非官方辅导资料，如有错漏、纯属正常。

基于 Official （ISC)^2 Guide to the CISSP CBK, 4th 英文版翻译（**CBK_4**）

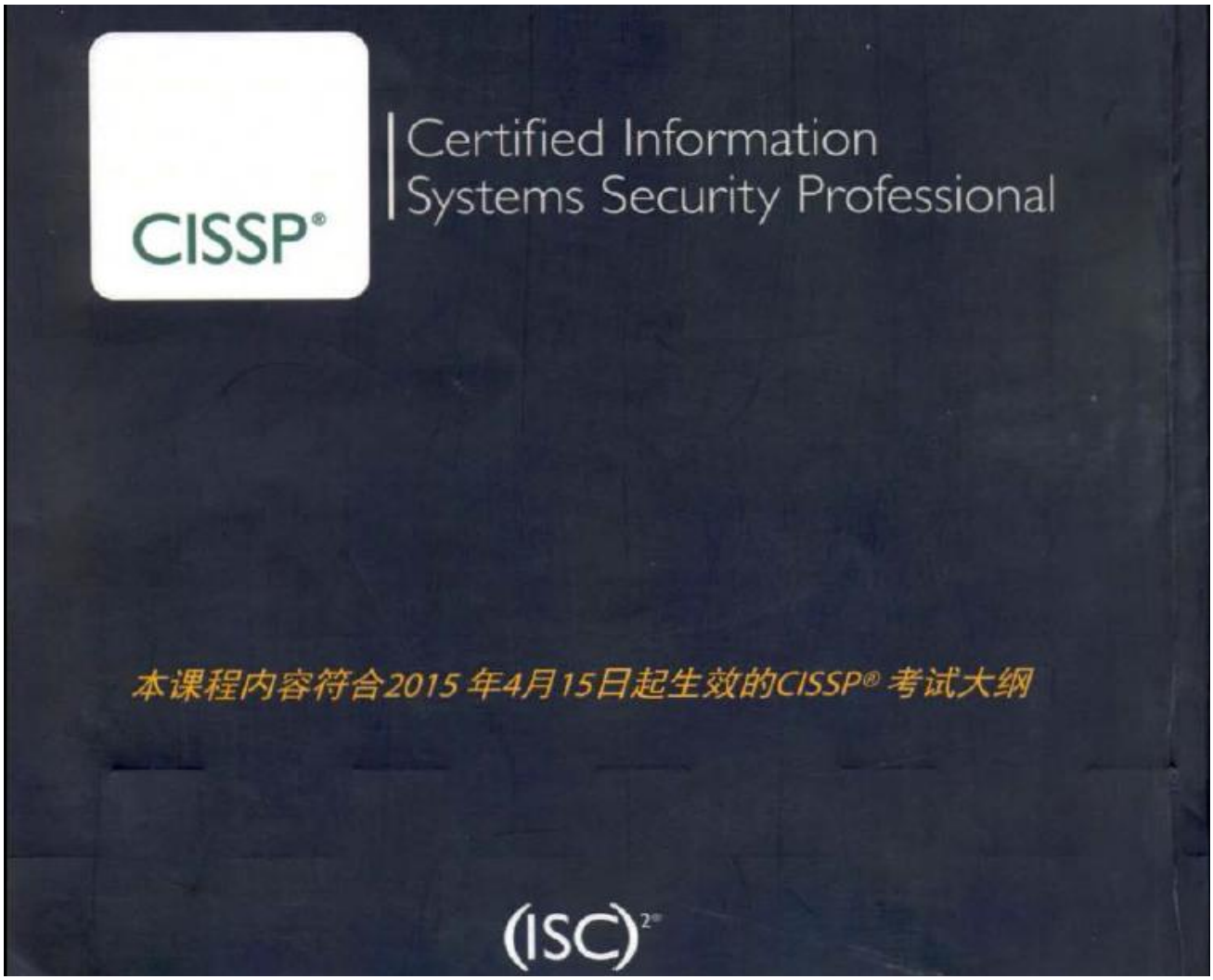
根据 CISSP Official Study Guide, 7th （**OSG_7**）和

CISSP All-In-One Exam Guide, 7th （**AIO_7**）进行补充完善

参考 CISSP All-In-One Exam Guide, 6th （**AIO_6**）中文版规范措词

结合官方习题集、历年真题和 Certpass、TestKing 最新模拟题对考试要点、难点进行归纳

2017.02 版



目　录

前　言

(ISC)²是一个注册商标，读作 ISC-Squared，是 6 个首写字母 IISSCC 的缩记，其全名是：The International Information Systems Security Certification Consortium，中文名是：国际信息系统安全认证联盟。它是全球最大的信息、网络、软件与基础设施安全认证会员制非营利组织，是 CISSP 认证考试的管理机构。

一、考试介绍

CISSP 考试是面向管理的，技术要求并不高，但要求知识面广，即“一英尺深一英里宽”。

1.考试的特点

①**全面**。8 个域的内容什么都会考，随机抽取，没有重点，但是有的知识域（章节）出题权重(数量)比较多。从准备角度来看，必须掌握大纲、教材或辅导书里的全部知识点；从做题角度来看，押题或收集真题是没必要也没意义的，官方的章节练习题、测试习题都很好的覆盖了知识点以及题型，且考试不会出现曾经做过的一样的题，但做好了习题集就一定能过。

②**基础**。考试没有技术难度大的分析，不研究具体的算法和协议，只要求理解各种模型、标准、算法、协议、流程的优缺点、应用方法与要求等，有计算机基础的人肯定看得懂。目的是知道该用什么技术来解决什么问题，而不是钻研某个技术的详细实现。大量考题都是在一个设定的场景里考基本的理论。

③**有限**。考试内容一定在 CBK 或者官方指定教材中，绝不会超出；据不完全统计，按照考试大纲，8 个域共有 65 个章节(模块)、198 个小节(要点)、1486 个知识点(考点)。

④**交叉**。大部分知识点并不是独立的，是互相关联、综合运用的，必须通过反复阅读和归纳总结来理清关系，建立知识体系，清晰的掌握相关联知识的应用领域、应用场景和方法。

⑤**离散**。CISSP 的通过率不高，不是我们不聪明，是没有中文版本的成体系的、全套的、完善的教材、辅导书和习题集，而且任何一本书都没有 100%的覆盖和详细描述 1486 个知识点，也没有把各章节的知识点关系串联起来，准备考试要花大量的时间去收集资料、梳理资料、理解资料、形成笔记，而且好资料全是英文版本的（中文的除了 AIO_6 和 OSG_7，其它的翻译都很滥，习题翻译更烂）。现在知识点都整理好了，过与不过全看你做了没做。

⑥**跑偏**。考试中出现的难题，一般是教材中没有详细讲述但 CBK 里有列举的知识点，或者是自己了解比较少的、不常用的标准/法规/协议/模型/流程等内容，总之要想考过，必须老老实实花时间来积累知识，攻克隐晦难懂的外国的标准/法规/协议/模型/流程。这里要强调的一点就是：不管你是科班出身还是半路出家，CISSP 对都是一个全新的知识领域，很多内容是可以和工作经验相关联，但绝不是你曾经学过的那些技术知识，一定要研究透它的知识体系。

⑦**易错**。做错题一般不是因为自己技术不好、理论不扎实，而是因为：看错题干；对自己工作领域以外的知识掌握不牢；按经验做题，没理解题目的出处、原文或考的知识点是什么；没建立知识体系、不理解美国思维，肯定会错；英文不好，不能从超滥的中文翻译反推出英语原文，肯定会错（看不懂英文原题也肯定会错）；逻辑不清晰、思考不仔细肯定会错（做完一半/150 题/3 小时，大脑就疲劳了）。考题的很多技巧与英语六级阅读理解题是完全一致的，必须理解题目的知识点、回忆到教材的原文出处，千万别扫一眼题目和答案就胸有成竹的作出选择，要看清问的是什么，考的是哪个知识点，所以英语阅读理解的技巧是同样适用的，如：

欢迎点击这里的链接进入精彩的Linux公社网站

Linux公社（www.Linuxidc.com）于2006年9月25日注册并开通网站，Linux现在已经成为一种广受关注和支持的一种操作系统，IDC是互联网数据中心，LinuxIDC就是关于Linux的数据中心。

Linux公社是专业的Linux系统门户网站，实时发布最新Linux资讯，包括Linux、Ubuntu、Fedora、RedHat、红旗Linux、Linux教程、Linux认证、SUSE Linux、Android、Oracle、Hadoop、CentOS、MySQL、Apache、Nginx、Tomcat、Python、Java、C语言、OpenStack、集群等技术。

Linux公社（LinuxIDC.com）设置了有一定影响力的Linux专题栏目。

Linux公社 主站网址：www.linuxidc.com 旗下网站：www.linuxidc.net

包括：**Ubuntu 专题** **Fedora 专题** **Android 专题** **Oracle 专题** **Hadoop 专题** **RedHat 专题** **SUSE 专题** **红旗 Linux 专题** **CentOS 专题**

Linux 公社微信公众号：linuxidc_com

有 any、only、every、must 等绝对性的描述肯定不对；文字最长的选项就是答案；在对立的选项里 2 选 1；字面很像的选项很可能是干扰项等等。

⑧**没用**。应试和运用是完全不同的，考过了这个证还是什么都不会，仍然成不了技术专家；当然，有这个公认的含金量高的认证，是一种认可，方便找工作和升职，而且学习过程可以梳理构建自己的知识体系，知道如何构建和运营一个完善的安防体系，也能结交人脉，对于提升综合能力有很大帮助。就像考驾照一样，考过了就有资格开车上路了，但你还是不敢马上独立跑高速、跑长途，必须搞台车练练手，才能成为老司机；相反，很多老司机常年跑车，但让他去再考一次驾照，不好好准备肯定过不了。技术高手不需要证书来证明，而且技术高手考试的通过率还都不高，因为他没有掌握考试的精髓。相反，管理人员的通过率高些。

2. 通过考试的必要条件

①**信息**。自己收集、整理相关的资讯和学习资料；搞清楚怎么约考、怎么背书、怎么维持 CPE 就行了；很多收费的资料都可以在网上找到免费的下载，但资料搞全后，就没必要浪费时间上网了（其实是在看电影、打游戏），需要上的网站只有几个，在汇编资料里有网址。

②**精读**。选择最新最全的 1 到 2 本教材，理解到每一句话，必须总结归纳出自己的学习笔记，该宝典就是作者边学边记的，不整理自己的笔记，就不能牢固的建立起自己的知识体系，碰到题目就不能快速查找资料，就没有一个辅助复习和方便查阅的知识要点集。这是一个从薄到厚，再从厚到薄的过程。

③**做题**。很多考点书上讲的不多、不全、不细，全靠做题来巩固。而且必须通过做题来理解它的出题思路和答题技巧。作者因为记忆差，考前把 8000 多道题反复做了 4 遍，复习半年后，3 小时可以轻松做 250 道题；当然，绝世高手可能不做题也能过。

④**英语**。看中文效率最高，以中文为主来看书是可以的，但最好扎扎实实看点英文资料，做大量英文题，因为很多考题的翻译很烂，需要看英文术语、用英文思维才能准确理解题干、判断混淆项和最佳项，而且考试真题的简体中文翻译也不符合我们平时学习的思维和表述。作者的知识体系全是用中文建立的，但做题只做英文题，做中文题实在难受，还会产生误解。建议：主看中文书学得最快，辅看英文书加深理解，只做英文题准确无误。

