光环国际
AURA INTERNATIONAL

《信息系统项目管理师》直播课2022.10.12

主讲老师：黄俊玲

目录

光环软考
AURA INTERNATIONAL

计算题进阶

光环国际
AURA INTERNATIONAL

资源优化题串讲

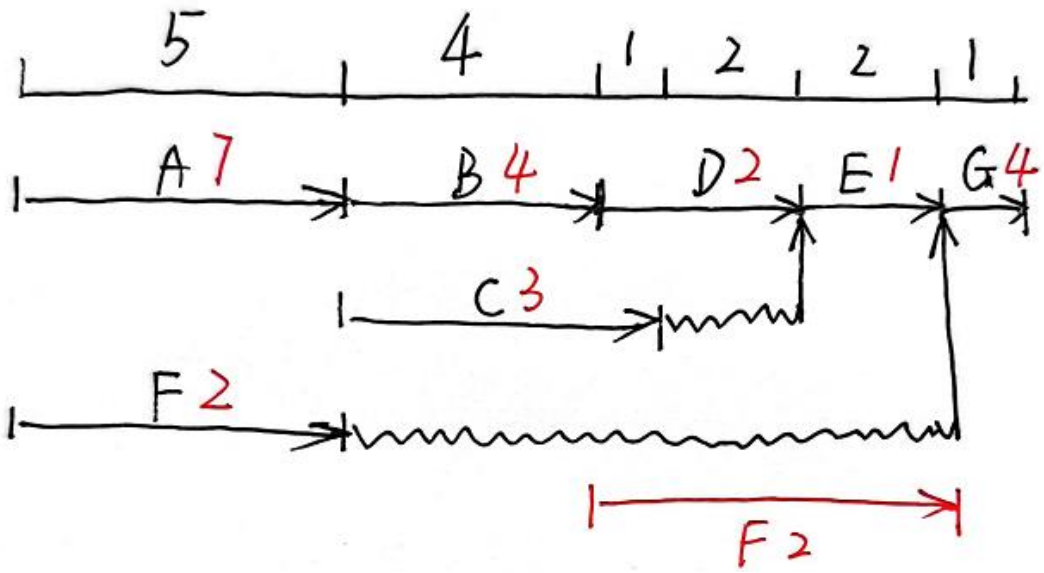
计算题-资源优化题

某工程包括A、B、C、D、E、F、G七项工作，各工作的紧前工作、所需时间以及所需人数如下表所示（假设每个人均能承担各项工作），该工程的工期应为（1）天。按此工期，整个工程最少需要（2）人。

(1)A. 13　B. 14C. 15D. 16
(2)A. 7 B. 8C. 9D. 10

工作	A	B	C	D	E	F	G
紧前工作	—	A	A	B	C、D	—	E、F
所需时间（天）	5	4	5	3	2	5	1
所需人数	7	4	3	2	1	2	4

解析：先找出关键路径，关键路径为ABDEG，则工期为5+4+3+2+1=15天
画时标网络图得知，最少7个人就可以完成了。
参考答案（C）、（A）



高项2022上半年

试题二

已知某公司承担一个旅游信息监管系统的开发。整个项自划分为四个阶段九项活动，项目相关信息如表所示：

（2）如果项目人员均为多面手，可以从事任意活动，请指出项目实施需要的最少人数。

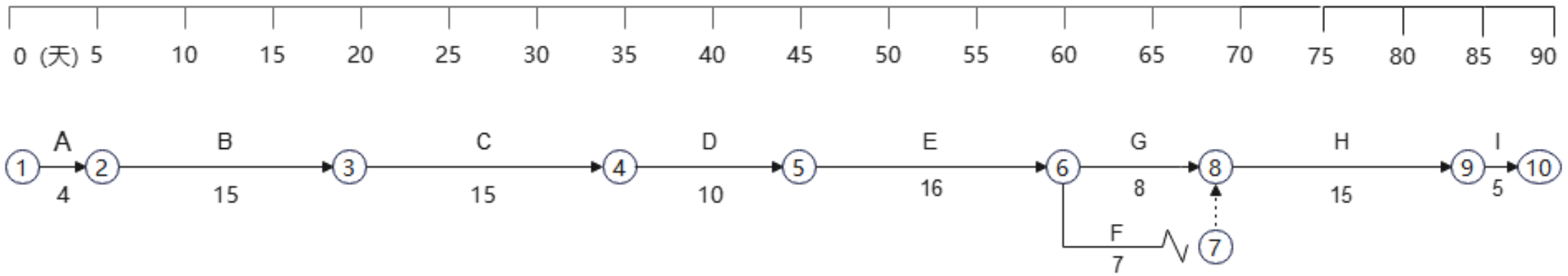
	活动名称	工期/天（乐观、可能、悲观）	紧前活动	人数/人	总预算（万元）
需求分析	A 任务下达	（1，4，7）		6	0.6
	B 需求分析	（12，14，22）	A	15	6.3
设计研发	C 总体设计	（13，14，21）	B	13	10.4
	D 初样实现	（8，9，16）	C	17	24.7
	E 正样研制	（10，17，18）	D	18	10.2
系统测试	F 密码测评	（6，7，8）	E	9	5.1
	G 软件测试	（5，8，11）	E	12	10.6
	H 用户试用	（9，16，17）	F、G	20	15.7
项目收尾	I 收尾	（3，5，7）	H	10	3

参考答案：

A=4；B=15；C=15；
D=10； E=16；F=7；G=8；H=15；I=5。

（2）参考答案：最少需要21人。

	活动名称	工期/天（乐观、可能、悲观）	紧前活动	人数/人	总预算（万元）
需求分析	A 任务下达	（1，4，7）		6	0.6
	B 需求分析	（12，14，22）	A	15	6.3
设计研发	C 总体设计	（13，14，21）	B	13	10.4
	D 初样实现	（8，9，16）	C	17	24.7
	E 正样研制	（10，17，18）	D	18	10.2
系统测试	F 密码测评	（6，7，8）	E	9	5.1
	G 软件测试	（5，8，11）	E	12	10.6
	H 用户试用	（9，16，17）	F、G	20	15.7
项目收尾	I 收尾	（3，5，7）	H	10	3



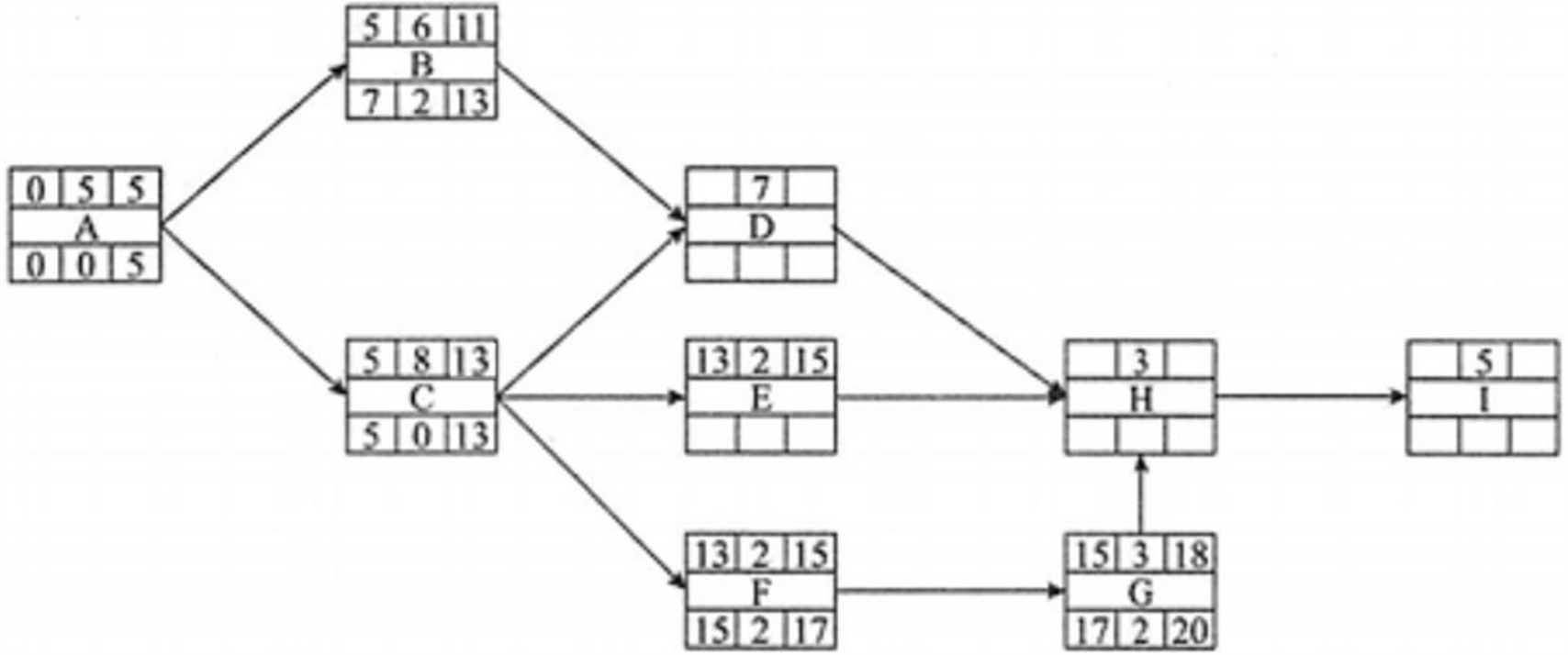
● 中项

试题二（共 17 分）

阅读下列说明，回答问题 1 至问题 3，将解答填入答题纸的对应栏内。

【说明】

项目经理根据甲方要求估算了项目的工期和成本。项目进行到 20 天的时候，项目经理对项目进展情况进行了评估，得到各活动实际花费成本（如下表所示）。此时 ABCDF 已经完工，E 仅完成了二分之一，G 仅完成了三分之二，H 尚为开工。



工作代号	紧前工作	估计工期	赶工一天增加的成本	计划成本	实际成本
A	无	5	2100	5	3
B	A	6	1000	4	7
C	A	8	2000	7	5
D	CB	7	1800	8	3
E	C	2	1000	2	3
F	C	2	1200	1	1
G	F	3	1300	3	1
H	DEG	3	1600	4	0
I	H	5	1500	5	0

