8. 动态发展原则

要根据变化不断调整安全措施，以适应新环境新需求。

9. 易操作性原则

安全措施需要人去实施，去完成，但如果措施过于复杂，对人的要求过高，那么这本身就降低了安全性。

历年论文子题目参考范例

9、安全需求的内容有哪些?

参考要点:

安全需求有下面的五个内容：身份认证，授权控制，数据加密，数据完整性和抗抵赖性。

1. 身份认证

它是授权控制的基础，身份认证必须做到准确无二义地将对方辨别出来。提供双向认证，即互相证明自己的身份。在单机下身份认证主要分为三种类型：一是双方共享某个秘密信息如用户口令；二是采用硬件设备来生成一次性口令；三是根据人的生理特性如指纹声音来识别。

在网络状态下身份验证更加复杂，主要考虑验证身份的双方一般都是通过网络而非直接交互。目前一般采用基于对称密钥或公开密钥加密的方法。

2. 授权控制

是控制不同用户对信息资源访问权限，对授权控制要求：一致性，即没有二义性；统一性，对信息资源集中管理，统一贯彻安全策略；要求有审计功能，对所有授权记录可以核查。

3. 数据加密

有两大类：一类是对称密钥加密算法，另一类是基于非对称密钥加密算法。

加密手段可以分为硬件加密和软件加密法。硬件加密速度快效率高，安全性好，成本高；软件加密成本低且灵活。密钥管理包括了密钥产生分发更换。

4. 数据完整性

网上传输的数据应防止被修改，删除，插入，替换或重发。以保证合法用户接收和使用该数据的真实性。

5. 防抵赖性

通常采用数字签名，接收方确保对方不能够抵赖收到的信息是其发出的信息。

历年论文子题目参考范例

10、请解释适度安全、木桶效应这两个常见的安全管理中的概念，并说明安全与应用之间的关系。(2019年上)

参考要点：

木桶理论： 保护信息系统的各个安全要素是同等重要的，各方面要素都不可以忽视，安全管理在所有要素中有极其重要的地位。有人将安全管理的漏洞比作存在于木桶桶底的漏洞。如果安全管理有漏洞，其他的安全措施即使投入再大也无济于事。

适度安全的观点： 安全代价低，那么显然安全风险肯定很大，反之安全风险要降得很低，安全的代价也要很大。一个好的信息安全保障系统的标志就是有效控制两者的平衡点。既能保证安全风险的有效控制，又要使安全的代价可以接受。 三种不同架构的信息安全保障系统，网络信息安全等级保护等理念，都是适度安全的观点的体现。

安全与应用之间的关系：

应用需要安全，安全为了应用。

安全和应用是矛盾统一的。没有应用就不会产生相应的安全需求，发生安全问题，就不能更好地开展应用。

另外安全是有代价的，不但会增加系统的开销，也会增加系统建设和运行的费用。同时还会规定对使用的限制，从而给应用带来不便。

11、项目风险管理和安全管理的联系区别(2019年上)

参考要点：

随着互联网高速公路的畅通和国际化的信息交流，业务大范围扩展，信息安全的风险也急剧恶化。由业务信息系统来解决安全已经不能胜任。根据风险度的观点，我们不能一厢情愿的追求所谓的绝对安全，而是要将安全风险控制在合理程度或允许的范围内。

历年论文子题目参考范例

管理心得与不足之处

1.有规矩方能成方圆，一定要订立科学合理的信息安全管理制度

2.信息安全是一个系统工程，需要从多方面入手来系统防范

3.要有专人负责安全信息体系的落实执行

不足之处：

1.容灾和备份方案还不十分完善，应该尽快考虑和实施异地灾备

2.信息安全责任的落实如何和个人绩效更好的挂钩，还需要在考核体系中进一步完善。

绩效管理*历年考题子题目要求

项目的绩效管理，应该算是一个冷门论文考点了吧，官方教材上没有专门的教材说这部分内容。而且历年来总共就考察了两次，07年考了组织级的项目管理的绩效考核，9年后的16年下，考了项目的绩效管理。项目绩效管理的流程和方法是重要的考核点两次都涉及到了。07年的绩效中还考核了在绩效管理中遇到了什么问题。还考虑哦项目考核的优点是什么？这个理论知识。相比16年的绩效管理，07年考核的是组织级的项目绩效管理，所以在难度上比16年的论文高了很多。

此部分大家了解即可，不用学习，不需要准备！

绩效管理*历年考题子题目要求

1、论信息系统项目的绩效管理（2016年下）

绩效管理是任何组织都必须要面对的问题，是组织管理的重要组成部分。作为项目经理或项目团队的相关负责人员，不仅必须要关注项目绩效，激发员工的活力，并且还需要定期或不定期地对项目的绩效进行考核，保证项目能够按照预期的计划实施。如何有效地实施项目绩效管理，充分发挥项目团队每个成员的积极性，是项目经理在管理项目时必须面对的一项重要任务。