⑤**培训**。通过考试只能靠自己大量的学习和积累，培训班的作用是提供最新的中文资料，提供答疑、报名、背书和 CPE 维持服务，并不能用五天时间把知识全部塞进你的大脑，但可以介绍方法、思路、规则，提高你的学习效率，节省收集、整理的时间。其实，作者和身边的同事是同时参加了谷安、汇哲、爱思考、天融信的几个培训班，算是搞明白了，不过如此。我身边的人很多都没有时间听完全部的培训课程，而在线视频更是没一个人完整看下来了，我自己几十 G 的视音频资料从没看过，只要看 3 本书，做几千道题就够了。有了葵花宝典，你可以自己积累，钻研半年你也可以成为讲师了，不报班也能过。

报还是不报培训班，是个很纠结的问题，这里多说几句。如果有钱，肯定是报，某培训班研究 CISSP 很深入，全程服务也很细致。如果没钱，自学也完全可以通过，只是后续背书、CPE 维持挺烦琐的。还是举考驾照这个例子：现在国家新政策允许自学考驾照，不用再报驾校了，如果有一台车练手，按教程练肯定能不花钱轻松考到驾照，但如果对考场规则和流程不熟，而后续还有违章处理、上牌年审、保险理培什么的事，自己搞定是省钱了但费时伤神，花钱搞就省心了。不管报不报，花点小钱把资料搞齐还是可以的，相当于有台练手车，等熟练了，再决

定下一步怎么搞。

⑥**自信**。别想作弊、代考、押题什么的旁门左道了，从事安全行业，尤其是进入高层，必须具备最基本的职业道德和个人素养。

⑦**时间**。万事俱备，就差积累，最好封闭式学习，排除干扰，作者白天上班，晚上陪小孩家教再哄小孩睡觉，半夜 11 点到凌晨 2 点学习，坚持了 8 个月。

⑧**评测**。3 次闭卷模拟测试全部 80%正确率以上，就可以考试了。（有的培训班题目比较老旧，会要求学员模拟测试 90 分以上才能正式考）

⑨**考试**。内容熟悉的人，基本上 4 个小时以内就全部做完了，做的慢的都是模棱两可，知识不牢的人。总之，考试分数和复习时间成正比。做一个复习计划，然后按部就搬的执行就行了，过与不过全在于你做了没做，看你有多大的决心了。如果给一个标准的化，我认为，大部分人需要不间断学 2 小时×120 天就差不多了，基础较差、拖拖拉拉的人可能要 1 年以上。

3. 考试体验

①**时间**。约考不用太早，基本上提前个半个月预约就行了，会有考位的，约早了肯定准备不充分，总会纠结要不要延迟考试（50 美元/提前 24 小时改签），当然也可以早点约考，给自己一个明确的期限，倒逼自己抓紧时间。我是考前休假一周，每天一次连续完整的 250 题模拟考试，有把握通过了，才定的考试时间。模拟考中文题，一般 3 小时内完成；考英文题，一般 4 小时内完成。实际考试是简体中文，但全靠看英文对照做题，4.5 小时完成；中间自由休息几次；最后一个小时从头到尾把所有题检查了一遍，更正了 6 道题。考试时间绝大部分是上午 9 点到 15 点这个时间段，我约的是中午 13 点到 19 点这个时间段。如果上午考，早上准备工作仓促，路上拥堵奔波、人犯困，到了中午没饭吃，又饿、更困。如果下午考，有一上午时间轻轻松松慢慢做准备，在楼下吃个午餐，我还把葵花宝典完整看了一遍，然后提前 10 分钟到考场拍照、录掌纹。做完 150 道题，出来喝水撒尿；做完 250 题，又出来喝水撒尿，还跑楼梯间抽了根烟；最后一个小时完整检查了一遍，心想肯定过了，交卷走人，当场打印了成绩单。然后就约人吃火锅去了。

②**系统**。考试系统和考驾照科目四的理论考试系统差不多，和计算机等级、职称英语等很多机考的考试系统都差不多，界面看上去是很过时的、老旧的程序风格，字体也很粗糙，菜单和功能相当的简单，右上角显示剩余的时间和完成的题数。做题是不能跳着选做任一题的，必须从头到尾逐个的做，因为你除了点击答案，只能点“上一题、下一题、做标记”3 个按钮。老老实实一个一个的做，挺枯燥的，头昏眼花，如果不是长期加班学习和多次模拟考的磨练，根本坐不住 6 个小时。等全部做完 250 道题，才出现检查题目的功能菜单，可以比较灵活的选择性的检查做题了。检查题目支持 3 种方式做题：一是全部从头到尾检查，二是只显示做了标记的题，三是自己随时可以点击“检查”按钮按需选择要检查的题。

③**真题**。考试的真题没有和做过的练习题是一样的（老外确实用心出题了，题库保密工作还做得挺好）。真题仍然是大量的管理类、理论性、概念性、理解框架模型原理流程方法的题，虽然内容都很明显在考试大纲范围内，但很多的具体知识点的描述并不是熟悉的中文教材、辅导书里的原文；有的是在 CBK 或 NIST 800 系列特别出版物中有类似的描述；有的是在特定场景里的实际情况。如果不好好看书，归纳出学习笔记，光靠题海战术也是过不了的，何况 CISSP 没有一套像样的中文习题集（“天龙八部”里汇编了 3410 道中文练习题，我都很不满意，还

是要靠做英文题来积累和巩固）。250 道题，总共约有 3 道排序题、3 道拖拉匹配题、3 道图片点击选择题；其余全部是单选题。绝大部分是题干不长，就问 2 句话的简短问题，约有 200 道；还有 50 道是情景题，就是先描述一个场景，然后告诉你后面的 3 道题都是基于这个场景的；而且，每间隔 20 道普通简短题，就会出一道情景题，这个规律和节奏还是很稳的（情景题一定要小心，不然一偏差就会连错 3 道）。真题的中文翻译虽然是经过了审核校验的，但我还是一头雾水，所以全程都是点开英文来做题。感觉考试题是由香港人翻译成中文的，比如 organization 考试中翻成“机构”，教材中翻成“组织”，erase 考试中翻成擦除，教材中翻成清洗，还有好多差别不记得了。而且很多题前后有关联、暗示的关系，做到后面，会启发到原来前面那个题应该是这样的。所以必须留时间检查题目。

二、宝典内容

葵花宝典的核心是要点笔记，是一系列的资料汇编和整理（培训班的内部资料是没有的），包括 CISSP 必过三部曲：

1.九阴真经（知识之源）：最新的、最权威、最全面的官方的学习资料汇编，大部分已经是中文了。这是最基础的资料，英文中文都要看，反复看；先粗看后做题，做了题知道差距后再精看；最后就可以不看了，内容都吸收理解到学习笔记里了。包括：

①书籍（好多）

▲考试大纲中、英文版/Exam Outline,Candidate Information Bulletin-2015（**CIB**）▲CBK 官方指南_第 4 版中英文/Official (ISC)2 Guide to the CISSP CBK, 4th（**CBK4**）▲CISSP 官方学习指南_第 7 版/CISSP Official Study Guide, 7th英文版（**OSG7**）▲CISSP 认证考试指南_第 6 版/CISSP All-In-One Exam Guide, 6th中文版（**AIO6**）▲CISSP 认证考试指南_第 6 版/CISSP All-In-One Exam Guide, 6th英文版（**AIO6**）▲CISSP 学习指南一步登天/11th Hour CISSP Study Guide▲CISSP 预习指南黄金版/CISSP.Prep.Guide.Gold.Edition.Wiley▲CISSP 内训核心辅导书/Study Guide, Third Edition-2016▲CISSP 必考要点笔记/CISSP Comprehensive Review Notes-2016▲中文资料▲备考经验介绍一大堆

②课件（共 8 套）

▲中文培训讲义 8 个域 2016▲知名机构 CCCURE 的新版培训课件 8 个域 CBK4_2015▲美国 CISSP 特训班完整讲义（1500 页）▲官方中文培训讲义 10 个域 2013▲国内培训机构自制讲义 10 个域 2013▲AIO 中文培训课件 10 个域 2013▲AIO 英文培训课件 10 个域 2013▲Shon Harris (CISSP all in one 的作者)编写的 CISSP 讲义▲中文思维导图全集▲英文思维导图全集

③视频（共 5 套）

▲10 个域中文培训辅导视频全集 2013▲8 个域英文培训辅导视频全集 2015▲美国 5 天特训班完整培训视频全集 2015▲美国知名机构完整培训视频全集 2015

④音频（共 3 套）

▲国内机构中文 5 天培训完整音频全集 2015▲美国 5 天特训班完整培训音频全集+讲义+习题 2015▲知名机构 CCCURE 的新版培训录音 8 个域 CBK4_2015

2.葵花宝典（去粗取精）：全部知识点的梳理。按照考试大纲的结构，把各大权威资料的知识点进行汇总，梳理成知识笔记，覆盖率达到 95%以上。学习过程就以该笔记为基础，边看书、边自己理解，再整理完善这个笔记；精读完几本官方教材后，就可以甩开书了，以笔记为

参考，大量做题，用好 Word 的导航窗格、PDF 的导航标签以及内容搜索功能，可以快速找到任一考题的知识点；做完各章节的题，基本上就建立知识体系了，就可以冲刺复习，做 N 套综合的模拟考试题，把笔记里已经掌握的知识逐步删掉，只留下需要重点回顾记忆的知识，最后就变成一个小册子了，考前好好过一遍就可以进考场了。为了方便学习，该宝典提供完整的 Word 版本，可以自行编辑整理。（友情提示：该宝典的内容仍有部分错误和偏差，复习过程中自己去感受、修正吧，模棱两可没把握的知识点一定要自己去查验核实）

3.天龙八部（百炼成仙）：2016 年以来的最新的、最权威、最全面的官方的习题集汇编（精品题库 12000 道，备选题库好多好多套）。其中核心题集涵盖了 AIO、OSG、CBK 和官方出版物的最有价值的习题共 7812 道（其中中文 3410 道，真题回忆 640 道）；整理的 2016 年综合模拟测试题共 10 套、3380 道；全部都有答案解析，不用来回翻看几本书、到处查找答案，而且知识疑惑直接在葵花宝典里可以找到原文。当然，AIO7 附带的练习题光盘（1629 道选择+90 道拖拉匹配）和 OSG7 提供的在线练习题（1400 道，拖拉、卡片各种形式）是非常好的学习资源，也有必要做，做完必过。关于 PDF 题库的使用方法：用 PDF 编辑软件看书和习题（ACROBAT 什么的），用下划线、加色等方式可以注释笔记、选择答案和做过的题，比用纸质书的效率要高。（此外，第二梯队备选题库，汇总了国外知名的英文模拟题和 2015 年以前的各大中文题集等，如果精力旺盛看看也行）汇编前的原文题库有：

▲CISSP Official ISC2 Practice Tests 官方指定习题集及解析（2016 出版备考必看）

▲CISSP Practice Exams 最新官方习题集第四版（2016 出版备考必看）

▲Certpass.CISSP 最新模拟题集 V2016-01-04

▲CISSP 正版题库 TestKing.v10.245Q

三、培训机构

2013 年起，考试已经是简体中文；OSG7 中文版已于 2017 年出版；知名培训机构也研究撰写了大量中文资料和测试题；CISSP 的应试难度将有所下降，通过率和持证人数应该会大幅提高。关于培训班的对比，本来详细列了很多对比，算了，不说了。**关于通过率：**瞎猜测 2016 年全国约考人数 398 人，参加考试约 304 人，第一次通过约 207 人。