【问题 1】（6 分）基于以上案例，项目经理得到了代号网络图，请将以上图补充完整。

【问题 2】（5 分）基于补充后的网络图

（1）请推出项目的工期、关键路径和活动 E 的总时差。

（2）项目经理现在想通过赶工的方式提前一天完成项目，应该压缩哪个活动最合适？为什么？

【问题 3】（6 分）请计算项目当前的 PV、EV、AC、CV、SV，并评价项目进度和成本绩效。

【问题 2】

（1）**答案：**工期 28 天；关键路径为 ACDHI；E 的总时差=20-15=5 天。

解析：考核关键路径的判断和总时差的算法以及工期压缩的选择。

（2）**答案及解析：**压缩 I，因为 I 是关键工作，且赶工成本最低。

【问题 3】

答案：按照网络图，到 20 天，ABCDEFG 工作应该全部完成，所以

PV=5+4+7+8+2+1+3=30 万元

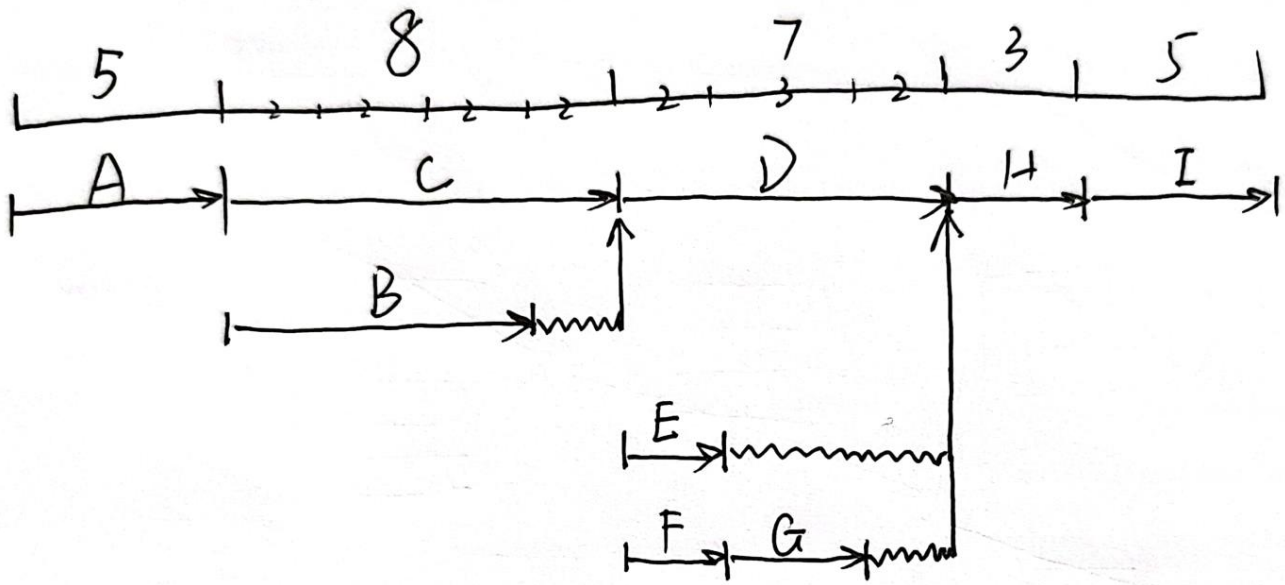
EV=5+4+7+8+2X1/2+1+3X2/3=28 万元

AC=3+7+5+3+3+1+1=23 万元

SV=28-30=-2 万元<0 进度滞后

CV=28-23=5 万元>0 成本节约

解析：考核挣值计算的能力。



高项

【试题二】

某信息系统项目包括10个活动，各活动的历时、活动逻辑关系如下表所示。

活动名称	活动历时	紧前活动
A	2	-
B	5	A
C	2	B、D
D	6	A
E	3	C、G
F	3	A
G	4	F
H	4	E
I	5	E
J	3	H、I

【问题1】

1. 请给出该项目的关键路线和总工期。
2. 请给出活动E、G的总浮动时间和自由浮动时间。

【问题2】

在项目开始前，客户希望将项目工期压缩为19天，并愿意承担所发生的所有额外费用。经过对各项活动的测算发现，只有活动B、D、I有可能缩短工期，其余活动均无法缩短工期。活动B、D、I最多可以缩短的天数以及额外费用如下表所示。

在此要求下，请给出费用最少的工期压缩方案及其额外增加的费用。

活动名称	最多可以缩短的天数	每缩短一天需要增加的额外费用（元）
B	2	2000
D	3	2500
I	3	3000

【问题2】

在项目开始前，客户希望将项目工期压缩为19天，并愿意承担所发生的所有额外费用。经过对各项活动的测算发现，只有活动B、D、I有可能缩短工期，其余活动均无法缩短工期。活动B、D、I最多可以缩短的天数以及额外费用如下表所示。在此要求下，请给出费用最少的工期压缩方案及其额外增加的费用。

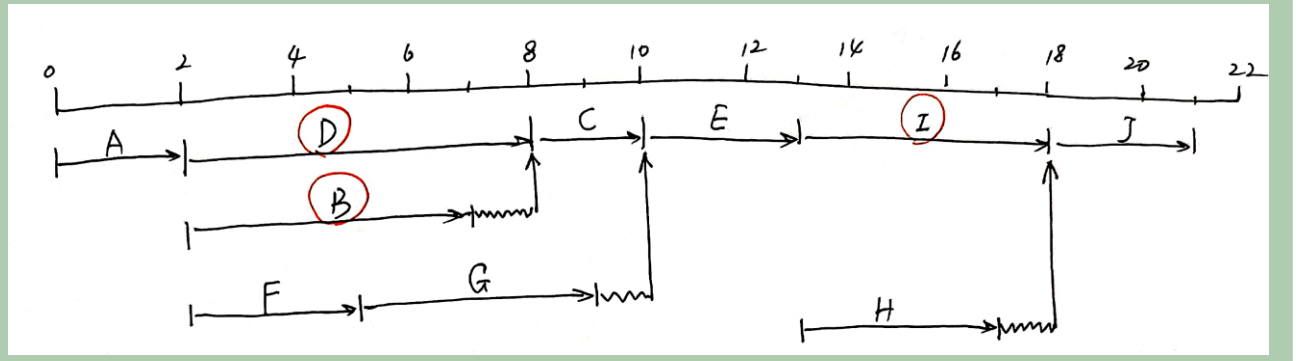
活动名称	活动历时	紧前活动
A	2	-
B	5	A
C	2	B、D
D	6	A
E	3	C、G
F	3	A
G	4	F
H	4	E
I	5	E
J	3	H、I

【参考答案】：

由于题目中给出限制，“只有活动B、D、I有可能缩短工期”，因此，费用最少的工期压缩方案为：D缩短1天，I缩短1天；额外增加的费用为5500元。

下图为当工期为21天时的时标网络图。

工期为21天要压缩为19天。



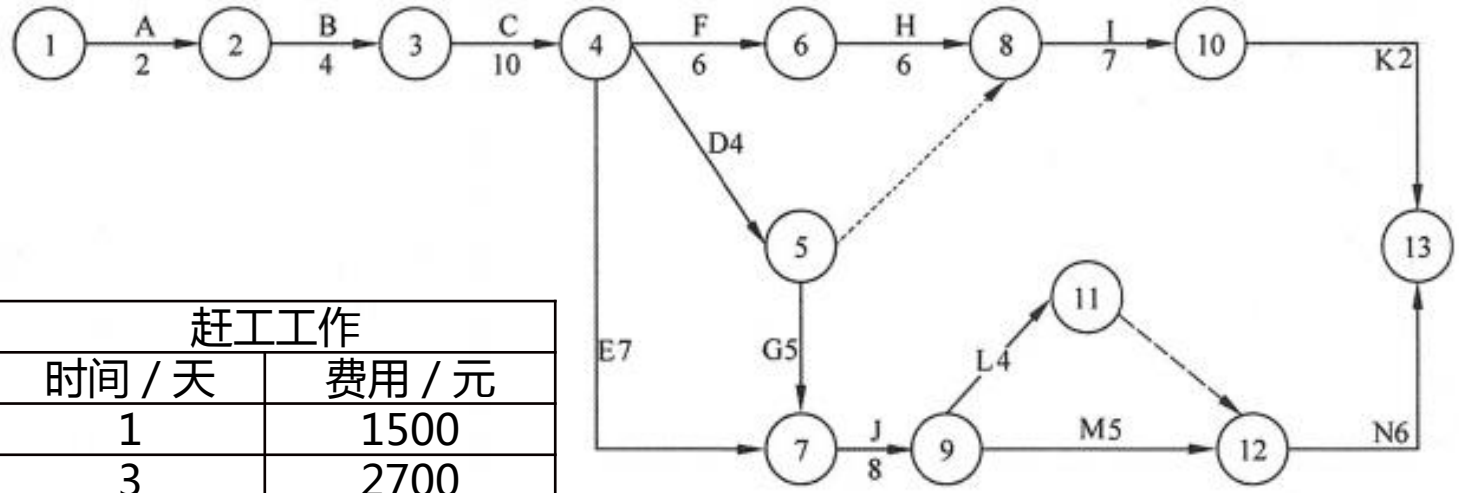
活动名称	最多可以缩短的天数	每缩短一天需要增加的额外费用（元）
B	2	2000
D	3	2500
I	3	3000

高项2016年5月真题-计算题

试题一

下图所示的是一个信息系统项目的进度网络图。

下表给出了该项目各项作业正常工作与赶工工作的时间和费用。



活　动	正常工作		赶工工作	
	时间 / 天	费用 / 元	时间 / 天	费用 / 元
A	2	1200	1	1500
B	4	2500	3	2700
C	10	5500	7	6400
D	4	3400	2	4100
E	7	1400	5	1600
F	6	1900	4	2200
G	5	1100	3	1400
H	6	9300	4	9900
I	7	1300	5	1700
J	8	4600	6	4800
K	2	300	1	400
L	4	900	3	1000
M	5	1800	3	2100
N	6	2600	3	2960

高项2016年5月真题-计算题

【问题3】

（1）请计算关键路径上各活动的可缩短时间，每缩短1天增加的费用和增加的总费用。将关键路径上各活动的名称以及对应的计算结果填入答题纸相对应的表格中。

（2）如果项目工期要求缩短到38天，请给出具体的工期压缩方案并计算需要增加的最少费用。

【问题3】

（1）请计算关键路径上各活动的可缩短时间，每缩短1天增加的费用和增加的总费用。将关键路径上各活动的名称以及对应的计算结果填入答题纸相对应的表格中。

（2）如果项目工期要求缩短到38天，请给出具体的工期压缩方案并计算需要增加的最少费用。

活动	可缩短时间(天)	增加的总费用(元)	每缩短一天增加的费用(元)
A	1	300	300
B	1	200	200
C	3	900	300
D	2	700	350
G	2	300	150
J	2	200	100
M	2	300	150
N	3	360	120

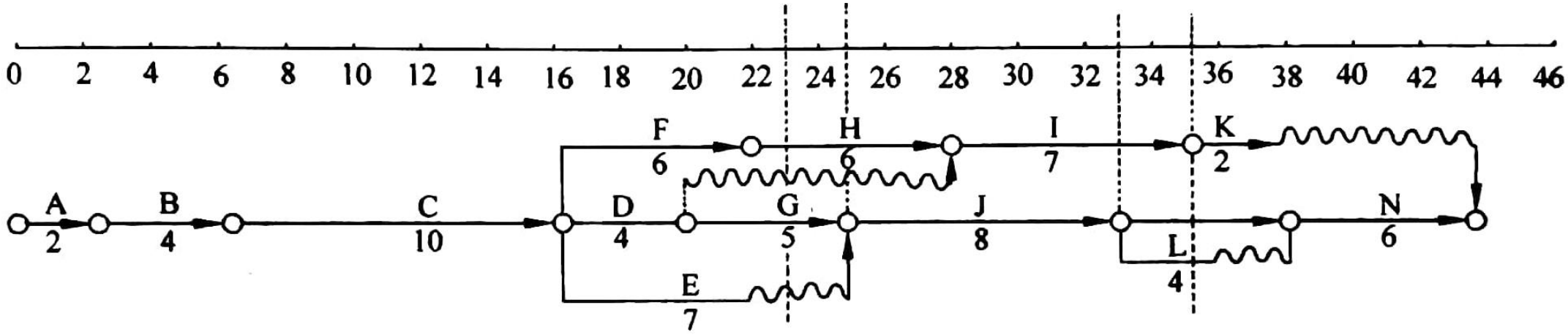
【问题3】

（1）填表如图:

（2）关键路径：A-B-C-D-G-J-M-N，长度44天。

压缩作业GJN或MJN，其中G或M压缩一天，J压缩2天，N压缩3天，增加的费用最少。

150+200+360=710（元）。



中项2015年11月-资源优化题

2015 下半年　资源争议题

试题四

某项目由 A、B、C、D、E、F、G、H 活动模块组成，下表给出了各活动之间的依赖关系，以及它们在正常情况和赶工情况下的工期及成本数据。假设每周的项目管理成本为 10 万元，而且项目管理成本与当周所开展的活动多少无关。

活动	紧前活动	正常情况		赶工情况	
		工期（周）	成本（万元/周）	工期（周）	成本（万元/周）
A	—	4	10	2	30
B	—	3	20	1	65
C	A、B	2	5	1	15
D	A、B	3	10	2	20
E	A	4	15	1	80
F	C、D	4	25	1	120
G	D、E	2	30	1	72
H	F、G	3	20	2	40

【问题 1】

找出项目正常情况下的关键路径，并计算此时的项目最短工期和项目总体成本。

【问题 2】

假设项目必须在 9 周内（包括第 9 周）完成，请列出此时项目中的关键路径，并计算此时项目的最低成本。

【问题 3】

在计划 9 周完成的情况下，项目执行完第 4 周时，项目实际支出 280 万元，此时活动 D 还需要一周才能够结束，计算此时项目的 PV、EV、CPI 和 SPI（假设各活动的成本按时间均匀分配）。