请以“信息系统项目的绩效管理”为题，分别从以下三个方面进行论述：

1、简要说明你参与的信息系统项目的背景、目的、发起单位的性质，项目的技术和运行特点、项目的周期、绩效管理的特点，以及你在项目中的主要角色和职责。

2、结合你参与的项目，论述项目绩效管理的流程、方法、以及使用的基本工具。

3、根据你的项目绩效管理实践，说明你是如何进行项目绩效管理的，有哪些经验和教训。

绩效管理*历年考题子题目要求

2、论组织级项目管理的绩效考核（2007年下）

目前，虽然项目管理的理念已经深入人心，但是项目管理在每个单位的实施程度却是参差不齐。有的单位已全面引入了项目管理制度，已经在按项目进行考核，项目经理的地位也得到了加强，单位也尝到了实施项目管理的好处。但是，很多单位对项目的组织形式还是弱矩阵，即项目经理责任很大，权限很小，这不利于项目的实施。

请围绕“组织级项目管理的绩效考核”论题，分别从以下三个方面进行论述：

1.介绍你所在单位信息系统项目管理的现状（项目管理制度和流程、项目的组织形式）。

2.阐述项目考核的优点是什么？在项目考核过程中会遇到哪些问题？

3.论述你单位项目的人力资源绩效考核的目的、流程和效果。

绩效管理*子题目参考要点

1.结合你参与的项目，论述项目绩效管理的流程，方法，以及使用的基本工具。（2016年下）

参考要点：

在项目开始时，我们就梳理出了项目绩效管理的基本流程。

第一步，绩效考核动员。让被考核者理解绩效考核对自身的好处，让他们从心底里乐于接受考核。

第二步，绩效考核办法的制定。围绕岗位职责和工作内容，和被考者一起制订合理，科学的绩效考核办法。

第三步，绩效考核方法的宣传，让被考核者充分了解绩效考核指标。清楚自己的行动方向。

第四步，绩效考核的辅导。根据工作需要进行培养和辅导，让被考核者具备胜任绩效指标要求的能力。

第五步，绩效考核的进行，工作结束后，不折不扣，公平公正公开地执行绩效考核办法。

第六步，绩效考核的面谈，让被考核者知道自己的考核结果，并向其解释考核结果，指出其成绩和待改进的地方。

第七步，绩效考核的总结。总结绩效考核办法和绩效考核过程中的经验和不足，作为下一个绩效考核周期内绩效考核改进的依据。

工具：发放奖金，授予荣誉证书，赢取外派学习的机会，晋升等。

2.阐述项目考核的优点是什么？在项目考核过程中遇到哪些问题？（2007年下）

参考要点：

优点：通过项目考核，我们明显感觉到项目的利润率提高了，客户满意度提升了，计划准确性也提高了。对个人而言原来干多干少一个样，每月拿固定工资，实施项目考核后，技术好，工作积极和出活多的员工收入明显增加，这些员工大受项目经理的欢迎，这样也迫使那些后进的员工积极提升技术能力，主动索取工作任务以及增强自己的团队合作意识。

遇到的问题：个别项目经理和个别项目组成员比较短视，为了得到公司对项目组或项目经理对个人工作绩效的更好评价，他们有时候会以牺牲项目质量为代价而赶工赶进度，这样给项目的后续工作带来了一定程度的不利影响。另外由于有些考核指标在准确量化上还存在一些偏差，时常也导致考核者与被考核者之间一些矛盾和不满情况的发生。

绩效管理*子题目参考要点

3.论述你单位项目的人力资源绩效考核的目的，流程和效果。（2007年下）

参考要点：

效果：

员工工作面貌焕然一新，大家感觉更有奔头，员工离职率明显下降。

项目经理的工作轻松了不少，以前大家都不愿意当项目经理，现在想当项目经理的员工越来越多。

公司管理水平上了新台阶，企业核心竞争力明显增强，公司利润从2010年开始每年都保持在50%以上的增长速度。

目的：

我们考核的目的就是要激发大家的工作热情和工作贡献程度，激励员工提升技能，激励员工之间的良性竞争和精诚合作。

绩效管理*子题目参考要点

绩效管理的心得：

1）绩效考核永数据说话，提升了可信度喝大家的认可程度

2）项目管理制度一定要坚持执行，在执行中发现问题和不断改善。

3）设置的绩效考核指标只有把公司，项目组，项目成员三者的利益统一起来，才具有更强大的效用。

4）绩效考核的最终目标不是奖惩，而是改进工作绩效，因此绩效面谈很重要。

不足之处：

1）绩效考核办法不尽完善，个别急功近利的员工，想方设法钻考核办法的空子，损公肥私。

2）考核指标的量化程度还不够，这在一定程度上损害了个别优秀的员工的个人利益。

分论题解答

非常感谢您的聆听

加入正版课程获得VIP全套增值服务

问题咨询联系江山老师 QQ/微信：51815498 /915446173

江山老师答疑微信

官方公众号

备份公众号

扫一扫
加关注
抢先学
早拿证

微信扫码做题