四、主流教材

可以作为学习教材或辅导书的只有 OSG、AIO、CBK 这 3 本，其它的精品英文书籍也很多，中文讲义也很多，可以做为补充资料、参考资料，CBK 的内容比较全、但看得难受，其它都不全，但容易理解。葵花宝典的内容是全面而且高度归纳的，没有精读过教材直接看宝典很难快速理解透，每一句话都有大量的信息，这是一个学习和思考的过程。建议：

①精读 OSG7_2 遍，搞定这一本就够了，边看边梳理葵花宝典笔记；

②通读 AIO6 中文版和 CBK4 中文版各 1 遍，边看边完善笔记，补充、巩固知识点；

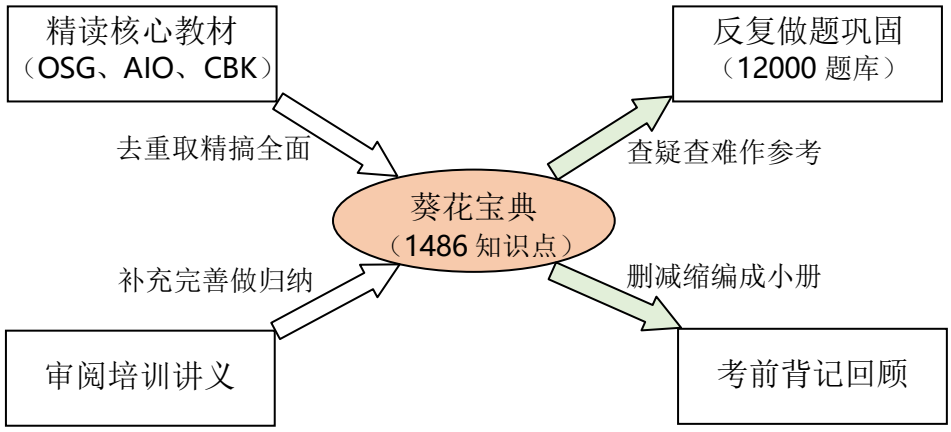
③阅读 AIO7 英文版新增的内容，继续完善笔记；

③审阅 1 遍中文 PPT 讲义，继续完善笔记（如果报了班，就在培训时边听边完善笔记）；

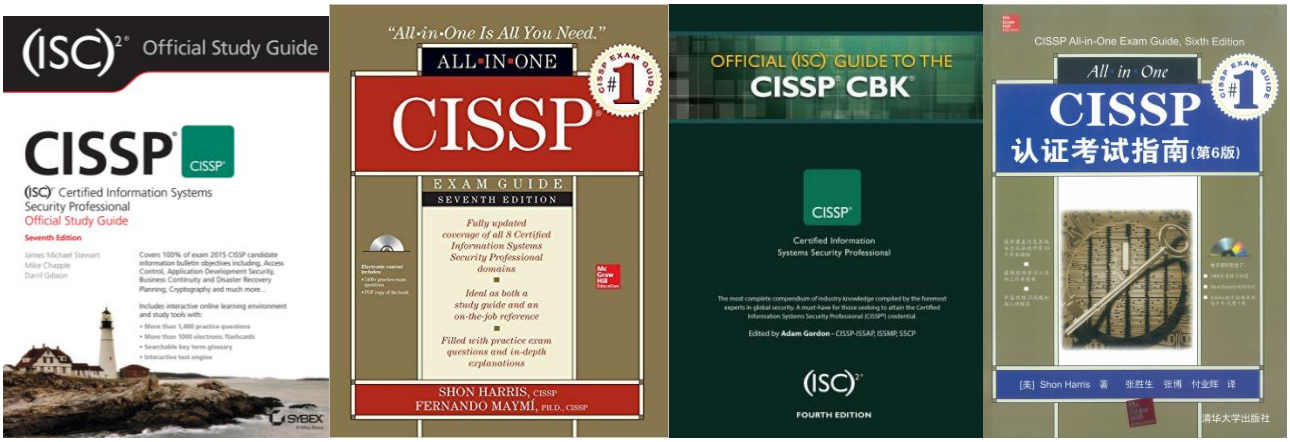
④学完做题，做完再学，学完再做。

作者采用的是学习方法是“一看二记三做题，查漏补缺模拟考”，先看中文书学的快，只做英文题理解透，属于笨鸟型学习法，对于学霸型人才，肯定有更高效快速的学习方法。

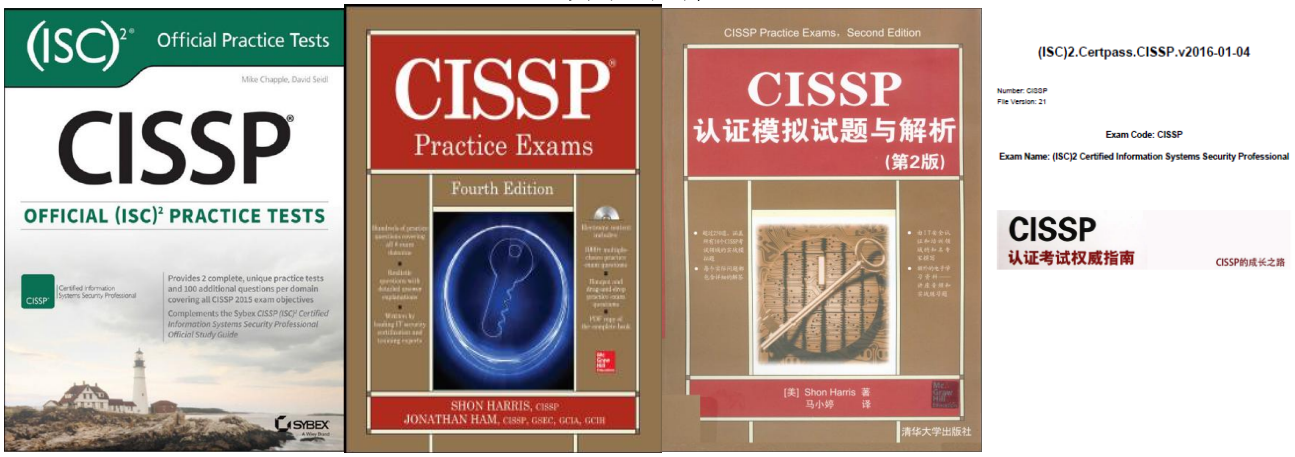
关于葵花宝典的作用与方法，下面这个图可以做个参考：



教材按重要程度排序：



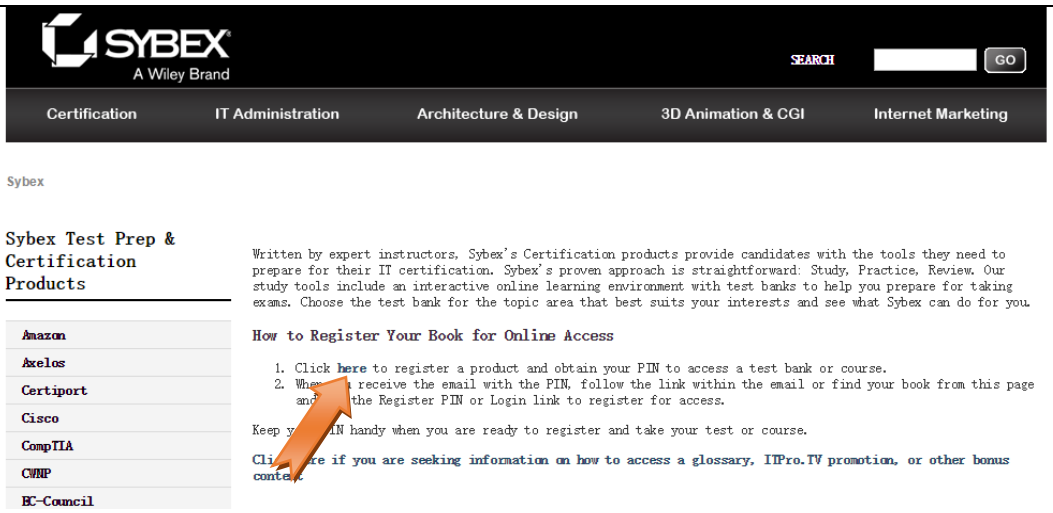
常用习题集：



OSG7 在线练习题的注册方法：

OSG7 书上的网址是错的，可以登陆 www.wiley.com/go/sybextestprep 注册，根据提示回答问题就行了。也可以登陆 sybextestbanks.wiley.com，

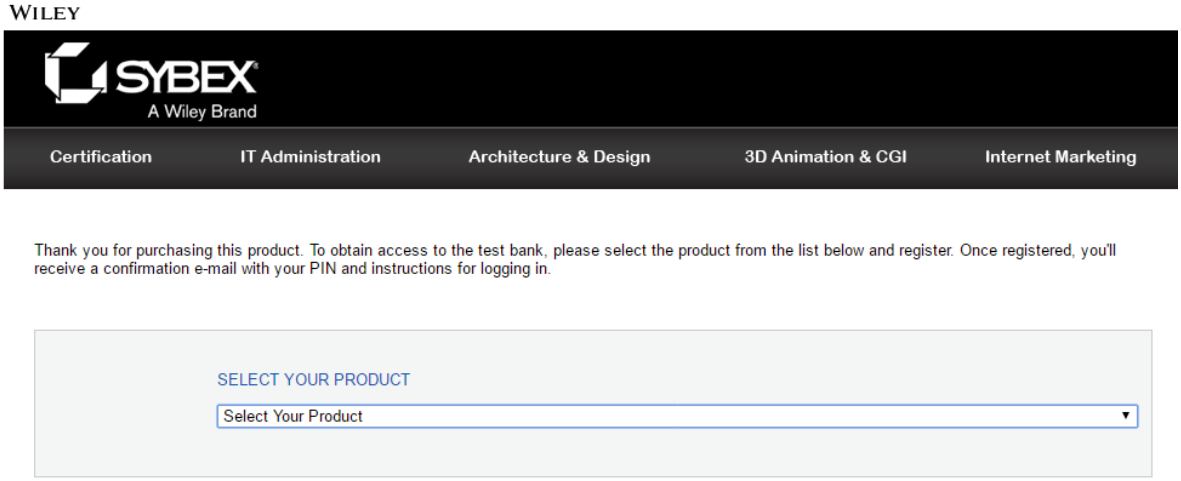
或 http://sybextestbanks.wiley.com/course/index/id/102，选择 ISC2，即进入在线学习，要先注册。点击 here 就可以进到注册页面了。