【问题 1】

找出项目正常情况下的关键路径，并计算此时的项目最短工期和项目总体成本。

【问题 2】

假设项目必须在 9 周内（包括第 9 周）完成，请列出此时项目中的关键路径，并计算此时项目的最低成本。

【问题 3】

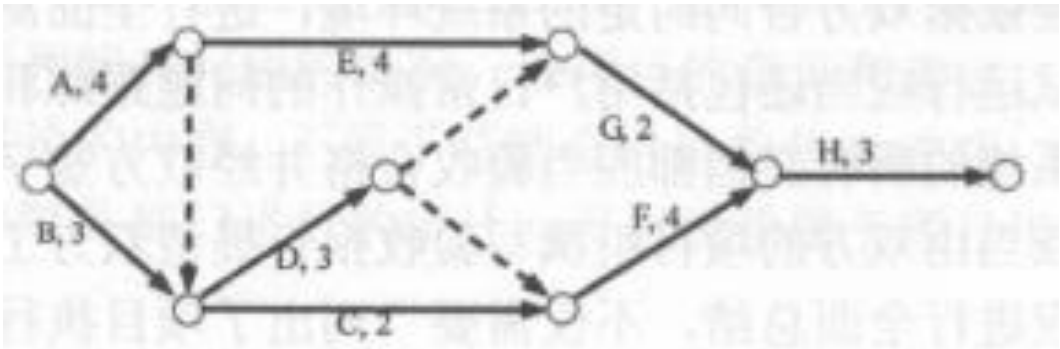
在计划 9 周完成的情况下，项目执行完第 4 周时，项目实际支出 280 万元，此时活动 D 还需要一周才能够结束，计算此时项目的 PV、EV、CPI 和 SPI（假设各活动的成本按时间均匀分配）。

有三种答案：

可以改变关键路径，但必须整体压缩，计算就是本题的 585

不能改变关键路径，计算是 587

可以改变关键路径，且可以按每周单独压缩，计算是 582



585 是官方思路:假设每个活动的压缩工期必须整体进行,要么压缩要么不压缩

活动	赶工压缩，周数	费用增加情况	每压缩 1 周 需要增加的费用	赶工效率排序
A	4→2，可压 2 周	40→60，增 20 万	20/2=10 万	4
B	3→1，可压 2 周	60→65，增 5 万	5/2=2.5 万	1
C	2→1，可压 1 周	10→15，增 5 万	5/1=5 万	2
D	3→2，可压 1 周	30→40，增 10 万	10/1=10 万	4
E	4→1，可压 3 周	60→80，增 20 万	20/3～6.67 万	3
F	4→1，可压 3 周	100→120，增 20 万	20/3～6.67 万	3
G	2→1，可压 1 周	60→72，增 12 万	12/1=12 万	5
H	3→2，可压 1 周	60→80，增 20 万	20/1=20 万	6

原来 14 周，要变成 9 周，需要压缩 5 周。

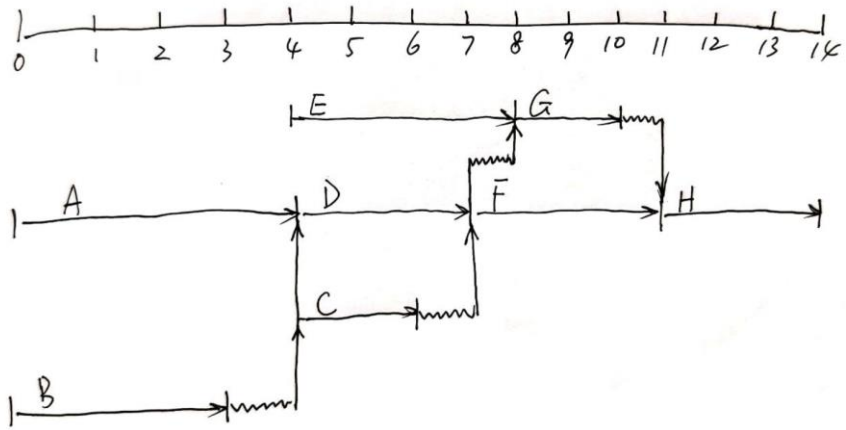
关键路径是 ADFH。所以按优先级，先压缩 F，关键路径变成 AEGH=4+4+2+3=13 周。

关键路径变成了 AEGH，按优先级，再压缩 E，关键路径变成 ADGH=4+3+2+3=12 周。

关键路径变成了 ADGH，按优先级，再压缩 A，关键路径变成 BDGH=3+3+2+3=11 周。

关键路径变成了 BDGH，按优先级，再压缩 B，关键路径变成 ADGH=2+3+2+3=10 周。

关键路径变成了 ADGH，按优先级，再压缩 D，关键路径变成 ADGH=2+2+2+3=9 周。



所以共压缩的活动是 A、B、D、E、F

所以 ABDEF 用赶工成本，CGH 用正常成本，再加管理成本

（2*30+1*65+2*20+1*80+1*120）+（2*5+2*30+3*20）+（9*10）=585 万

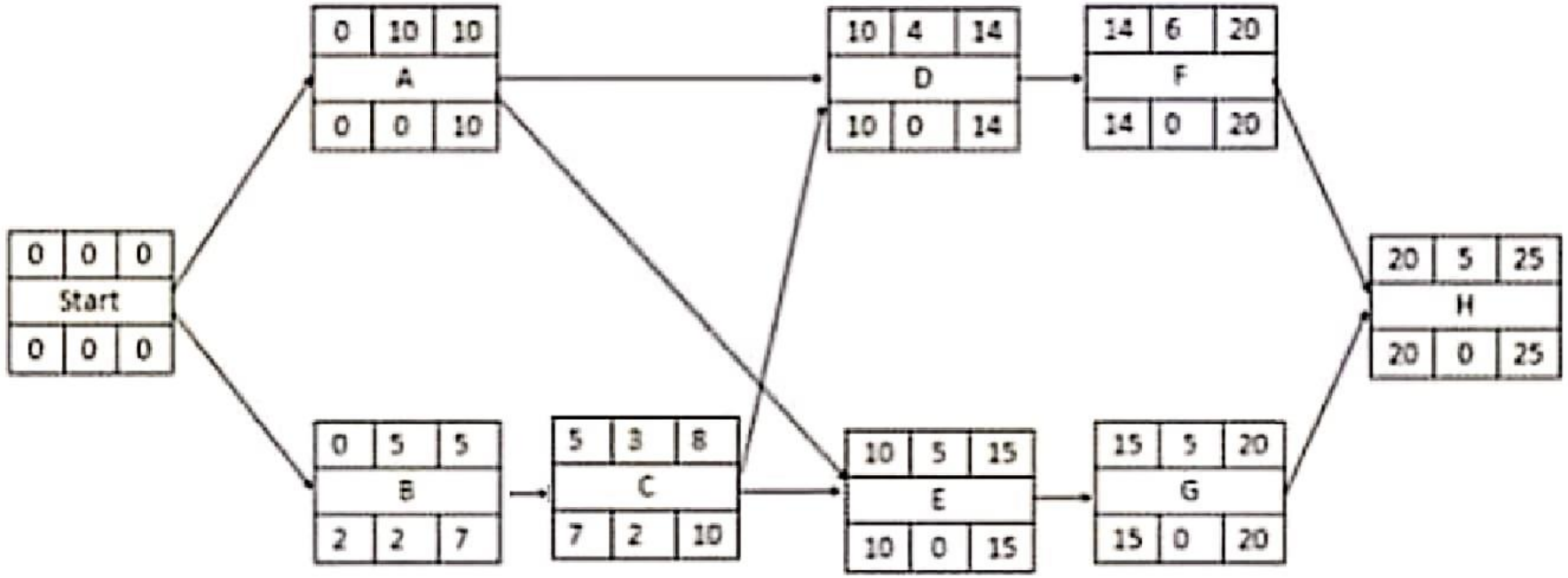
试题二（25分）

阅读下列说明，回答问题1至问题5，将解答填入答题纸的对应栏内

【说明】

某项目的网络图如下：

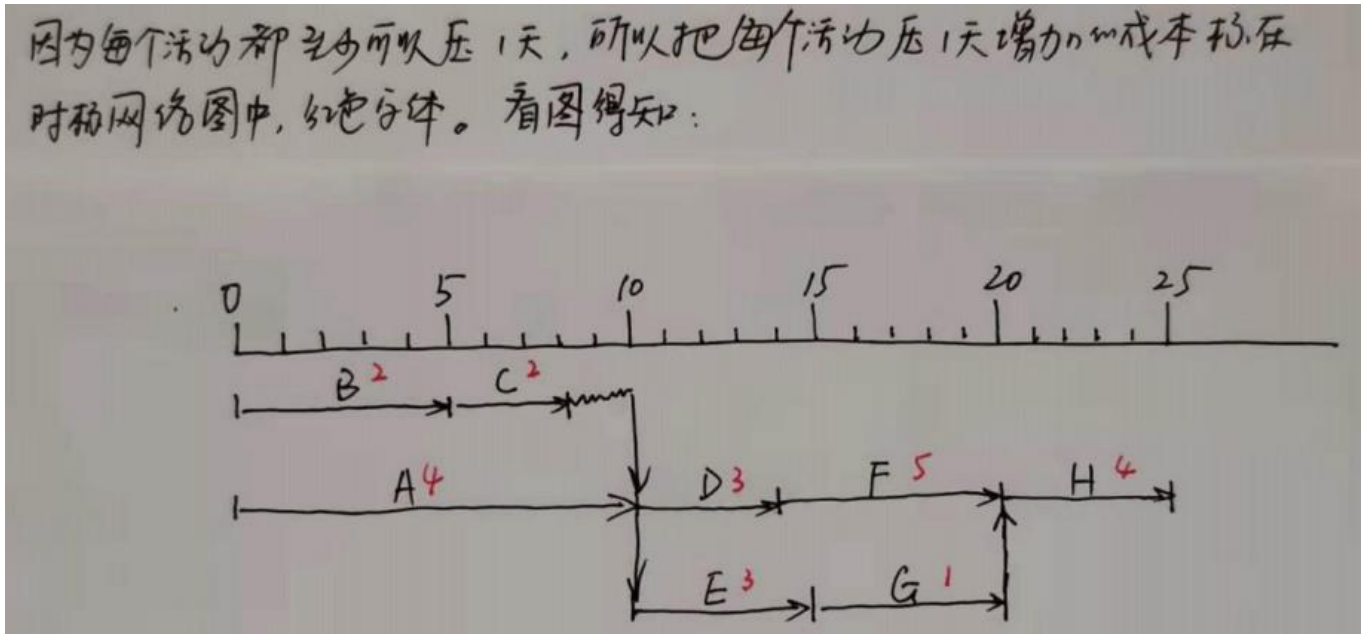
其中，各活动正常完工时间、正常完工直接成本、最短完工时间、赶工增加直接成本（如下表所示）。另外，项目的间接成本为500元/天



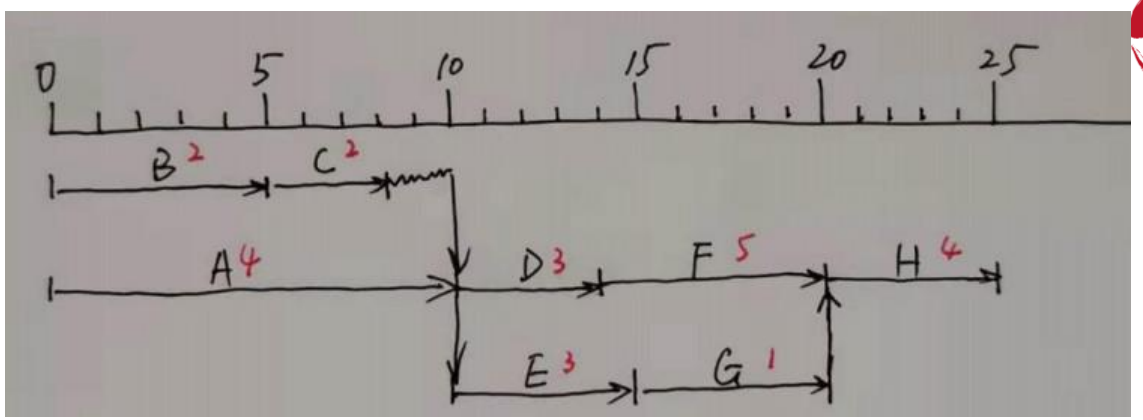
活动	正常完工时间（天）	正常完工直接成本（百元）	最短完工时间（天）	赶工增加直接成本（百元/天）
A	10	30	7	4
B	5	10	4	2
C	3	15	2	2
D	4	20	3	3
E	5	25	3	3
F	6	32	3	5
G	5	8	2	1
H	5	9	4	4
合计		149		

【问题1】（4分）
请确定项目的关键路径。
【问题2】（3分）
根据网络图确定项目正常完工的工期是多少天？所需的成本是多少？
【问题3】（3分）
讨论下列事件对计划项目进度有何影响：
（1）活动D拖期2天；
（2）活动B拖期2天；
（3）活动F和G在规定进度之前1天完成。
【问题4】（7分）
项目想提前1天完工，基于成本最优原则，可以针对哪些活动赶工？赶工后的项目成本是多少？
【问题5】（8分）
（1）基于项目整体成本最优原则，请列出需要赶工的活动及其工期：
（2）基于以上结果，确定赶工后的项目工期及所需成本。

【问题4】（7分）
项目想提前1天完工，基于成本最优原则，可以针对哪些活动赶工？赶工后的项目成本是多少？



【问题4】
方案1:同时压缩G和D各1天，增加了费用400元；
方案2:只压缩A 1天，增加费用400元；
方案3:只压缩H1天，增加费用400元；
但间接费用可省500元/天，因此总共可节省100元。
所以可以针对ADGH活动进行赶工，
赶工后的项目成本=27400-100=27300元



【问题5】

假设1：压缩1天，

通过问题四得知，可节省100元；

假设2：压缩2天，

最优方案：A压缩2天，增加800元，或A和H各压缩1天，增加800元，共节省200元。

假设3：压缩3天，

最优方案：A压缩2天增加800元+G压1天100元+D压1天300元=1200元，或A压缩2天增加800元+H压1天增加400元=1200元，共节省300元。

假设4：压缩4天，

最优方案：A压缩2天增加800元+H压1天增加400元+G压1天100元+D压1天300元=1600元，共节省400元。

假设5：压缩5天，

最优方案：A压缩3天增加1200元+B1天200+C1天200+H压1天增加400元+G压1天100元+D压1天300元=2400元，共节省100元。

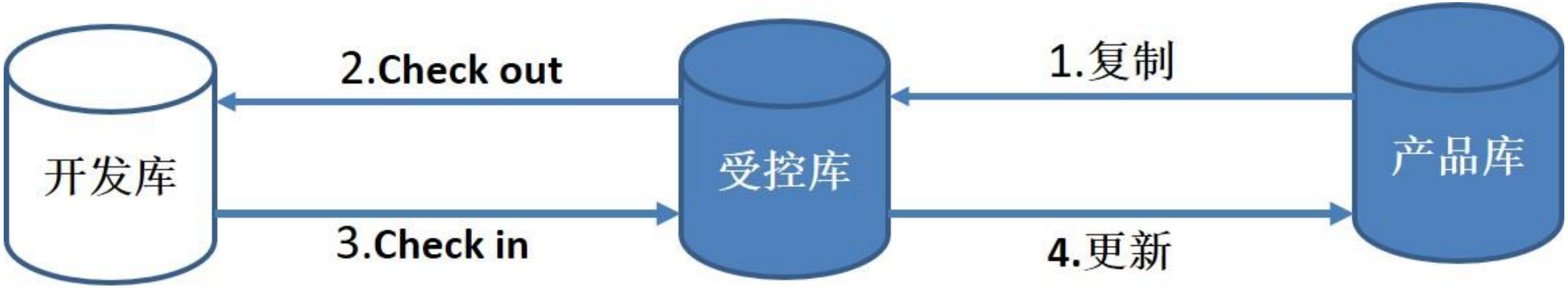
所以，最佳方案是压缩4天，最后工期为=25天-4天=21天， 项目成本=27400-400=27000元

光环软考
AURA INTERNATIONAL

案例分析进阶

复习配置管理

基于配置库的变更控制如图所示。



复习配置管理

光环国际 AURA INTERNATIONAL

1．配置管理包括**6**个主要活动：制订配置管理计划、配置标识、配置控制、配置状态报告、配置审计、发布管理和交付。

制订配置管理计划：是对如何开展项目配置管理工作的规划，是配置管理过程的基础，应该形成文件并在整个项目生命周期内处于受控状态。配置控制委员会负责审批该计划。
配置管理计划的主要内容为：
(1)配置管理活动，覆盖的主要活动包括配置标识、配置控制、配置状态报告、配置审计、发布管理与交付。
(2)实施这些活动的规范和流程。
(3)实施这些活动的进度安排。
(4)负责实施这些活动的人员或组织，以及他们和其他组织的关系。

配置标识（**Configuration Identification**）：也称配置识别，包括为系统选择配置项并在技术文档中记录配置项的功能和物理特征。
配置标识是配置管理员的职能，基本步骤如下。
(1)识别需要受控的配置项。
(2)为每个配置项指定唯一性的标识号。
(3)定义每个配置项的重要特征。
(4)确定每个配置项的所有者及其责任。
(5)确定配置项进入配置管理的时间和条件。
(6)建立和控制基线。

配置控制：即配置项和基线的变更控制，包括下述任务：标识和记录变更申请，分析和评价变更，批准或否决申请，实现、验证和发布已修改的配置项。

复习配置管理

配置状态报告（**Configuration Status Reporting**）：也称配置状态统计**(Configuration Status Accounting)**，其任务是有效地记录和报告管理配置所需要的信息，目的是及时、准确地给出配置项的当前状况，供相关人员了解，以加强配置管理工作。配置状态报告应该包含以下内容。
(1)每个受控配置项的标识和状态。一旦配置项被置于配置控制下，就应该记录和保存它的每个后继进展的版本和状态。
(2)每个变更申请的状态和已批准的修改的实施状态。
(3)每个基线的当前和过去版本的状态以及各版本的比较。
(4)其他配置管理过程活动的记录。

配置审计**(Configuration Audit)**也称配置审核或配置评价，包括功能配置审计和物理配置审计，分别用以验证当前配置项的一致性和完整性。
配置审计的实施是为了确保项目配置管理的有效性，体现了配置管理的最根本要求——不允许出现任何混乱现象，例如：
(1)防止向用户提交不适合的产品，如交付了用户手册的不正确版本。
(2)发现不完善的实现，如开发出不符合初始规格说明或未按变更请求实施变更。
(3)找出各配置项间不匹配或不相容的现象。
(4)确认配置项已在所要求的质量控制审核之后纳入基线并入库保存。
(5)确认记录和文档保持着可追溯性。

复习配置管理

发布管理和交付活动：发布管理和交付活动的主要任务是：有效控制软件产品和文档的发行和交付，在软件产品的生存期内妥善保存代码和文档的母拷贝。
(1)存储。应通过下述方式确保存储的配置项的完整性：
选择存储介质使再生差错或损坏降至最低限度。
根据媒体的存储期，以一定频次运行或刷新已存档的配置项。
将副本存储在不同的受控场所，以减少丢失的风险。
(2)复制。复制是用拷贝方式制造软件的阶段。
应建立规程以确保复制的一致性和完整性。
应确保发布用的介质不含无关项（如软件病毒或不适合演示的测试数据）。
应使用适合的介质以确保软件产品符合复制要求，确保其在整个交付期中内容的完整性。
(3)打包。应确保按批准的规程制备交付的介质。应在需方容易辨认的地方清楚标出发布标识。
(4)交付。供方应按合同中的规定交付产品或服务。
(5)重建。应能重建软件环境，以确保发布的配置项在所保留的先前版本要求的未来一段时间里是可重新配置的。

复习配置管理

2．配置项

GB/T11457-2006对配置项的定义为：“为配置管理设计的硬件、软件或二者的集合，在配置管理过程中作为一个单个实体来对待。”

典型配置项包括项目计划书、需求文档、设计文档、源代码、可执行代码、测试用例、运行软件所需的各种数据，它们经评审和检查通过后进入配置管理。

所有配置项都应按照相关规定统一编号，按照相应的模板生成，并在文档中的规定章节（部分）记录对象的标识信息。在引入配置管理工具进行管理后，这些配置项都应以一定的目录结构保存在配置库中。

所有配置项的操作权限应由**CMO**（配置管理员）严格管理，基本原则是：基线配置项向开发人员开放读取的权限；非基线配置项向**PM**、**CCB**及相关人员开放。

3、基线

配置基线（常简称为基线）由一组配置项组成，这些配置项构成一个相对稳定的逻辑实体。基线中的配置项被“冻结”了，不能再被任何人随意修改。对基线的变更必须遵循正式的变更控制程序。

一组拥有唯一标识号的需求、设计、源代码文卷以及相应的可执行代码、构造文卷和用户文档构成一条基线。产品的一个测试版本（可能包括需求分析说明书、概要设计说明书、详细设计说明书、已编译的可执行代码、测试大纲、测试用例、使用手册等）是基线的一个例子。

基线通常对应于开发过程中的里程碑**(Milestone)**，一个产品可以有多个基线，也可以只有一个基线。交付给外部顾客的基线一般称为发行基线**(Release)**，内部开发使用的基线一般称为构造基线**(Build)**。

复习配置管理

光环国际 AURA INTERNATIONAL

4．配置项状态

配置项的状态可分为“草稿”“正式”和“修改”三种。配置项刚建立时，其状态为“草稿”。配置项通过评审后，其状态变为“正式”。此后若更改配置项，则其状态变为“修改”。当配置项修改完毕并重新通过评审时，其状态又变为“正式”。

4．配置项版本号

配置项的版本号规则与配置项的状态相关。

(1)处于“草稿”状态的配置项的版本号格式为0.YZ，YZ的数字范围为01—99。随着草稿的修正，YZ的取值应递增。YZ的初值和增幅由用户自己把握。

(2)处于“正式”状态的配置项的版本号格式为X.Y，X为主版本号，取值范围为1～9。Y为次版本号，取值范围为0～9。

配置项第一次成为“正式”文件时，版本号为1.0。

如果配置项升级幅度比较小，可以将变动部分制作成配置项的附件，附件版本依次为1.0，1.1，….。当附件的变动积累到一定程度时，配置项的Y值可适量增加，Y值增加一定程度时，X值将适量增加。当配置项升级幅度比较大时，才允许直接增大X值。

(3)处于“修改”状态的配置项的版本号格式为X.YZ。配置项正在修改时，一般只增大Z值，X.Y值保持不变。当配置项修改完毕，状态成为“正式”时，将Z值设置为0，增加X.Y值。参见上述规则(2)。

复习配置管理

光环国际 AURA INTERNATIONAL

5．配置库

配置库（**Configuration Library**）存放配置项并记录与配置项相关的所有信息，是配置管理的有力工具，利用库中的信息可回答许多配置管理的问题。配置库可以分开发库、受控库、产品库**3**种类型。

(1)开发库**(Development Library)**，也称为动态库、程序员库或工作库，用于保存开发人员当前正在开发的配置实体，如：新模块、文档、数据元素或进行修改的已有元素。动态中的配置项被置于版本管理之下。动态库是开发人员的个人工作区，由开发人员自行控制。库中的信息可能有较为频繁的修改，只要开发库的使用者认为有必要，无需对其进行配置控制，因为这通常不会影响到项目的其他部分。

(2)受控库**(Controlled Library)**，也称为主库，包含当前的基线加上对基线的变更。受控库中的配置项被置于完全的配置管理之下。在信息系统开发的某个阶段工作结束时，将当前的工作产品存入受控库。