注册使用在线练习题：

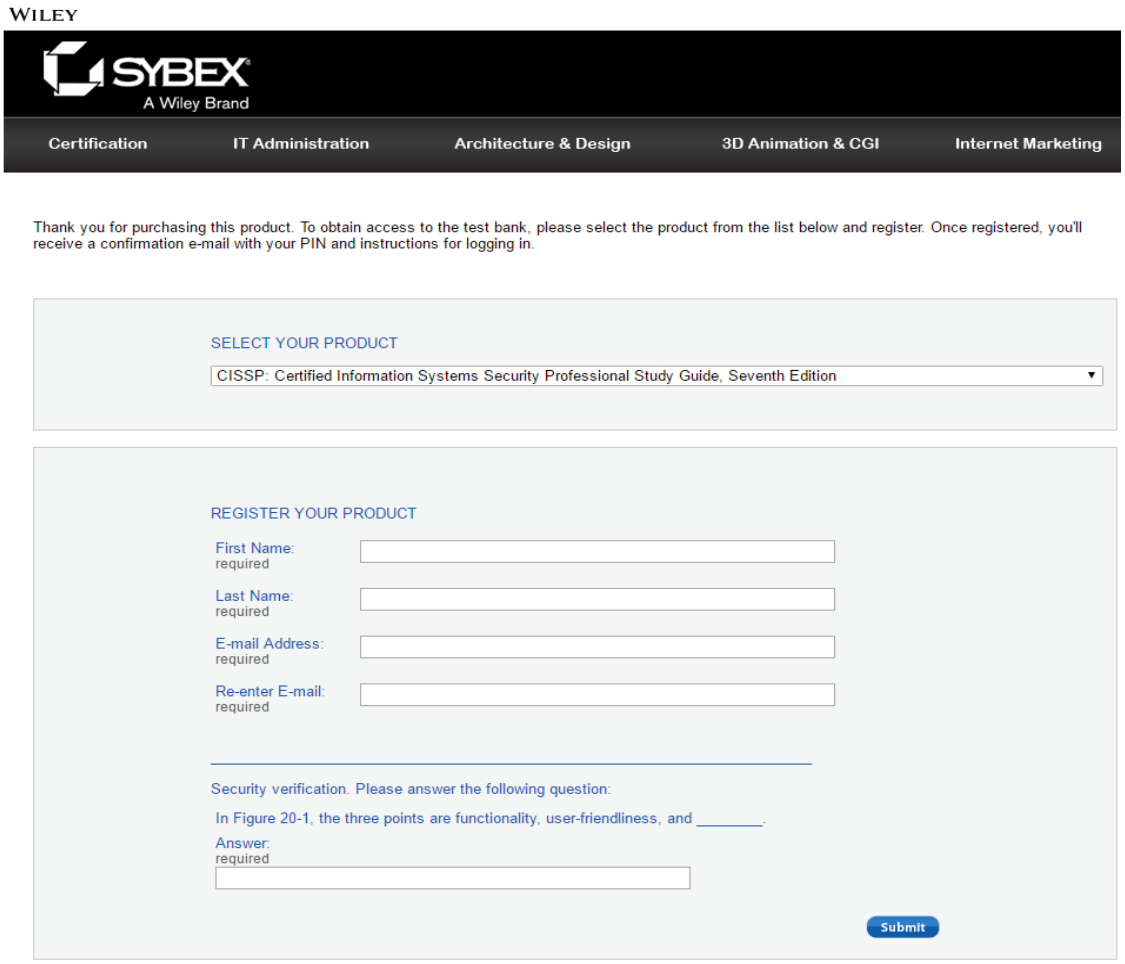
页面 1 地址如下，选择 CISSP Study Guide 7th 这本书就行了，自动进入页面 2.

http://customer.wiley.com/CGI-BIN/lansaweb?procfun+shopcart4+SH4FN19+funcparms+PARMKEYG%28A0060%29:SYBEX



页面 2 地址如下，填写资料并回答一个关于书本内容的验证问题，就 OK 了。

http://customer.wiley.com/CGI-BIN/LANSAWEB?WEBEVENT+ROE37314884A6B8014146071+PRD+ENG



上面讲的乱七八糟的，其实只要搞对网址，内容都看得懂，都有提示。

另外就是 AIO7 附带的光盘习题 1692 道，是非常接近真题的。

五、知识简析

老外干什么事情，最喜欢的就是标准化思路，按科学的套路来。先搞清楚原理、机制，然后制定出一套标准/框架/模型什么的；然后遵循这个标准/框架/模型，根据实际需求来拟制出完善详细的策略/方案/计划；接着就按计划通过一系列的管理/治理/运营的方法手段来实施和执行各项具体的工作；还要对完成的每项工作或者产品进行测试评估和认证认可才能接受或验收；最后根据业务的完成效果再来修订标准/框架/模型。为什么要搞架标准/框架/模型呢？这就是“标准化”观念，可以实现高效协同、量化管控、避免误解。

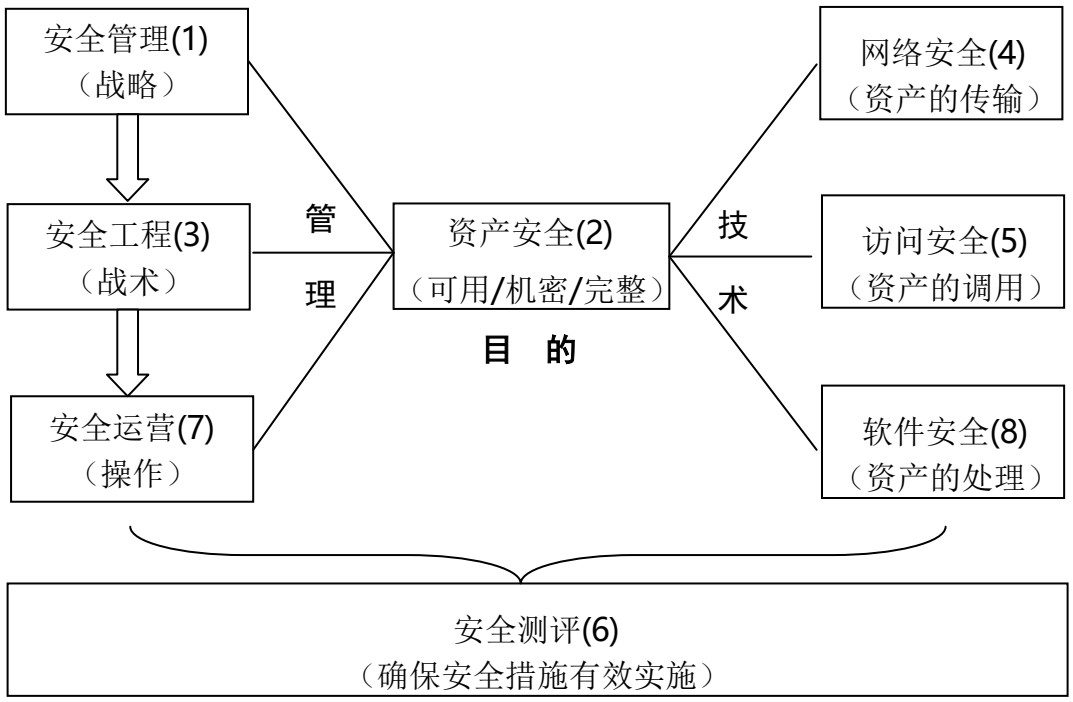
针对 CISSP 的应试，基本路子就是要通过学习充分理解其 CBK 的内容，建立起自己的信息安全知识体系。在全部 8 个知识域中，各域的层级不同、方向不同、相互关联。通过学习建立起自己知识体系的一个重要标志就是：看到任何一段内容或题目，能快速反应，知道它对应于 CBK 或考试大纲里的哪章？哪节？或者对应于教材里的哪个知识点，这就是有的放矢。当然，知道那么多点知识点的位置出处还不够，还要理解它的内容（需要大量时间积累）。建议先初步建立起知识框架，再仔细理解所有内容细节。

1. 知识框架

属于管理范畴的知识域有 3 个，涵盖了信息安全各个专业领域，包括从高管管理到中层组织到基层操作的 3 个层次：**安全管理（即统筹治理）=>安全工程（即组织实施）=>安全运营（即具体操作）。**

属于技术范畴的知识域有 5 个，针对某类信息安全业务工作，包括：**网络安全；资产安全；访问安全；软件安全；安全测评。**

具体看图：



总的来看，8 个域知识可概括为：

从三个层次来逐级抓好安全管理工作；（左）

从三个方面来合力完成资产安全任务；（右）

通过测试与评估来确保工作有效落实。（下）

当然，你也可以从攻与防、安全内核到外部的层级、数据的生命周期、系统的安全需求与安全确认等角度来理解和构建各域知识。

2. 知识概要

①安全和风险管理（安全管理）

这是上层的，讲方法、讲原则、讲策略、讲宏观、讲管理。包括：

*安全的目标：三元组；

*实现的途径：安全治理，治理的方法和思路；

*解决的方案：各种角色分工合作、联动协调；

*实现的策略：策略、指南、操作 3 个层次；

*工作的落实：应尽职责、应尽关注；

*法规的依据：法律、法规、道德的约束；

*管理的核心：把“事”管死，把“人”管活；

*实现安全先要搞清楚风险：包括风险管理的基本要素、概念；还有流程（识别和评估）；也有方法（定量和定性）；还有风险的处置（消减、转嫁、接受）；还有风险管理的架构与威胁建模。

*风险管的再好，也会出现问题，那么业务连续性的工作和灾难恢复的工作必须要做。

②资产安全

*什么是资产：要分类和分级，要搞清关系（资产所有者、监管者）；

*怎么保护敏感资产：就要搞清数据质量，正确的处置和重用数据；

*保护资产的安全措施：保存、传输、使用都要有措施，最低的标准就是基线。

③安全工程

作为一个安全总监，怎么管好一个公司的整体信息安全呢？

*工程的生命周期：各阶段怎么做安全，安全原则啊；

*做安全体系的各种模型：BLP、好多，就是做安全系统用的；

*模型的检测、评估和选优：TCSEC、CC、ISO15408 好多，有分功能和水平；

*通用硬件、软件的基本架构和安全功能、安全原理；

*实现安全的基本手段：密码学，反正不考数学和算法，不难，对称、非对称，散列什么 的，最重要的搞清密码学的应用，什么加密用在加解密、完整性、身份认证等什么场景，怎么用；

*怎么搞好一个站点的安全：设计、规划、建设和运维一个站点，各种物理安全要懂。

④通信与网络安全

*肯定先学网络架构和安全原则了：最重要的分层的思想，安全边界的运用，封装和解封的各层的协议。

*然后要清楚基本网络组件的安全：各种硬件设备啦、终端啦、介质啦；

*通信最重要的就是信道的安全了，最重要的方法就是 VPN 了，最重要的措施就是接入认证了；

*搞清楚各种针对网络的攻击和防御。

⑤身份与访问管理

*先是背景理论：什么是访问控制；

*访控的四个要素：好多要素，几个步骤；

*实现 4 个要素的身份管理系统：SSO 什么的；

*如何做好身份的标识和认证呢：单因素多因素什么的；

*授权机制：不同的需求和出发点用不同的授权；

*针对访问管理 IAM 的攻击和防御。

⑥安全评估与测试

安全好没好，只有搞了评估才知道。

*策略：目标、人员和责任；

*怎么做评估与测试,几个方面的工作：日志分析、代码测试、渗透测试，好多方法；

*收集了好多评估和测试的结果数据，就感知到企业的威胁了，安全态势出来了，安全措施必须要加强了；

*审计完了，审计报告怎么写呢？

⑦安全运营

*老外认为运维的第一重要工作合法合规，是要调查取证，不是为了保障业务。

*配置管理，这就是具体的运营工作了；

*运营的原则：可信路径、隐蔽通信什么的，好多；

*又讲一遍怎么具体的保护资产；

*运营的流程：事件的管理最重要。

*出了问题怎么办：

*怎么预防问题和事件：

*变更要管理，灾难要恢复；

*运营也包括对物理设施的运维，就是要保护好物理空间，都是物理的访问控制技术。

⑧软件开发安全

*软件开发的基础和安全原则，SDL，有数据库啊、语言啊什么的。基础内容很多，但不是直接出题的，题都在后面的内容里，放在具体场景里出；

*软件开发可能存在很多问题：漏洞、恶意代码、病毒；

*老美还很在意软件的评测和购买。

3.各域按出题比例排序（权重）：

01_安全与风险管理_Security and Risk Management_16%，40 题；

07_安全运营_Security Operations_16%，40 题；

05_身份识别与访问控制_Identity and Access Management_13%，33 题；

04_通信与网络安全_Communication and Network Security_12%，30 题

03_安全工程_Security Enginering12%，30 题；

06_安全评估与测试_Security Assessment and Testing_11%，27 题；

02_资产安全_Asset Security_10%，25 题；

08_软件开发安全_Software Development Security_10%，25 题。

共 250 道题。

第一域　安全与风险管理（例如安全、风险、合规、法律、法规、业务连续性）

Chapters 1,2,3,4,19 in OSG 7th

Chapters 2,9 in AIO 6th

A. 理解并应用保密性、完整性和可用性的概念

1. 安全的主要目的和目标就是 CIA 三要素/三元组

①机密性（Confidentiality）：机密性是指因为工作需要而访问敏感资源。机密性通常通过最小权限原则来实现。安全架构师使用数据分类、访问控制和加密来确保资源的机密性。

②完整性（Integrity ）：完整性包括两个方面，一是确保信息被正确处理且不被未授权的人修改，二是保护网络上传输的信息。完整性控制包括事务控制、数字签名等。

③可用性（Availability）：可用性确保资源可用、系统正常运行。可用性的防护措施多种多样，诸如集群、发电机、备份和热站等。影响可用性的威胁包括自然的、人为的灾难，还有拒绝服务攻击等。

这三个目标的对立面通常称为 DAD，即：破坏，篡改，和泄露。

这三个因素之间彼此影响。如：客体缺乏完整性，则机密性就无法被维护。又如：加密提供机密性，但如果密钥丢失，就会产生可用性问题。

不同机构对三元组的重要性排序也不同，如军队首先看重机密性，而企业更重视可用性。

2. 安全管理涉及的其它重要概念

在第五域还会复习这些概念。

①身份识别/标识（identification）ID

用户向系统声称其真实身份的方式。身份标识是一个过程，主体先表明或提供自己的身份，然后认证、授权，并且具备可问责性。计算机无法区分不同的人，只能通过 ID 账号来区别。（用户名是识别工具）

②身份认证（authentication）鉴别

测试并认证用户的身份。认证或检测所表明的身份是合法的过程，就是身份认证。最常见形式是使用密码。通过与合法身份(也就是用户账号)数据库中的一种或多种因素进行比较，身份认证能够识别并承认主体的身份。身份认证和上面的身份标识总是作为一个过程中的两个步骤被一起使用，不能分开。（密码、令牌都是认证工具）

③分配权限（authorization）授权

为用户分配并校验资源访问权限的过程。确保主体获得符合其身份级别的访问权限。（访问控制列表 ACL 是授权工具）

④可问责性/可追溯性（accounting）

确认系统中个人行为和活动的能力。只有在主体的活动可问责时，你才能够保持安全性。就是必须要检验主体的身份，并跟踪记录其活动。只通过密码认证是最不安全的，用户可能推卸自己的过失操作行为。

⑤不可否认性/抗抵赖性（undeniable）

能确认信息发送者即创建者的能力。不可否认性确保主体无法否认其已经发生的行为事件。不可否认性是可问责性不可缺少的部分，如果嫌疑人不承认有关证据或指控，那么他的行

为就无法被问责。

⑥AAA 服务（authentication、authorization、accounting）

就是指认证、授权和可问责，常用于身份认证系统，实际包括了五个方面的元素：识别、认证、授权、审计和可问责性。如果一个安全机制缺少这五个元素中的任何一个，则这个机制就是不完整的。

3. 几种实现安全的解决机制（考题会问 XX 方法是利用和实现了什么安全机制？）

在操作系统里这些机制全都有应用，在第三域里要掌握，在第八域里也要掌握。

①分层

简单地使用、连续的多重控制，也被称为深层防御。比如物理上设置多道安检大门，技术上部署多套独立的不同原理的安防系统。“分层”和操作系统里的“环形”是差不多的。

②抽象

抽象有 2 种方式，一是面向对象编程，被抽象的对象组件内的操作和数据都是不可见的（黑箱）；二是将实体抽象分级，提高管理效率，比如：客体按密级分类，主体按职能分配角色等。

③数据隐藏

数据的物理存储空间是不能公开，也不能直接访问的，从而防止主体发现或访问数据。比如阻止应用程序直接访问硬件，不让未授权的访问者访问数据库等。

④加密

加密技术是安全控制非常重要，尤其在系统之间的传输数据时。

⑤进程隔离

进程隔离要求操作系统为每个进程的指令和数据提供不同的内存空间，并强制实施分界，以阻止某一进程读取或写入属于另外一个进程的数据。这样可以阻止未经授权的数据访问，也可以保护进程的完整性。

4. 两种数据分级方案 classification

以前书上叫“分类”，以后用“分级”个词更准确。

一般公开的、非涉密的数据不列入分类级别，也不适用于“分级”这个专业术语。

①军政一般分三级

绝密(top secret)—秘密(secret)—机密(confidential)，和非机密(unclassified)。

这是教材的字面翻译，其实与中国实际不同，在国内军政是这么分的：

（核心）、绝密、机密、秘密、内部、公开。

②商业一般分三级（不同公司的标准不一样，CISSP 考的是这种标准）

机密(Confidential)——隐私(Private)——敏感(Sensitive)，以及公开(Pulbic)。

Confidential 是企业的，更高的是国家的 secret，最低的是个人的 Private。

B. 应用安全治理原则

什么是安全治理 secure governance？其实就是信息安全管理。

安全治理是与支持、定义和指导组织安全工作相关的实践集合。安全治理与企业治理和 IT 治理密切相关，其目标都是相同的，都是维持业务流程，同时努力追求增长和弹性。

安全治理是一个框架：即管理层提目标，实施层操作，共同实现企业安全的一个有效机制。

主要内容有：组织的安全目标、任务，组织级的流程，安全角色和职责，安全战略等等。（目标、责任、方法、检查）。第三方治理通常包括外部人员或审计人员，重点是外包服务的安全目标、要求、法规和合同义务的合规性。

常用的安全治理的实践标准有：ITIL、ISO27001、COSO、COBIT 等。

B.1 使安全功能与组织战略、目标和使命相一致 （例如：商业案例、预算和资源）

没什么要考的内容。

B.2 组织级过程 （例如：并购、剥离、治理委员会）

没什么要考的内容.

B.3 安全角色与职责

1.按照在安全环境中出现的逻辑顺序介绍六种安全角色：

在第二域 B 章节又把与处理数据相关的角色讲了一篇。

首先是信息安全官 CFO（Information Security Officer / Chief Security Officer），不解释了，分管安全的最高领导，还是要服从 CEO 的。

①高级管理者 Senior management

组织所有者(高层管理者)，负责所有策略、负有最终责任。所有活动在被执行之前，都必须得到高层管理者的认可和签字。

②安全专家/信息系统安全专家（Information systems security professionals）

安全专家、信息安全官或计算机应急响应团队(CIRT)，是受过培训和经验丰富的网络、系统和安全工程师，他们对落实高层管理部门下达的安全任务。主要包括制定和实现安全策略。安全专家不是决策制定者，他们只是实现者。

③数据所有者（Data owners）

负责对信息进行分级的人，是层次较高的、最终负责数据保护的管理者。不过实际管理数据的任务会委派给数据管理员来实施。数据所有者具有“应尽关注”的职责，要负责数据的分级，如果数据所有者工作繁忙，可以将数据保护的日常维护工作委托给数据管理员完成。

④数据管理员/保管员（Custodian）

负责实施安全策略和上层管理者下达的保护任务。包括：完成和测试数据备份、确认数据的完整性、部署安全解决方案以及根据分类管理数据存储。

⑤用户（user）

是具有安全系统访问权限的任何人。要求了解组织的安全策略，并遵守规定的操作过程，在已定义的安全参数内进行操作，以便维护安全策略。

⑥审计人员（Information systems auditor）

负责测试和认证安全策略是否被正确实现，以及相关的安全解决方案是否合适。审计人员要撰写合规情况报告和有效性报告，高层管理者会审查这些报告。负责检查系统，判断系统是否满足安全需求，以及安全控制是否有效

⑦安全委员会（security committee）

成员来自：高级管理层代表、IT 管理者、业务部门和职能部门负责人、信息安全官等。安全委员会的责任：决策并批准安全相关事务、策略、标准、指南和程序。

⑧安全管理员（Security Administrator）

负责实施、监视并执行安全规定和策略；各部门可以设立自己的安全管理员，负责执行本部门安全管理事务；向安全委员会/信息安全官报告。

⑨其它

帮助台（Help desk）：接报并确认安全事件，向合适的人员转达以便响应。

审计委员会（Audit Committee）：由董事会授权帮助检查和评估公司内部运行、内部系统审计以及财务报告的透明度和精确度以帮助相关利益人持续对公司有信心。

灾难恢复/应急计划人员：从整体上负责组织的应急计划；与应用所有者、信息安全人员等协同工作，取得其他应急计划支持。

应急响应团队 CIRT（Computer Incident Response Team）：评价安全事件和造成的损害，提供修补系统正确的响应，搜集证据。

搞清数据所有者、系统监管员、安全管理员的关系（必考）！

B.4 控制框架

安全规划步骤中最重要的一步，也是第一步，就是考虑组织想要的安全解决方案的整体控制框架或结构。而 CISSP 考试的一个重点构架就是**信息及相关技术控制目标**（COBIT），但不考它的详细内容，具体参考第九域中的法规。

1.3 种类型的控制：

①管理控制/软性控制（Administrative controls）。

②技术控制/逻辑控制（Technical controls）。是软件或硬件，例如防火墙、ID、加密、身份认证以及鉴别机制等。

③物理控制（physical controls）。保护基础设施、人身安全以及资源安全的物理设施。

2.常用的企业管控与治理的实践框架：

1.安全方案开发：ISO/IEC 27000 信息安全管理

2.企业架构开发：①Zachman, TOGAF 企业架构框架；②TOGAF；③DoDAF；④MODAF

3.安全企业架构开发：SABSA 安全架构框架

4.公司治理：COSO 企业内控管理模型

5.安全控制开发：①COBIT IT 内部控制；②NIST 800-53 安全控制参考

6.流程管理：①CMMI 软件开发管理；②ITIL IT 服务管理；③Six Sigma 业务流程管理

7.其他相关：①PMBOK, Prince2 项目管理；②ISO9000 质量管理；③ISO 38500 IT 治理；④ISO22301 业务连续性管理

这些不同的安全标准和框架不会考具体内容，但一定要清楚各自的目的和用途，会考某个情景应该选择哪种控制框架！（详见第九域）也要理解安全规划（宏观的安全管理）必须具有不断循环的生命周期，不断对其进行评估和改进。任何进程中的生命周期都可以用不同的方式描述，通常使用下面的步骤：