(3)产品库**(Product Library)**，也称为静态库、发行库、软件仓库，包含已发布使用的各种基线的存档，被置于完全的配置管理之下。在开发的信息系统产品完成系统测试之后，作为最终产品存入产品库内，等待交付用户或现场安装。

6、配置库权限设置

受控库的权限设置

人员 / 权限		项目经理	项目成员	QA	测试人员	配置管理员
文档	Read	√	√	√	√	√
	Check	√	√	√	√	√
	Add	√	√	√	√	√
	Destroy	×	×	×	×	√
代码	Read	√	√	√	√	√
	Check	√	√	×	×	√
	Add	√	√	×	×	√
	Destroy	×	×	×	×	√

说明：√表示该人员具有相应权限，×表示该人员没有相应权限。

Release（产品库）					
人员 / 权限	项目经理	项目成员	QA	测试人员	配置管理员
Read	√	√	√	√	√
Check	√	√	√	√	√
Add	×	×	×	×	√
Destroy	×	×	×	×	√

说明：√表示该人员具有相应权限，×表示该人员没有相应权限。

复习配置管理

光环国际 AURA INTERNATIONAL

6、配置库的建库模式：
配置库的建库模式有两种，按配置项类型建库和按任务建库。
(1)按配置项的类型分类建库，适用于通用软件的开发组织。在这样的组织内，往往产品的继承性较强，工具比较统一，对并行开发有一定的需求。使用这样的库结构有利于对配置项的统一管理和控制，同时也能提高编译和发布的效率。但由于这样的库结构并不是面向各个开发团队的开发任务的，所以可能会造成开发人员的工作目录结构过于复杂，带来一些不必要的麻烦。
(2)按开发任务建立相应的配置库，适用于专业软件的开发组织。在这样的组织内，使用的开发工具种类繁多，开发模式以线性发展为主，所以就没有必要把配置项严格地分类存储，人为增加目录的复杂性。对于研发性的软件组织来说，采用这种设置策略比较灵活。

7.配置控制委员会
配置控制委员会（**Configuration Control Board**，**CCB**），负责对配置变更做出评估、审批以及监督已批准变更的实施。通常，**CCB**不只是控制配置变更，而是负有更多的配置管理任务，例如：配置管理计划审批、基线设立审批、产品发布审批等。

复习配置管理

光环国际 AURA INTERNATIONAL

8．配置管理员

配置管理员（**Configuration Management Officer**，**CMO**），负责在整个项目生命周期中进行配置管理活动，具体有：

编写配置管理计划。　建立和维护配置管理系统。　建立和维护配置库。

配置项识别。　版本管理和配置控制。　配置状态报告。

配置审计。　发布管理和交付。　对项目成员进行配置管理培训。

9、物理配置审计

物理配置审计**(Physical Configuration Audit)**是审计配置项的完整性（配置项的物理存在是否与预期一致），具体验证如下几个方面。

要交付的配置项是否存在。

配置项中是否包含了所有必需的项目。

10、功能配置审计

功能配置审计（**Functional Configuration Audit**）是审计配置项的一致性（配置项的实际功效是否与其需求一致），具体验证以下几个方面。

配置项的开发已圆满完成。

配置项已达到配置标识中规定的性能和功能特征。

配置项的操作和支持文档已完成并且是符合要求的。

复习配置管理

光环国际 AURA INTERNATIONAL

11、配置变更流程

（**1**）变更申请

变更申请主要就是陈述：要做什么变更，为什么要做，以及打算怎么做变更。

相关人员如项目经理填写变更申请表，说明要变更的内容、变更的原因、受变更影响的关联配置项和有关基线、变更实施方案、工作量和变更实施人等，并提交给**CCB**。

（**2**）变更评估

CCB负责组织对变更申请进行评估并确定以下内容。

变更对项目的影响。

变更的内容是否必要。

变更的范围是否考虑周全。

变更的实施方案是否可行。

变更工作量估计是否合理。

CCB决定是否接受变更，并将决定通知相关人员。

（**3**）通告评估结果

CCB把关于每个变更申请的批准、否决或推迟的决定通知受此处置意见影响的每个干系人。

如果变更申请得到批准，应该及时把变更批准信息和变更实施方案通知给那些正在使用受影响的配置项和基线的干系人。

如果变更申请被否决，应通知有关干系人放弃该变更申请。

复习配置管理

（4）变更实施
项目经理组织修改相关的配置项，并在相应的文档或程序代码中记录变更信息。
（5）变更验证与确认
项目经理指定人员对变更后的配置项进行测试或验证。项目经理应将变更与验证的结果提交CCB，由其确认变更是否已经按要求完成。
（6）变更的发布
配置管理员将变更后的配置项纳入基线。配置管理员将变更内容和结果通知相关人员，并做好记录。
（7）基于配置库的变更控制
现以某软件产品升级为例，简述其流程。
①将待升级的基线（假设版本号为V2.1）从产品库中取出，放入受控库。
②程序员将欲修改的代码段从受控库中检出（Checkout），放入自己的开发库中进行修改。代码被Checkout后即被“锁定”，以保证同一段代码只能同时被一个程序员修改，如果甲正对其修改，乙就无法Checkout。
③程序员将开发库中修改好的代码段检入（Checkin）受控库。Checkin后，代码的“锁定”被解除，其他程序员可以Checkout该段代码了。
④软件产品的升级修改工作全部完成后，将受控库中的新基线存入产品库中（软件产品的版本号更新为V2.2，旧的V2.1版并不删除,继续在产品库中保）。

中项2022上半年（广东卷）-配置管理

试题四（19分）

段1：A公司专门从事仿真软件产品的研发，近期承接了一个项目。公司任命老王担任项目经理，带领10人的开发团队完成该项目。老王兼任配置管理员，为方便工作，他给所有项目组成员开放了全部操作权限。

段2：测试人员首先依据界面功能准备了集成测试用例，随后和开发人员在开发环境中交互进行集成测试并完成的缺陷修复工作。测试期间发现特定参数下仿真图形显示出现较大变形的严重错误，开发人员认为彻底修复难度较大，可以在试运行阶段再处理，测试人员表示认可。

段3：在回归测试结束后，测试人员向项目组提交了测试报告，老王认为开发工作已圆满结束。在客户的不断催促下，老王安排开发工程师将代码从开发库中提取出来，连带测试用的用户数据一起刻盘后快递给客户。

【问题1】（10分）

结合案例，请分别简述项目在配置管理和测试过程存在的问题。

【问题2】（3分）

请指出功能配置审计需要验证哪些方面的内容。

【问题3】（6分）

请将下面（1）-（3）处答案填写在答题纸的对应栏内。

典型的配置库可以分为（1）种类型，（2）又称主库，包含当前基线和对基线的变更，（3）包含已发布使用的各种基线的存档，被置于完全的配置管理之下。

参考答案：

【问题1】（10分）

结合案例，请分别简述项目在配置管理和测试过程存在的问题。

【问题1答案】：

1．没有做好配置管理计划。

2．项目经理小王不应该担任配置管理员，应该安排其他人。

3．权限开通不对，必须控制相关人员的权限。

4．对于问题没有及时进行处理。

5．没有做好配置标识。

6．没有做好变更控制，因严格按照配置控制的变更流程进行处理。

7．没有做好配置审计。

8．没有做好相关培训工作。

9．团队之间和干系人之间没有做好沟通管理。

10．测试做的不全面，不完整。

11．测试没有验证就交给了客户。

12．没有做好测试审计。

【问题2】（3分）请指出功能配置审计需要验证哪些方面的内容。
【问题2答案】：
功能配置审计是进行审计以验证以下几个方面：
（1）配置项的开发已圆满完成。
（2）配置项已达到规定的性能和功能特定特性。
（3）配置项的运行和支持文档已完成并且是符合要求的。

解析：配置审计也称配置审核或配置评价，包括功能配置审计和物理配置审计，分别用以验证当前配置项的一致性和完整性。
1.功能配置审计：是审计配置项的一致性（配置项的实际功效是否与其需求一致），具体验证以下几个方面。
（1）配置项的开发已圆满完成.
（2）配置项已达到配置标识中规定的性能和功能特征。
（3）配置项的操作和支持文档已完成并且是符合要求的。
2.物理配置审计：是审计配置项的完整性（配置项的物理存在是否与预期一致），具体验证如下几个方面。
（I）要交付的配置项是否存在。
（2）配置项中是否包含了所有必需的项目。

【问题3】（6分）请将下面（1）-（3）处答案填写在答题纸的对应栏内。
典型的配置库可以分为（1）种类型，（2）又称主库，包含当前基线和对基线的变更，（3）包含已发布使用的各种基线的存档，被置于完全的配置管理之下。
【问题3答案】：
（1）三；（2）受控库；（3）产品库。

高项2021下半年-配置管理

试题三

某公司中标医院的信息管理系统。公司指派小王担任项目经理，并组建相应的项目团队。由于人手有限，小王让负责项目质量工作的小杨同时担当配置管理员。小杨编写并发布了质量管理计划和配置管理计划。

小杨利用配置管理软件对项目进行配置管理，为了项目管理方便，小杨给小王开放所有的配置权限，当有项目组成员提出配置变更需求时，小杨直接决定是否批准变更请求，小杨为项目创建了三个文件夹，分别作为存放开发、受控、产品文件的目录，对经过认定的文档或经过测试的代码等能够形成配置基线的文件，存放到受控库中，并对其编号，项目研发过程中，某软件人员打算对某段代码作一个简单修改，他从配置库检出特修改的代码段，修改完成并经测试没问题后，检入配置库，小杨认为代码改动不大，依然使用之前的版本号，并移除了旧的代码。公司在质量审计过程中，发现项目管理方面的诸多问题。

【问题 1】(10 分)

请结合案例，简要分析该项目在配置管理方面存在的问题。

【问题2】(8分)

请结合案例，描述在软件升级过程中的配置库变更控制流程。

【问题 3】(5分)

请简述质量审计的目标。

【问题 4】(2分)

在候选答案中选择正确选项，将该选项的编号填入答题纸内。

通常来说，质量管理人员不应具备的权限。

A.产品库代码的 **Check** 权限

B.产品库文档的 **Check** 权限

C.受控库代码的 **Check** 权限

D.受控库文档的 **Check** 权限

参考答案：

【问题 1】(10 分)请结合案例，简要分析该项目在配置管理方面存在的问题。

【问题1答案】：

1.小杨不能一个人编制质量管理计划和配置管理计划，需要相关干系人参与。

2.小杨不能直接发布质量管理计划和配置管理计划，需要相关领导的审批。

3.小杨不能给小王开放所有的配置权限。

4.小杨不能直接决定是否批准变更请求。

5.小杨不能删除旧的代码。

6.没有按照配置控制中的变更流程处理相关变更。

7.软件人员不能随意的从配置库中提取要修改的代码段。

9.修好完成的并经过测试的代码段不能随意放入配置库，也需要经过审批通过后才能放入。

10.对经过认定的文档或经过测试的代码等能够形成配置基线的文件，不能随意的存入受控库中，需经过批准与审批。

【问题2】(8分)请结合案例，描述在软件升级过程中的配置库变更控制流程。

【问题2答案】：

配置控制即配置项和基线的变更控制，包括下述任务:标识和记录变更申请，分析和评价变更，批准或否决申请，实现、验证和发布已修改的配置项。

1. 变更申请；
2. 变更评估；
3. 通告评估结果；
4. 变更实施；
5. 变更验证与确认；
6. 变更的发布；

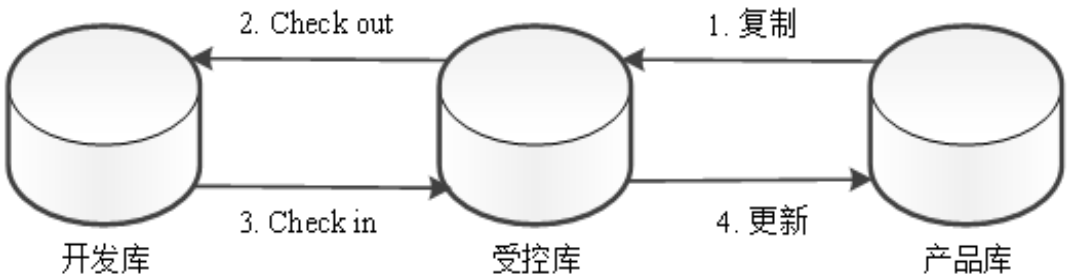
7、基于配置库的变更控制流程：

（1）将要升级的基线从产品库取出，放入受控库；

（2）程序员将经修改的代码段从受控库检出，放入自己的开发库中进行修改；

（3）程序员将开发库中修改好的代码段检入受控库；

（4）软件产品的升级修改工作全部完成后将受控库中的新基线存入产品库。



【问题 3】(5分)请简述质量审计的目标。
【问题3答案】：
质量审计的目标是：
(1) 识别全部正在实施的良好及最佳实践；
(2) 识别全部违规做法、差距及不足；
(3) 分享所在组织或行业中类似项目的良好实践；
(4) 积极、主动地提供协助，以改进过程的执行，从而帮助团队提高生产效率；
(5)强调每次审计都应对组织经验教训的积累做出贡献。

【问题 4】(2分)
在候选答案中选择正确选项，将该选项的编号填入答题纸内。
通常来说，质量管理人员不应具备的权限。
A.产品库代码的 Check 权限
B.产品库文档的 Check 权限
C.受控库代码的 Check 权限
D.受控库文档的 Check 权限
【问题4答案】：
C

受控库的权限设置

权限 \ 人员		项目经理	项目成员	QA	测试人员	配置管理员
文档	Read	√	√	√	√	√
	Check	√	√	√	√	√
	Add	√	√	√	√	√
	Destroy	×	×	×	×	√
代码	Read	√	√	√	√	√
	Check	√	√	×	×	√
	Add	√	√	×	×	√
	Destroy	×	×	×	×	√

说明：√表示该人员具有相应权限，×表示该人员没有相应权限。

Release（产品库）

权限 \ 人员	项目经理	项目成员	QA	测试人员	配置管理员
Read	√	√	√	√	√
Check	√	√	√	√	√
Add	×	×	×	×	√
Destroy	×	×	×	×	√

说明：√表示该人员具有相应权限，×表示该人员没有相应权限。

案例分析实战---配置管理类

试题三（25分）

阅读下列说明，回答问题1至4，将解答填入题纸的对应栏里。

【说明】

A公司是提供SaaS平台服务业务的公司，小张作为研发流程优化经理，他抽查了核心产品的配置管理和测试过程，情况如下：项目组共10人，产品经理小马兼任项目经理和配置管理员，还有7名开发工程师和2名测试工程师，采用敏捷的开发方式，2周为一个迭代周期，目前刚刚完成一个3.01版本的上线。

小张要求看一下配置管理库，小马回复："我正忙着，让测试工程师王工给你看吧，我们10个都有管理权限"。小张看到配置库分为了开发库和产品库，产品库包括上线的3 个大板块的完整代码和文档资料，而且与实际运行版本有偏差。小版本只能在开发库中找到代码，但没有相关文档，而且因为新需迭代太快，有些很细微的修改，开发人员随手进行了修改，文档和代码存在一些偏差。

小张策划对产品做一次3.01版本的系统测试，以便更好的解决研发流程和系统本身的问题。

案例分析实战---配置管理类

【问题1】（5分）

结合本案例，从配置管理的角度指出项目实施过程中存在的问题。

【问题2】（10分）

结合本案例，请帮助测试工程师从测试目的、测试对象、测试内容、测试过程、测试用例设计依据，测试技术6个方面设计核心产品3.01版本的系统测试方案。

【问题3】（6分）

如果系统测试中需要采用黑盒测试，白盒测试和灰盒测试，请阐述三种测试的含义和用途。

案例分析实战---配置管理类

光环国际 AURA INTERNATIONAL

【问题4】（4分）

从候选答案中选出正确选项，将该选项编号填入答题纸对应栏内。

配置项的状态通常可分为三种，配置项初建时其状态为（ ）。配置项通过评审后，其状态变为（ ）。此后若更改配置项，则其状态变为（ ）。当配置项修改完毕并重新通过评审时，其状态友变为（ ）.

A.送审稿　B. 草稿　C. 报批稿

D.征求意见　E. 修改　F. 正式

【问题1】答案：

1、没有制订规范的配置管理计划

2、没有安排专职的配置管理员

3、没有建立起合理的配置管理系统

4、没有做好配置标识

5、没有做好配置控制。

6、没有做好配置状态报告

7、没有做好配置审计

8、没有做好发布管理和交付

9、没有配置管理变更管理流程

配置管理包括6个主要活动：

速记词：计时制，状态审计不符

计	时	制	状态	审计	不符
软件配置管理计划	软件配置标识	软件配置控制	软件 配置状态记录	软件配置审计	软件发布管理与交付

【问题2】（10分）

结合本案例，请帮助测试工程师从测试目的、测试对象、测试内容、测试过程、测试用例设计依据，测试技术6个方面设计核心产品3.01版本的系统测试方案。

【问题2】答案：

测试目的：发现软件缺陷、识别软件问题

测试对象：3.01测试系统

测试内容：源代码、文档

测试过程：测试计划-测试施行-发布测试结果

测试用例设计依据：需求分析说明书等

测试技术：白盒、黑盒，灰盒

【问题3】（6分）

如果系统测试中需要采用黑盒测试，白盒测试和灰盒测试，请阐述三种测试的含义和用途。

【问题3】答案：

黑盒测试：也称功能测试，它是通过测试来检测每个功能是否都能正常使用。在测试中，把程序看作一个不能打开的黑盒子，在完全不考虑程序内部结构和内部特性的情况下，在程序接口进行测试，它只检查程序功能是否按照需求规格说明书的规定正常使用，程序是否能适当地接收输入数据而产生正确的输出信息。黑盒测试着眼于程序外部结构，不考虑内部逻辑结构，主要针对软件界面和软件功能进行测试。

白盒测试：又称结构测试，白盒测试可以把程序看成装在一个透明的白盒子里，也就是清楚了解程序结构和处理过程，检查是否所有的结构及路径都是正确的，检查软件内部动作是否按照设计说明书的规定正常进行。其目的是通过检查软件内部的逻辑结构，对软件中逻辑路径进行覆盖的测试，可以覆盖全部代码、分支、路径和条件。

灰盒测试：介于白盒测试与黑盒测试之间的测试。灰盒测试关注输出对于输入的正确性，同时也关注内部表现，但这种关注不像白盒测试详细、完整，只是通过一些表征的现象、事件、标志来判断内部的运行状态。灰盒测试是基于程序运行时的外部表现同时又结合程序内部逻辑结构来设计用例，执行程序并采集程序路径执行信息和外部用户接口结果的测试技术。

【问题4】（4分）

从候选答案中选出正确选项，将该选项编号填入答题纸对应栏内。

配置项的状态通常可分为三种，配置项初建时其状态为（ ）。配置项通过评审后，其状态变为（ ）。此后若更改配置项，则其状态变为（ ）。当配置项修改完毕并重新通过评审时，其状态友变为( ).

A.**送审稿**　　B. **草稿**　　C. **报批稿**

D.**征求意见**　　E. **修改**　　F. **正式**

【问题4】 答案：

（1）B；（2）F；（3）E；（4）F。

复习信息安全

光环国际 AURA INTERNATIONAL

1．信息安全是指保护信息的保密性、完整性、可用性，以及其它属性。
保密性：是指信息不被泄露给未授权的个人、实体和过程或不被其使用的特性。数据的保密性可以通过下列技术来实现：最小授权原则、防暴露、信息加密、物理加密。
完整性：是指保护资产的正确和完整的特性。简单地说，就是确保接收到的数据就是发送的数据。数据不应该被改变。确保数据完整性的技术包括：协议、纠错编码方法、密码校验和方法、数字签名、公证。
可用性：是指需要时，授权实体可以访问和使用的特性。确保可用性的技术有：磁盘和系统的容错，可接受的登录及进程性能、可靠的功能性和安全进程和机制、数据冗余及备份。
保密性、完整性和可用性是信息安全最为关注的三个属性，也被称为信息安全三元组。这也是信息安全通常所强调的目标。

2、信息系统安全策略的核心内容就是“七定”，即定方案、定岗、定位、定员、定目标、定制度、定工作流程。按照系统安全策略“七定”的要求，系统安全策略首先要解决定方案，其次就是定岗。

3、 木桶效应
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。

复习信息安全

光环国际 AURA INTERNATIONAL

4、 计算机信息系统安全保护等级划分准则

《计算机信息系统安全保护等级划分准则》是建立安全等级保护制度，实施安全等级管理的重要基础性标准，它将计算机信息系统分为以下五个安全保护等级。计算机信息系统安全保护等级划分准则如表所示。

表：计算机信息系统安全保护等级划分准则

级别	等级	对象
第一级	用户自主保护级	用于普通内联网用户
第二级	系统审计保护级	用于内联网、国际网进行商务活动的、需要保密的非重要单位
第三级	安全标记保护级	用于地方国家机关、金融单位、邮电通信、能源与水源供给部门、交通运输、大型工商与信息技术企业、重点工程建设等单位
第四级	结构化保护级	用于中央级国家机关、广播电视部门、重要物资储备单位、社会应急服务部门、尖端科技企业集团、国家重点科研单位、国防建设等部门
第五级	访问验证保护级	用于国防关键部门、依法需要对计算机信息系统实施特殊隔离的单位

复习信息安全

光环国际 AURA INTERNATIONAL

5、信息系统安全保护的等级

信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。

一是受侵害的客体。等级保护对象受到破坏时所侵害的客体包括公民、法人和其他组织的合法权益；社会秩序、公共利益；国家安全。

二是对客体的侵害程度。等级保护对象受到破坏后对客体造成侵害的程度分为造成一般损害；造成严重损害；造成特别严重损害。

《信息安全等级保护管理办法》将信息系统的安全保护等级分为以下五级。

第一级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级：信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级：信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级：信息系统受到破坏后，会对国家安全造成特别严重损害。

案例分析实战---安全管理类

试题四（18分）

系统集成A公司承接了某市政府电子政务系统机房升级改造项目，任命小张为项目经理。升级改造工作实施前，小张安排工程师对机房进行了检查，形成如下14条记录：

（1）机房有机架30组

（2）机房内中各个区域温度保持在25度左右

（3）机房铺设普通地板，配备普通办公家具

（4）机房照明系统与机房设备统一供电，配备了应急照明装置

（5）机房配备了UPS，无稳压器

（6）机房设置了避雷装置

（7）机房安装了防盗报警装置

（8）机房内配备了灭火器，但没有烟感报警装置

（9）机房门口设立门禁系统，无人值守

（10）进入机房人员需要佩戴相应证件

（11）工作人员可以使用个人手机与外界联系

（12）所有来访人员需经过正式批准，批准通过后可随意进入机房

（13）来访人员可以携带笔记本电脑进入机房

（14）机房内明确标示禁止吸烟和携带火种

[问题1]（8分）

根据以上检查记录，请指出该机房在信息安全管理方面存在的问题，并说明原因（将错误编号及原因填写在答题纸对应表格）。

[问题2]（4分）

信息系统安全的属性包括保密性、完整性、可用性和不可抵赖性。请说明各属性的含义。

[问题3]（6分）

请列举机房防静电的方式。

【问题1】（8分）

根据以上检查记录，请指出该机房在信息安全管理方面存在的问题，并说明原因（将错误编号及原因填写在答题纸对应表格）。

【参考答案】问题1

错误记录编号	原因
（3）	机房地板与家具需考虑防静电
（4）	机房照明系统与机房设备应独立供电
（5）	机房需配置稳压器
（8）	机房需配置烟感报警装置
（9）	机房须有专人值守
（11）	工作人员不可携带手机进入机房
（12）	获准进入机房的来访人员须由专人陪同
（13）	来访人员不可携带笔记本电脑进入机房