①计划和组织——②实现——③运营和维护——④监控和评估

3.与系统架构相关的概念定义

①架构 Architecture。就是一个客观存在的系统组织体系，包括系统的成员组成、相互

关系、设计原则等。

②架构描述 Architectural description (AD)。采用标准的表达方式描述架构组成的一系列文档。

③受益主体 Stakeholder Individual。其利益与该系统密切相关的团队、机构等。

④视图 View。从某些方面对整个系统的状况、态势进行展现。

⑤视角 Viewpoint。根据不同需要选择从哪些关注面去构建和使用一个视图。

B.5 尽职关注/应尽关注(Due Care)

①应尽关注/适度关注/应有义务/适度谨慎 Due care：就是通过合理的关注保护组织利益，例如：开发规范化的安全结构，包含安全策略、标准、基线、指导方针和程序等内容。

②应尽调查/应尽职责/应有责任/适度勤勉 Due Diligence：就是维持好应尽关注的成果。例如，将上述安全结构应用到组织的 IT 基础设施中。

企业要实现安全，就必须高度关注做好具体业务，还要高度重视做好审查分析。

讲了那么多，还是搞不清楚什么是关注，什么是调查，其实是先要做好了“调查”，才能做好“关注”。再换一种通俗的说法：

①**应尽关注 Due care（遵循规范/补漏洞）**：企业必须要承担这样的责任：尽心做好安全管理、尽力阻止安全漏洞、尽量消减安全风险，以减少潜在的利益损失和负面影响。举个例子：一家公司如果不花钱建立完善的防火措施，他就是没有履行“关注”的责任；当真的发生火灾了，股东、员工和客户都可以依法起诉这家公司，因为它没有履责而造成了重大损失。

②**尽职调查 Due Diligence（限定时间/找漏洞）**：企业必须要开展这样的活动：全面了解安全隐患、准确发现安全漏洞、客观评估安全风险，确保后续能真正有效地实施安全控制与保护工作。也就是说：公司必须经常分析潜在风险、发现火灾威胁，从而能及时提出要实施的防火措施。

B.6 尽职调查/应尽职责(Due Diligence)

写在上面了。

C. 合规

法律、法规相关的内容在第七域 B.4 章节也有。

合规性是符合或遵守规则、策略、法规、标准或要求的行为。

C.1 法律法规的合规

法律到底考什么，考多深，说不清楚，国际性的通用法规标准肯定会考到。这对所有应试者都是薄弱的章节，各种法案太多太乱了。不过再怎么样，也不会超出宝典里的内容，虽然很难记住。实际参加完考试，并没有回忆出太多太具体的直接考法规的题，尤其美国本土的法律原则上是不会考的，虽然各种练习题里有很多。

1.法律的类型

①民事法（民事准则）Civil law(code)：欧洲使用的，与美国的民事法律概念不同，下级法院不用服从上级法院。Rule-based law, not precedence-based。

②普通法 Common law：英国制定的，美、加、澳都用，包括刑法、民法（民事侵权）、行政（管理）法，使用法官和陪审团。Based on previous interpretations of laws。

③习惯法 Customary law：中国、印度等采用混合法律的地区使用，主要处理个人行为。Deals mainly with personal conduct and patterns of behavior。

④宗教法律体系 Religious law：伊斯兰国家使用，并不创建法律，而是试图发现法律的真理。Based on religious beliefs of the region。

⑤法例法律体系：通常由民法和普通法组成，荷兰、加拿大、南非等国用。

CISSP 考的是普通法法律体系（Common law），包括 3 类法：

①民法（侵权法）Civil law：处理针对个人或公司遭受的破坏或者损失，民事诉讼导致的结果是经济赔偿和或社区服务，而不是坐牢。如果有人在民事法庭状告另一人，陪审团会判断是谁的责任，而不是宣判有罪或者无罪。

②刑法 Criminal law：在一个人的行为违反政府法律时使用，是为了保护公众，判罚通常是坐牢。

③行政（管理）法 Administrative law：政府机构创建，用于监管公司或特定行业人员的表现和行为，如食品安全标准、防火规范等。

关于符合性(GRC)的概念

符合性通常指确保行为符合既定的规则以及提供工具来验证符合性的行为，它包括法律以及企业自身策略的符合性。

C.2 隐私要求的合规

详见 D.5 章节。

D. 在全球化背景下理解与信息安全相关的法律和法规问题

D.1 计算机犯罪

主要讨论美国的法律，CISSP 会考以下每个法律的目的是什么，主要内容是什么？（虽然原则上只考国际法规，但官方题库中涉及到了以下的所有法案）。

1. 计算机诈骗和滥用法案（Computer Fraud and Abuse Act）（历史第一个）

国会在 1984 年制定了计算机诈骗和滥用法案（CFAA），主要针对下列罪行：

①非法访问联邦系统中的机密信息或财务信息。

②非法访问联邦政府使用的计算机，以及联邦计算机进行欺诈活动

③对联邦计算机系统造成恶意损失超过 5000 美元的行为。

④非法修改计算机中的医疗记录。

⑤非法买卖计算机密码。

该法案在 1986 年进行了修正，主要拓展了使用范围，涵盖了：

①由美国政府专门使用的所有计算机。

②由金融机构专门使用的所有计算机。

③被用于进行犯罪的所有计算机组合。

2. 计算机安全法案（CSA 1987 年）Computer Security Act of 1987

国会还是不满 CFAA 的 1986 修正案，又制定了计算机安全法案(1987 年)，为所有的联邦

机构设置了安全要求基准。CSA 的四个主要目的是：

①明确由美国国家标准技术研究所(NIST)负责开发联邦计算机系统标准和准则，由美国国家安全局(NSA)提供技术性建议和援助。

②颁布并施行上述的标准和准则。

③要求所有使用涉密联邦计算机系统的操作人员，都要制定安全计划。

④所有相关的 管理、使用和操作人员强制性参加定期培训。

⑤它还指定了 NIST 负责公开系统的安防，NSA 负责机密级系统的安防。

这条法案的相关要求经过多年演进后，形成了联邦计算机安全策略的基础。

3. CFAA 修正案（1994 年）

1994 年，国会对上述法案又进行了大改。包括以下条款：

①生成任何类型恶意代码的行为是不合法的。

②法案适用于所有被用于州间贸易的计算机。

③允许关押罪犯，不管他们是否造成了实际的损坏。

④计算机犯罪的受害者可以提起民事诉讼，其受到的损失可以获得减轻和补偿。

2015 年，奥巴马也准备做个修改，把计算机犯罪纳入 RICO 条款范围中，即反诈骗腐败组织集团犯罪法(the Racketeer Influenced and Corrupt Organizations Act)，不知道现在正式颁布没有。

4.国家信息基础设施保护法案(1996 年)（National Information Infrastructure Protection Act of 1996）

1996 年，国会还是不满 CFAA，又通过了一系列修正案，再进一步扩展了其保护的范围，包括以下新覆盖的领域：

①放宽了法案的范围，除了用于州间贸易的计算机，还包括用于国际贸易的计算机系统。

②扩展了对国家基础设施(铁路、燃气、电力和通信线路等)的类似保护。

③故意造成国家基础设施重大损坏的行为，要从重处理。

5.联邦判决指导方针（Federal Sentencing Guidelines）

1991 年发布的联邦判决指导方针主要提供计算机犯罪的处罚指导、解释说明等，它最重要的三个条款是：

①提出**审慎者规则**（prudent man rule）。就是要谨慎工作，这种规则要求高管确保他能常态化的、持续的保持适度关注（due care）的态度；其它人员同样也要求保持谨慎工作的态度。这个规则以前用在在财政领域。（就是领导责任制）

②提出从轻处罚规则。对于有违法行为的组织机构和执行官，如果它能证明其保持并运用了适度关注的原则，并履行了自己的信息安全责任，那么可以从轻处罚。

③明确了要证明疏忽或差错确实成立的三个要素。即：被控人员必须具有法律上认可的责任；被控人员必须未遵守公认的标准；疏忽行为和后续损害之间必须存在因果关系。

④高管渎职可以处以最高 2 亿美元的罚款。

6.文书精简法案(1995 年)（Paperwork Reduction Act of 1995）

文书精简法案（199 年）要求组织机构必须获得美国行政管理和预算局 OMB(Office of Management and Budget) 的批准后，才能请求使用各类基础公共信息。2000 年的政府信息安

全改革法案 GISRA（The Government Information Security Reform Act）对它进行了修正。

7.政府信息安全改革法案(2000 年) GISRA （Government Information Security Reform Act of 2000）

国会要求 GISRA-2000 的拟制满足以下**五个基本目标：**

①要提供 1 个内容全面的体制。确保所有政府相关的信息资源安全、有效。

②要确保网络协同安全、有效。一切系统都是基于网络的，所以必须安全。

③要有效监控和掌握所有与安全风险相关的活动和信息。每个人的每个行为都要被监控。

④开发和维护联邦政府的信息安全防护系统。既要满足安全需求，也要实现最小成本。

⑤提供改进机制。能持续优化、完善联邦机构的信息安全监督体系。

GISRA 仍然明确，NIST 负责非机密系统，NSA 负责机密系统，并实行领导负责制。

GISRA 重新定义了计算机系统的分类，明确了**关键系统要满足以下条件：**

①被法律条款定义为国家安全系统。

②有机密信息且被相应的措施保护。

③系统被攻击会对机构的业务产生不良影响。

在这之后，国会总算不再折腾了，没有通过任何新的关于计算机犯罪的重大事项。虽然提了一些草案，都还没通过，如：2012 年的网络安全法案和 2013 年的网络情报共享和保护法案。

8.联邦信息安全管理法案 FISMA（Federal Information Security Management Act）

在 2002 年通过的联邦信息安全管理法案（FISMA），要求联邦政府实施一个信息安全项目，涵盖了政府部门的运营和外包商的活动。NIST 开发了 FISMA 的实施指南，提出了确保信息安全项目有效的关键要素：定期评估风险、安全意识培训、定期渗透测试、记录突发情况、制定应急响应流程等。

D.2 许可与知识产权（例如：版权、商标、数字版权管理）

世界知识产权组织(World Intellectual Property Organization,WIPO)简明地定义了知识产权。将知识产权分为两类：

①版权：涵盖了文学和艺术作品。**②工业产权：**如发明(专利)、工业设计和商标。

1.版权主要保护 8 类作品：

文学作品、音乐作品、戏剧作品、哑剧和舞蹈作品、绘画图形和雕刻作品、电影和其它音像作品、声音录音、建筑作品。

法律规定，只要创作者的作品产生出来，起就立即自动享有版权。如果能证明你就是作品的创作者，那么你就会受到版权法的保护。不过，在官方机构正式注册作品，可以政府承认他们在具体的日期收到了你的作品，并认可你的版权。越来越多的“盗版软件”(warez)站点出现了，这个 Warez 就是指非法传播盗版。

版权法不像商业秘密法那样保护特定的资源，它保护的是有资源意义的表达而不是资源本身。它保护表达方式，而不是其本身。

专利更多地针对发明本身，而版权则涉及如何再生产和分发。从这个角度看，对版权的保护弱于对专利的保护，但是版权保护的时间更长。版权的保护期是在受保护者的寿命基础上再加上 70 年。（死后再保护 70 年）