【问题2】（4分）

信息系统安全的属性包括保密性、完整性、可用性和不可抵赖性。请说明各属性的含义。

【参考答案】问题2

1．保密性是应用系统的信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。

2．完整性是信息未经授权不能进行改变的特性。

3．可用性是应用系统信息可被授权实体访问并按需求使用的特性。

4．不可抵赖性也称作不可否认性，在应用系统的信息交互过程中，确信参与者的真实统一性。

[问题3]（6分）

请列举机房防静电的方式。

【参考答案】问题3

机房防静电的措施以下7条：

①接地与屏蔽：采用必要的措施，使计算机系统有一套台理的防静电接地与屏蔽系统。

②服装防静电：人员服装采用不易产生静电的衣料，工作鞋采用低阻值材料制作。

③温、湿度防静电：控制机房温湿度，使其保持在不易产生静电的范围内。

④地板防静电：机房地板从表面到接地系统的阻值，应控制在不易产生静电的范围内。

⑤材料防静电：机房中使用的各种家具，如工作台、柜等，应选择产生静电小的材料。

⑥维修电路保护：在硬件维修时，应采用金属板台面的专用维修台，以保护电路。

⑦静电消除要求：在机房中使用静电消除剂等，以进一步减少静电的产生。

光环软考
AURA INTERNATIONAL

论文写作进阶

2019年上半年
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与区别。
（2）项目风险管理的主要过程和方法。
（2）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。

论信息系统项目的风险管理与安全管理

一、在规划阶段做好规划风险管理、风险识别、风险的定性和定量分析，根据风险登记册做好风险应对计划，根据适度安全的相关标准做好防止“木桶效应”的相关计划和措施。

我们的工作越依赖计算机，信息安全工作就越重要，从项目计划阶段，我们就要充分考虑信息安全工作的部署。在风险管理的规划阶段，我组织召开相关会议，与相关干系人和相关专家，根据项目管理计划、项目章程、干系人登记册、事业环境因素和组织过程资产等等相关资料制定了风险管理计划和安全管理计划。其主要内容是：根据合同及国家相关标准执行风险和安全管理，加强风险和安全的相关知识培训，进行全面质量管理，让干系人时刻保持安全和质量意识。该项目的风险分为已知风险和未知风险，分别做好应急储备和管理储备。安全管理计划的核心策略是做好“七定”（定方案、定岗、定位、定员、定目标、定制度、定工作流程），提高系统的安全性和稳定性。首先定方案按照适度安全的标准，我们设定等保是第二级系统审计保护级，并制定安全管理制度体系，明确信息安全的目标、建立和完善信息安全管理制度。其次成立安全管理小组，明确组员的职责等等内容。

根据项目管理计划和安全管理计划等等资料，我们采用文档审查、信息收集、**SWOT**分析等技术进行风险识别。经会议研究得到已知的风险有范围蔓延，成本超支，质量问题，安全管理不到位，沟通不到位等等；未知的风险有国家政策和技术标准的变动，自然灾害等等，分别制定了相关应对措施清单，风险责任人，并制定了相关的应急储备和管理储备。之后整理会议，得到风险登记册，并更新相关文件。

论信息系统项目的风险管理与安全管理

根据风险登记册等等相关资料，我们采用风险分类和风险紧迫性评估技术进行风险定性分析，对相关风险进行排序，已知风险的顺序是：沟通不到位，质量问题，范围蔓延，成本超支，安全管理不到位；未知风险的顺序是：自然灾害，国家政策和技术标准的变动。随后我们采用了定量风险分析和专家判断技术进行了风险的定量分析，我首先将风险发生的概率分为“极低、低、中、高、极高”这五级（对应值是5、4、3、2和1），沟通不到位影响程度是5。质量问题影响程度是5。范围蔓延影响程度是4。成本超支，影响程度是3，安全管理不到位影响程度是4。对于未知风险：自然灾害、国家相关政策变动、技术更新影响程度是5。随后进行项目文件更新。

根据风险登记册，我们采用风险应对策略技术制定了相关的风险应对措施，对于沟通不到位我们采用定期、不定期采用会议，发放需求调查表和问题提交表等等方式就行沟通处理。加强全面质量管理和培训，提高质量意识。在安全管理方面严格按照系统审计保护级实施了粒度更细的自主访问控制，通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。因为信息系统就和一个木桶一样，其安全水平是由构成木桶最短的那快木板决定的，因此我加强设备安全、数据安全、内容安全、行为安全管理，减少“木桶效应”。会议中对其它风险做好应对计划，做好应急储备和管理储备。会后把风险应对计划上报高层，经其批准，随后更新相关的项目管理计划和项目文件。

论信息系统项目的风险管理与安全管理

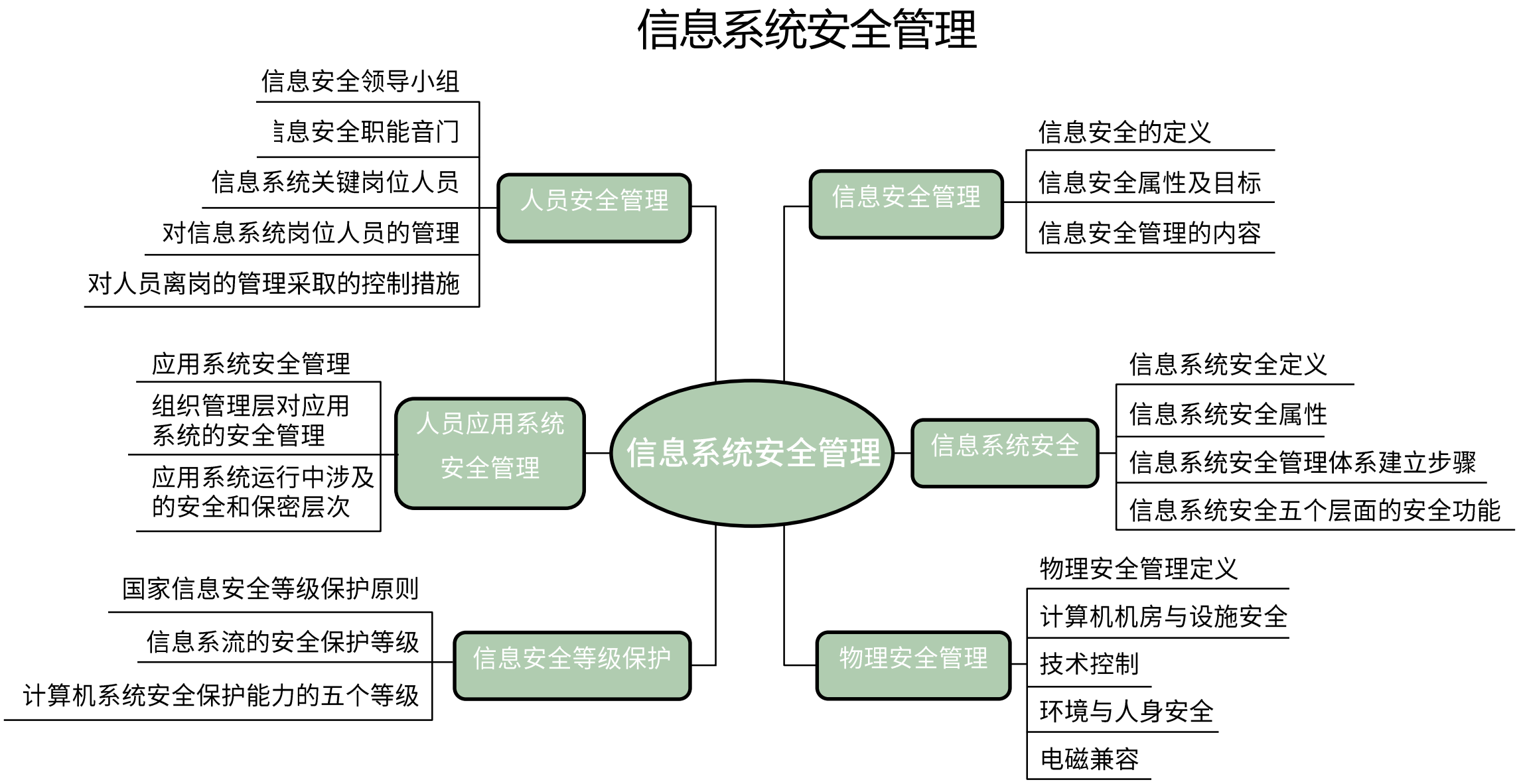
二、在风险和安全控制阶段，严格按照相关制度和流程进行风险和安全管理，依据风险应急计划处理相关风险，减少信息安全负面影响。

在该过程组中，我要求项目管理办公室定期或不定期的到相关科室收集需求调查表和问题提交表，总结归纳，然后交于我们项目团队进行处理。我每天都对当前活动收集齐**AC,EV,PV,CV,SV**等相关进度、成本工作数据，对其进行分析，对好的、坏的都进行分析归纳，找出其中的机会和威胁，进行相关的措施。为减少“信息安全负面影响”，严格执行系统审计保护级的规定，进行系统安全再评估、日志分析等控制方法，同时对重点监控日志采取了动态评估及定期评审，我以周和里程碑为单位，定期对系统安全日志实行再评估、审计。每周的项目例会中将系统安全管理作为单独一个议程，对系统威胁应对措施实施的有效性以及当前系统的状态进行检查。如果发现问题，团队成员集体讨论，对应对措施进行纠偏。

三、提高信息安全意识，确保信息系统项目风险可控

信息安全是一场不见硝烟的战场，我们必须高度重视，在该项目的风险和安全管理中，好的安全管理可以减少或减轻风险带来的危害。严格按照安全管理制度执行相关安全工作，是保证信息系统安全的有利保障。同时如果不注意安全管理的相关工作，就会给项目带来更多的风险，因此加强设备安全、数据安全、内容安全、行为安全管理是十分必要的，减少了“木桶效应”，提高大家的安全意识。

论文写作素材---信息安全类



论文写作素材---信息安全类

1．信息安全是指保护信息的保密性、完整性、可用性，以及其它属性。
保密性：是指信息不被泄露给未授权的个人、实体和过程或不被其使用的特性。数据的保密性可以通过下列技术来实现：最小授权原则、防暴露、信息加密、物理加密。
完整性：是指保护资产的正确和完整的特性。简单地说，就是确保接收到的数据就是发送的数据。数据不应该被改变。确保数据完整性的技术包括：协议、纠错编码方法、密码校验和方法、数字签名、公证。
可用性：是指需要时，授权实体可以访问和使用的特性。确保可用性的技术有：磁盘和系统的容错，可接受的登录及进程性能、可靠的功能性和安全进程和机制、数据冗余及备份。
保密性、完整性和可用性是信息安全最为关注的三个属性，也被称为信息安全三元组。这也是信息安全通常所强调的目标。

2、信息系统安全策略的核心内容就是“七定”，即定方案、定岗、定位、定员、定目标、定制度、定工作流程。按照系统安全策略“七定”的要求，系统安全策略首先要解决定方案，其次就是定岗。

3、 木桶效应
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。

论文写作素材---信息安全类

4、 计算机信息系统安全保护等级划分准则

《计算机信息系统安全保护等级划分准则》是建立安全等级保护制度，实施安全等级管理的重要基础性标准，它将计算机信息系统分为以下五个安全保护等级。计算机信息系统安全保护等级划分准则如表所示。

表：计算机信息系统安全保护等级划分准则

级别	等级	对象
第一级	用户自主保护级	用于普通内联网用户
第二级	系统审计保护级	用于内联网、国际网进行商务活动的、需要保密的非重要单位
第三级	安全标记保护级	用于地方国家机关、金融单位、邮电通信、能源与水源供给部门、交通运输、大型工商与信息技术企业、重点工程建设等单位
第四级	结构化保护级	用于中央级国家机关、广播电视部门、重要物资储备单位、社会应急服务部门、尖端科技企业集团、国家重点科研单位、国防建设等部门
第五级	访问验证保护级	用于国防关键部门、依法需要对计算机信息系统实施特殊隔离的单位