2.数字千禧年版权法案(DMCA)（Digital Millennium Copyright Act）

DMCA 中有 2 个条款（**打击盗版**）：

①阻止用户破坏版权保护机制。非法的复制会被处以巨额罚款。

②网络服务商（ISP）的线路被用于传播盗版，也要承担相应的责任。

3.商标（Trademarks）

商标是单词、口号和标志语，用于标识某家公司及其产品或服务。保护商标的主要目的是在保护个人和组织机构知识产权的时候避免市场的混乱。与版权的保护一样，为了获得法律的保护，商标不需要正式注册，可以使用 ™ 符号来表示出你想要保护作为商标的单词或口号。如果想让别人正式承认商标，那么可以在美国专利和商标局(US-PTO) 进行注册。注册的商标用 ® 符号表示。

在美国，商标准许的初始期是 10 年，可以再连续不受限制地使用 10 年（共 20 年）。

4.专利（Patents）

专利是最强的知识产权保护形式，保护发明者的知识产权，是授予个人或公司的法律所有权，使他们能够拒绝其他人使用或复制专利所指的发明。专利保护期一般是 20 年。

专利要满足以下要求：

①该发明必须是新的。（新）

①该发明必须是有用的。（有用）

③该发明不能是显而易见的。（难）

5.商业秘密（Trade Secrets）

商业秘密是公司特有的资产，对其生存和盈利有很大作用。版权和专利存在要公开细节，保护时限等问题，所有公司必须自己可是你办法保护商业秘密。很多公司都要求其员工签订一个保密协议 NDA(Non Disclosure Agreement)。

6.经济间谍法案(1996 年)(Economic Espionage Act of 1996)

经济间谍法案（1996 年）主要有 2 个规定：

①任何被发现为外国政府或机构而从美国公司窃取商业秘密的人，可以被处以高达 50 万美元的罚款和长达 15 年的监禁。

②任何被发现其它情况中窃取商业秘密的人，可以处以 25 万美元的罚款和 10 年的监禁。

7.许可证（Licensing）

要熟悉软件的许可证颁发协议。许可证有四种类型：

①签书面合同。②写在软件包装外面。③单击许可证协议来完善软件安装。④云服务许可协议，在屏幕上弹出一个确认已阅读并同意条款的确认框。

8.统一计算机信息处理法案 UCITA（Uniform Computer Information Transactions Act）

统一计算机信息处理法案(UCITA)，提供了计算机相关业务处理的共同架构，包括对软件许可证颁发的规定。UCITA 为上述的②、③形式的许可提供了法律描述和保护。还要求用户可以在安装之前拒绝许可证协议，生产商必须全额退款。它要求不同州之间的“许可协议”都符合统一的标准。

D.3 进口/出口控制

美国有两部法律与此相关：

①国际武器贸易条例法案(International Traffic in Arms Regulations Act，ITAR：1976)

②出口管理条例法案(Export Administration Regulations Act，EAR：1979)。

CISSP 考试要求对出口控制问题有大致的了解，是否有强加在科技和技术信息之上的限制和控制。

D.4 跨境数据流

瓦森纳协议(Wassenaar Arrangement)

WA 是对“常规武器和两用货品及技术”实施进出口管制的法律，来用阻止恐怖国家的军事实力增强，由 40 个国家共同制定了 9 类端口的出口规范，包括特殊材料、高科技设备、保密机等产品。

D.5 隐私

个人可识别信息 PII（Personally identifiable information）是用来唯一识别、联系或者定位一个人的数据，往往被用于身份盗窃、金融犯罪和各种犯罪活动中。

1.美国有关隐私的法律

好多，眼花缭乱。必考的，要背下来。

①第四修正案（Fourth Amendment of the Constitution）

隐私权的基础是美国宪法的第四修正案，内容如下：法律保护个人的人身、房屋、证件和财物不受无理的搜查和没收。搜查检索必须要有许可。

②隐私法案(1974 年)（Federal Privacy Act of 1974）

美国的隐私法案(1974 年)是对美国联邦政府有关公民个人私有信息处理的最重要的法律。任何机构在没有得到当事人书面同意的情况下，不得向他人泄漏隐私信息。

③电子通信隐私法案(1986 年)ECPA（Electronic Communications Privacy Act of 1986）

电子通信隐私法案(ECPA)规定对个人电子隐私的侵犯是犯罪行为。最重要的规定禁止窃听，不能偷电邮，否则处以最高达 500 美元的罚款和最高 5 年的监禁。（其实美国在窃听全世界）

④执法通信协助法案(1994 年)CALEA（Communications Assistance for Law Enforcement Act）

执法通信协助法案(CALEA)是对上面那个 1986 年的电子通信隐私法案的修正。它要求通信运营商允许持有法院命令的执法人员进行合法窃听。

⑤经济和专有信息保护法案(1996 年)EPPA（Economic and Protection of Proprietary information Act of 1996）

该法案将经济信息也视为财产，盗窃并不局限于物理产品。

⑥健康保险的易移植性和可问责性法案(1996 年)HIPAA（Health Insurance Portability and Accountability Act of 1996）

HIPPA 经常被考到，它要求医院、医师、保险公司和其它处理或存储个人医疗隐私信息的组织采取严格的安全措施，明确定义了个人在医疗记录方面的权利。

⑦2009 关于经济和临床健康的卫生信息技术法案 HITECH（Health Information Technology for Economic and Clinical Health Act of 2009）

关于经济和临床健康的卫生信息技术法案(HITECH)对 HIPAA 进行了修订。主要变化是针对商业伙伴(BAs)的。它将所有相关机构定义为：处理被保护的健康信息（PHI）的组织机构。任何 PHI 机构和一个商业伙伴（BA）之间的关系必须有书面合同管理，这个合同被称为业务联合协议（business associate agreement，BAA）。

HITECH 还明确了数据泄露的通告范围：发生泄密事件的 PHI 机构必须通知受影响的个人，影响超过 500 人时，必须通知卫生和人事服务部（the Secretary of Health and Human Services）的部长和媒体。

HITECH 是全国性的法律。此外，每个州都颁布了自己的相关法规。加利福尼亚州的 SB1386 是第一个发布的，涉及以下隐私信息：社会保险号、驾照号码、身份证号码、信用卡或借记卡号码、银行账户与安全代码、病历、医疗保险信息等。

⑧数据泄露通知法 DBNL（Data Breach Notification Laws）

若有泄密事件，当事单位必须在 60 天以内通知个人信息被非法访问。（如果影响超过 500 个人，还必须向媒体发布相关事件）。

⑨儿童联机隐私保护法案(1998 年)COPPA（Children’s Online Privacy Protection Act of 1998）

儿童联机隐私保护法案（COPPA）对儿童网站的信息保护提出了一系列要求。它要求任务组织必须要取得父母的同意后，才能收集 13 岁以下儿童的信息。

⑩Gramm-leach-Bliley 法案(1999 年) GLBA/金融服务现代化法案/格蕾姆

GLBA-1999，严格限制了银行、保险公司等商业机构之间的信息共享和服务提供。

⑪美国爱国者法案(2001 年)（USA PATRIOT Act of 2001）

这个是国会对 2001 年 911 事件的响应。它扩大情报机构的权限，将以前一次只能获取一条线路的监听授权扩大为可以获得对一个人的有所通信进行监听的一揽子授权。另一方面，允许网络服务提供商(ISPs)提供更多的信息。它 OpenID 还修正了计算机欺诈和滥用法案(CFAA)，对犯罪行为从重处理。

⑫子女教育权利和隐私法案 FERPA（Family Educational Rights and Privacy Act）

FERPA 是关于教育机构的，保护成年学生和未成年学生父母的隐私权。

⑬身份偷窃和冒用阻止法案(1998 年)（Identity Theft and Assumption Deterrence Act）

就是规定身份偷窃是严重的犯罪行为。

⑭萨班斯-奥克斯利法案(SOX-2002) Sarbanes-Oxley ACT

2002 年的该法案(简称为 SOX)适用于在美国上市的任何公司，其中的许多法律被用于监管会计行为以及公司上报财务状况所使用的方法。然而，某些部分(特别是 404 条款)直接适用于信息技术。SOX 对公司如何追踪、管理和报告财务信息提出了专门要求，这包括保护财务数据并保证它的完整性与真实性。大多数公司都依赖计算机设备和电子存储来进行事务处理和数据归档，因此公司必须采用适当的流程和控制来保护这些数据。公司管理人员，包括首席执行官(CEO)、首席财务官(CFO)和其他人员，如果不遵守 Sarbanes-Oxley 法案，那么可能导致严厉的处罚，甚至可能会入狱数年。

2.欧盟有关隐私的法律

①概括指令（directive outlining privacy measures）

1995 年，欧盟(EU)议会也通过了描述隐私措施的概括指令（directive outlining privacy measures）。要求所有个人数据的处理要满足有关标准，明确了个人对自己信息的处理权利。

②美国—欧盟安全港湾项目/安全避难所（避风港 Safe Harbor program）

经过与联邦数据保护和信息、委员会的商讨，美国商务部开发了独立的安全港湾框架来调和欧美对于隐私不同的处理方式，并给美国组织提供一种优化的方法以符合欧盟数据保护法的要求：数据出口方和进口方之间的合同必须需要事先获得国家数据保护当局的批准，方可传输数据到国外。为了符合安全避难所规定，在欧洲进行商业活动的美国公司必须满足 7 项处理个人信息的要求。这里强调下经常考的 7 个安全港原则。这是美国贸易部的一个控制机制，防止未授权的信息泄露，相关的术语有：

1)通知 notice：任何组织必须告知个人使用数据的目的。（告知我）

2)选择 Choice：任何组织必须为个人提供可选择的机会。（我选择）

3)向前传输 Onward transfer：组织只有在遵守通知及选择规则的基础上才能向其他组织传输资料。（别乱传）

4)安全 Security：组织必须保护好数据。（别泄密）

5)数据完整 Data integrity：组织不得将信息挪用，还要确保数据真实可信。（别乱改）

6)访问 Access：个人可以查、改或删组织所持有的他们的个人信息。（属于我）

7)执行 Enforcement：组织必须落实以上各条原则。（别搞事）

安全港湾项目的目的是有效衔接美国与欧盟不同的隐私法律与标准，主要针对的是欧盟的 The EU Data Protection Directive（欧联数据保护纲领），它就包括了上面的 7 个原则，不过它也将在 2018 年被 GDPR (European Union’s General Data Protection Regulation)取代。

3.支付卡行业数据安全标准（Payment Card Industry Data Security Standard）

支付卡行业数据安全标准(PCI-DSS) 是一个非法律但有合同义务的优秀合规要求典范。有 12 个主要要求，不列举了。它提供了一系列关于支付安全控制的标准。

D.6 数据泄露/数据破坏

了解下法规，基本上就是出现泄密事件必须 24 小时内上报。

1.电子通信服务规范(Regulation for Electronic Communication Service, EU: 2013)

欧洲电子通信服务提供者，需要在检测到个人数据泄露后不迟于 **24 小时**向国家主管当局提供个人数据泄露的数据泄露通知。

2.隐私和电子通信法规(Privacy and Electronic Communications Regulations.UK: 2013)

电子通信服务提供商，诸如电信，互联网服务供应商(ISPs)，在知道数据泄露的基本事实后必须在 **24 小时**内通知 UK 信息专员办公室。

E. 理解职业道德

E.1 践行(ISC)² 职业道德规范 Code of Ethics

在你参加考试和成为 CISSP 之前会被要求签署(ISC)²道德规范。你需要理解道德规范并把它应用到现实当中，诸如组织内的用户群体的道德责任。

1.(ISC)2 道德规范序文 Code of Ethics Preamble

The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

Therefore, strict adherence to this Code is a condition of certification.