论文写作素材---信息安全类

5、信息系统安全保护的等级

信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。

一是受侵害的客体。等级保护对象受到破坏时所侵害的客体包括公民、法人和其他组织的合法权益；社会秩序、公共利益；国家安全。

二是对客体的侵害程度。等级保护对象受到破坏后对客体造成侵害的程度分为造成一般损害；造成严重损害；造成特别严重损害。

《信息安全等级保护管理办法》将信息系统的安全保护等级分为以下五级。

第一级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级：信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级：信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级：信息系统受到破坏后，会对国家安全造成特别严重损害。

论文写作素材---信息安全类

6、信息安全系统的体系架构及其组成

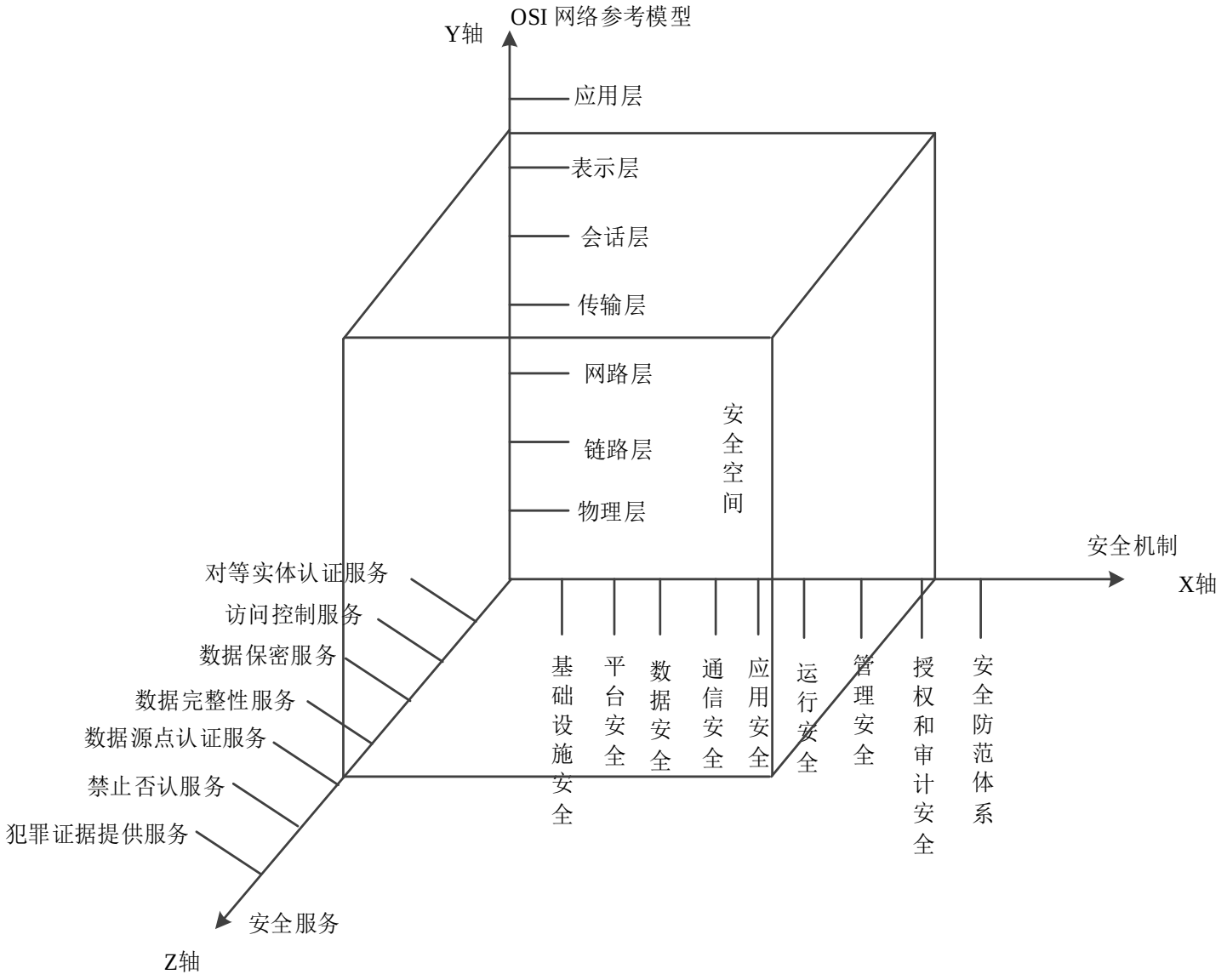
信息安全系统的体系架构及其组成，通常用信息安全空间来反应，如图所示。

X轴是“安全机制”。安全机制可以理解为提供某些安全服务，利用各种安全技术和技巧，所形成的一个较为完善的结构体系。如“平台安全”机制，实际上就是指的安全操作系统、安全数据库、应用开发运营的安全平台及网络安全管理监控系统等。

Y轴是“**OSI**网络参考模型”。信息安全系统的许多技术、技巧都是在网络的各个层面上实施的，离开网络，信息系统的安全也就失去了意义。

Z轴是“安全服务”。安全服务就是从网络中的各个层次提供给信息应用系统所需要的安全服务支持。如对等实体认证服务、访问控制服务、数据保密服务等。

由**X**、**Y**、**Z**三个轴形成的信息安全系统三维空间就是信息系统的“安全空间”。随着网络逐层扩展，这个空间不仅范围逐步加大，安全的内涵也更丰富，达到具有认证、权限、完整、加密和不可否认五大要素，也叫做“安全空间”的五大属性。



论文写作素材---信息安全类

7、安全技术

（1）加密技术

加密是确保数据安全性的基本方法。由于有加密技术的存在，必须有密钥管理技术的存在。在网络环境中，密钥管理显得格外重要。

（2）数字签名技术

数字签名是确保数据真实性的基本方法。利用数字签名技术还可以进行报文认证和用户身份认证。数字签名具有解决收发双方纠纷的能力，这是其他安全技术所没有的。

（3）访问控制技术

访问控制按照事先确定的规则决定主体对客体的访问是否合法。当一主体试图非法使用一个未经授权的资源时，访问控制将拒绝这一企图，并将这一事件报告给审计跟踪系统，审计跟踪系统将给出报警并记录日志档案。

（4）数据完整性技术

破坏数据的主要因素包括以下几个方面。

数据在信道中传输时受信道干扰影响产生错误或是被非法侵入所篡改，或是被病毒所感染等。

数据完整性技术通过纠错编码和差错控制来应对信道干扰，通过报文认证来应对非法入侵者的主动攻击，通过病毒实时检测来应对计算机病毒。

数据完整性技术包括数据单元的完整性和数据单元序列的完整性两种方式。

（5）认证技术

在计算机网络中认证主要有站点认证、报文认证、用户和进程认证等。

（6）数据挖掘技术

数据挖掘技术是及早发现隐患、将犯罪扼杀在萌芽阶段并及时修补不健全的安全防范体系的重要技术。

论文写作素材---信息安全类

8、 访问控制

访问控制是为了限制访问主体对访问客体的访问权限，从而使计算机系统在合法范围内使用的安全措施。

访问控制有两个重要过程。

一是认证过程，通过“鉴别”来检验主体的合法身份。

二是授权管理，通过“授权”来赋予用户对某项资源的访问权限。

（**1**）访问控制机制

访问控制机制分为强制访问控制（**MAC**）和自主访问控制（**DAC**）两种。

第一种，强制访问控制（**MAC**），用于将系统中的信息分密级和类进行管理，以保证每个用户只能访问到那些被标明可以由他访问的信息的一种访问约束机制。通俗的来说，在强制访问控制下，用户（或其他主体）与文件（或其他客体）都被标记了固定的安全属性（如安全级、访问权限等），用户不能改变他们的安全级别或对象的安全属性。在每次访问发生时，系统检测安全属性以便确定一个用户是否有权访问该文件。

第二种，自主访问控制（**DAC**），由客体的属主对自己的客体进行管理，由属主自己决定是否将自己的客体访问权或部分访问权授予其他主体，这种控制方式是自主的。也就是说，在自主访问控制下，用户可以按自己的意愿，有选择地与其他用户共享他的文件。在自主访问控制中每个客体都拥有一个限定主体对其访问权限的访问控制列表（**ACL**），每次访问发生时都会基于访问控制列表检查用户标志以实现对其访问权限的控制。

论文写作素材---信息安全类

（2）基于角色的访问控制（RBAC）
基于角色的访问控制中，角色由应用系统的管理员定义。而且授权规定是强加给用户的，用户只能被动接受，不能自主地决定，这是一种非自主型访问控制。其基本思想是，对系统操作的各种权限不是直接授予具体的用户，而是在用户集合与权限集合之间建立一个角色集合。每一种角色对应一组相应的权限。一旦用户被分配了适当的角色后，该用户就拥有此角色的所有操作权限。

（3）访问控制的授权方案
目前主流的访问控制授权方案，主要有以下四种。
其一，自主访问控制方式（DAC）：该模型针对每个用户指明能够访问的资源，对于不在指定的资源列表中的对象不允许访问。
其二，访问控制列表方式（ACL）：该模型是目前应用最多的方式。目标资源拥有访问权限列表，指明允许哪些用户访问。如果某个用户不在访问控制列表中，则不允许该用户访问这个资源。
其三，强制访问控制方式（MAC）：该模型在军事和安全部门中应用较多，目标具有一个包含等级的安全标签（如不保密、限制、秘密、机密、绝密）；访问者拥有包含等级列表的许可，其中定义了可以访问哪个级别的目标，如允许访问秘密级信息，这时，秘密级、限制级和不保密级的信息是允许访问的，但机密级和绝密级信息不允许访问。
其四，基于角色的访问控制方式（RBAC）：该模型首先定义一些组织内的角色，如局长、科长、职员；再根据管理规定给这些角色分配相应的权限，最后对组织内的每个人根据具体业务和职位分配一个或多个角色。

论文写作素材---信息安全类

9、安全审计

安全审计是记录、审查主体对客体进行访问和使用情况，保证安全规则被正确执行，并帮助分析安全事故产生的原因。

（**1**）安全审计的内容

安全审计具体包括以下几个方面的内容。

①采用网络监控与入侵防范系统，识别网络各种违规操作与攻击行为，即时响应（如报警）并进行阻断。

②对信息内容和业务流程进行审计，可以防止内部机密或敏感信息的非法泄漏和单位资产的流失。

安全审计系统采用数据挖掘和数据仓库技术，因此被形象地比喻为“黑匣子”和“监护神”。

（**2**）安全审计的作用

安全审计系统主要有以下作用。

①对潜在的攻击者起到震慑或警告作用。

②对于已经发生的系统破坏行为提供有效的追究证据。

③为系统安全管理员提供有价值的系统使用日志，从而帮助系统安全管理员及时发现系统入侵行为或潜在的系统漏洞。

④为系统安全管理员提供系统运行的统计日志，使系统安全管理员能够发现系统性能上的不足或需要改进与加强的地方。

论文写作素材---信息安全类

（3）安全审计的功能

CC标准将安全审计功能分为6个部分：安全审计自动响应功能；安全审计自动生成功能；安全审计分析功能；安全审计浏览功能；安全审计事件选择功能；安全审计事件存储功能。具体内容如下：

①安全审计自动响应功能：定义在被测事件指示出一个潜在的安全攻击时做出的响应，它是管理审计事件的需要，这些需要包括报警或行动。

②安全审计数据生成功能：要求记录与安全相关的事件的出现，包括鉴别审计层次、列举可被审计的事件类型，以及鉴别由各种审计记录类型提供的相关审计信息的最小集合。

③安全审计分析功能：定义了分析系统活动和审计数据来寻找可能的或真正的安全违规操作。它可以用于入侵检测或对安全违规的自动响应。

④安全审计浏览功能：要求审计系统能够使授权的用户有效地浏览审计数据，它包括审计浏览、有限审计浏览、可选审计浏览。

⑤安全审计事件选择功能：要求系统管理员能够维护、检查或修改审计事件的集合，能够选择对哪些安全属性进行审计。

⑥安全审计事件存储功能：要求审计系统将提供控制措施：以防止由于资源的不可用丢失审计数据。能够创造、维护、访问它所保护的对象的审计踪迹，并保护其不被修改、非授权访问或破坏。


百炼成钢
我们不仅仅要的是敲门砖
光环软考人
科创新力量