“我们坚守国家安全，对雇主负责，始终遵守最高的道德行为标准和相关要求。”

“因此，严格遵守这些准则是通过认证考试的必然条件。”

2.(ISC)2 道德规范准则 4 条/Code of Ethics Canons:

*Protect society, the common good, necessary public trust and confidence, and the infrastructure.

*Act honorably, honestly, justly, responsibly, and legally.

*Provide diligent and competent service to principles.

*Advance and protect the profession.

①保护社会，国家和基础设施。

②行为诚实、正直、公正、负责和合法。

③为雇主尽职尽责服务。

④提升能力和促进行业发展。

顺序很重要，①是最重要的准则。

3.尊重考试

A CISSP candidate and a CISSP holder should never discuss with others what was on the exam. This degrades the usefulness of the exam to be used as a tool to test someone’s true security knowledge. If this type of activity is uncovered, the person could be stripped of their CISSP certification because this would violate the terms of the NDA upon which the candidate enters prior to taking the test. Violating an NDA is a violation of the ethics canon that requires CISSPs to act honorably, honestly, justly, responsibly and legally.

已经通过 CISSP 考试的人不得与其它任何人谈论、议论或讲授关于考试内容的信息，针对应试而进行的真题收集等活动，将严重影响考试对考生真实能力素质的评估效果，从而大幅降低这项测试信息安全从业人员真实知识水平的，客观、准确、公平的认证考试的含金量和可靠度。有此类违规行为的 CISSP 人员，既违反了考试的保密协议，也违反了 CISSP 的职业道德，将吊销其证书。请不要尝试收集真题，保持其应有的考试难度，控制通过比例。

E.2 支持组织的道德准则

1.四类道德标准

①全球责任；②国家；③组织；④个人。

2.计算机道德协会(Computer Ethics Institute)

是一个非盈利组织，它以道德的方式帮助推进技术发展。制定了它自己的计算机道德 10 诫(Ten Commandments of Computer Ethics)：

(1)不得使用计算机伤害其他人。

(2)不得干预其他人的计算机工作。

(3)不得窥探其他人的计算机文件。

(4)不得使用计算机进行盗窃。

(5)不得使用计算机提交伪证。

(6)不得复制或使用尚未付款的专利软件。

(7)在未获授权或未提交适当赔偿的前提下，不得使用其他人的计算机资源。

(8)不得盗用其他人的知识成果。

(9)应该考虑你所编写的程序或正在设计的系统的社会后果。

(10)在使用计算机时，应考虑尊重人类。

3.互联网架构研究委员会(Internet Architecture Board, IAB)

IAB 是用于 Internet 设计、工程和管理的协调委员会。它负责对 Internet 工程任务组(Internet Engineering Task Force, IETF)的活动、Internet 标准流程(Internet Standards Process)的监督和上诉、注释请求(Request for Comment, RFC)的编辑进行架构监督。否则，Internet 将无法正常使用。

F.制定并实施文档化的安全策略、标准、程序和方针

以下描述的内容都是规范化的安全策略结构中的几大要素，搞清楚是什么：

1.安全策略(Security Policies)

规范化的最高层次被称为安全策略。安全策略是一个文档，包括：组织的安全需求、安全目标、安全原则、安全架构，定义所有相关的术语，定义角色、分配职责，指定审计要求等等。

安全策略是强制性的，包括特定问题的安全策略、特定系统的安全策略和综合的安全策略类，综合的安全策略有 3 种类型，包括：规章式的、建议式的和信息式的。

①**规章**式的策略（regulatory policy），主要涉及必须遵守的行业标准或法律规定；

②**建议**式的策略（advisory policy），解释了高层管理对内部安全和合性性的期望，包括可接受的行为和活动，并定义违背安全性的后果。大多数安全策略都是建议性的。

③**信息**式的策略（lnformative policy），提供了与相关的支持、研究或背景信息，用于提供特定的信息或知识，例如公司目标、任务声明或者组织如何与合作伙伴和客户进行交流。

根据内容策略分为 3 种类型：

①组织性策略（Organizational or program policy）：此类策略由高级管理层发布，该策略描述并委派信息安全责任，定义实现 CIA 的目标，强调需要特别关注的信息安全问题（例如保护信用卡公司或健康保险公司的机密信息，或者高可用性系统）。通常情况下，此类策略的范围是整个组织。

②功能型策略/特定问题策略（issue-specific policy）：针对特定安全领域或关注点，例如访问控制、持续性计划、职责分离等，或者针对特定的技术领域，例如使用互联网、电子邮件、无线访问、远程访问等。此类策略依赖于业务需要和可接受的风险水平。内容包括：对特定问题的阐述，组织针对该问题的态度，适用范围，符合性要求，惩戒措施等。

③特定系统策略（System-specific policy）：针对特定的技术或操作领域制定的更细节化的策略，比如特定应用或平台。

2. 策略链

策略是层次性的，下面是至上到下的策略链：

方针(最高策略)=>标准(技术方法)=>基线(最低标准)=>指南(运用标准)=>程序(操作实现)

它们的关系：安全策略是有组织的安全文档的总体结构的基础；然后，标准基于策略并受规章制度的管辖；指南从其中衍生而来；最后，程序基于前面三个基本要素。

①策略/方针 Policy：处于策略链的最高层次，它是由组织的高级管理层发布的、关于信息安全最一般性的声明。方针应该代表着高级管理层对信息安全承担责任的一种承诺，一旦发布，要求组织成员必须遵守。策略/方针的实施要依靠标准、指南和程序。

②标准 Standard： 标准规定了在组织范围内强制执行的对特定技术和方法的使用。标准起着驱动方针的作用，标准可以用来建立方针执行的强制机制。

③基线 Baseline： 基线建立的是满足方针要求的最低级别的安全需要。在建立信息安全整体框架之前，基线是需要考虑的最低标准。标准的开发通常都是以基线为基础的，基线可以看作是抽象的简单化的标准。大多数基线都是很具体的，或者与系统相关，或陈述某种配置。基准往往指的是行业或政府标准，例如可信任计算机系统评估标准(TCSEC)或信息技术安全评估和标准(ITSEC)或者 NIST(美国国家标准技术研究院)标准。

④指南 Guideline： 类似于标准，也是关于加强系统安全的方法，但它是建议性的。指南比标准更灵活，考虑到了不同信息系统的特点。指南也可用来规定标准的的开发方式，或者保证对一般性安全原则的遵守。作为安全专家和用户的操作指南，提供了如何实现标准和基准的建议。指南说明了应当部署哪些安全机制，概述了一套方法(包括行动建议)，但并非强制性的。彩虹系列、通用准则 CC、BS7799 等，都可以看作是此类。

⑤安全程序/过程/措施/实施 Procedure： 是执行特定任务的详细步骤。位于策略链的最低层次，是实现方针、标准和指南的详细步骤。安全程序是详细的、按部就班的指导文档，它描述了实现特定安全机制、控制或解决方案所需的确切行动。

G. 理解业务连续性要求

本章必考

1. 业务连续性计划（BCP）和灾难恢复计划（DRP）之间的差异。

①BCP 是预防性的、全面、持续的，必须被首先应用（实施），并持续的应用。

②DRP 是补救性的、应急、临时的，当 BCP 失败了(leaves off)，就会启动 DRP(picks up)。

灾难恢复 DRP 的目的是，尽量减少灾难或中断所带来的影响，尽可能快的恢复正常的业务活动。DRP 只在灾难发生后才实施。灾难恢复处理“我的天哪，天要塌了”，而连续性规划处理“好了，天塌下来了。现在，我们该如何继续经营?

虽然文字上都写的是“计划-PLAN”，但实际上它不只是一系列的文档方案，还包括了相关的应对工作、实施过程和实践操作。

考试中的灾难恢复 DR，是指对技术环境的恢复，是以信息技术为核心的，也就是信息系统的恢复，而不是对整个组织管理、业务运行、物理环境、生产能力的恢复。

业务连续性管理（BCM），是整体的管理过程，包含 DRP 和 BCP，提供一个框架，实施管理，形成能力。BCM 的主要目的是允许该组织继续在不同条件下进行业务操作。

2.业务连续性计划（BCP）的步骤

ISC² 定义的创建业务连续性计划的过程包括以下四个主要步骤：

①编制计划；②评估业务影响；③连续性计划；④批准和实现。

在第七域的 N 章节，详述了 NIST 800-34 规范的业务连续性管理的流程，和上面的不一样。

考题里问 BCP 的第一个步骤，一般选业务影响分析 BIA（包括分析关键业务、调研各个部门），而不是计划。

G.1 制定并记录项目范围和计划

业务连续性计划 BCP 的步骤流程就是下面的 1、2、3、4 步，其中的“企业组织架构分析”要做 2 次！BCP 第一步：先一个人来做企业组织架构分析；然后他牵头组建 BCP 团队；接着 BCP 团队再做一次企业组织架构分析，来修订和验证之前他做的分析；之后才获取资源干正事了。

1.先分析企业组织架构（业务组织分析）Business organization analysis

分析组织架构是重要的基础工作，为确定 BCP 团队成员提供了根据，通常由 BCP 先头部队来完成。需要考虑的关键部门有：核心业务运营部门、支撑保障部门（IT、维修等）、高管人员等。

2.再选择 BCP 团队 BCP team selection

团队要包括各种各样的关键人物，团队领导一定要是企业的高管之一，才好有效落实。

2.5 再做一次全面的企业组织架构分析。

3.再获得相关资源 resource consumed

不同阶段要有不同的资源来支撑保障 BCP 有效实施。

①BCP 开发：前面提到的四个步骤(项目范围和计划编制、业务影响评估、连续性计划、批准和实现)，最需要的资源就是人力，也就是抽组人员、集中办公、拟制计划。

②BCP 测试、培训和维护：这时候要有基础环境的保障，也就是软、硬件设施。当然，人力总是不可缺少的。

③BCP 实现：当灾难和意外发生时，更就需要大量的资源来执行 BCP，反正什么都要。

4.还要考虑法律、法规要求（合规）Legal and regulatory assessment

在业务连续性计划实施过程中，聘请法律顾问是非常重要的。

5.安全管理计划小组应该开发三类计划：

①战略计划（strategic plan）是长期计划（例如 5 年），相对稳定，定义了组织的目标和使命。

②战术计划（tactical plan）是中期计划（例如 1 年），是对实现战略计划中既定目标的任务和进度的细节描述，例如维护计划、系统开发计划、变更管理、技术革新、容灾备份等。

③操作计划（operational plan）是短期的高度细化的计划，须经常更新（每月或每季度），例如培训计划、系统部署计划、产品设计计划等。

G.2 开展业务影响分析

BCP 团队完成了准备创建业务连续性计划的四个阶段，就会进入工作的核心部分：**业务影响分析/评估(BIA)**。BIA 先确定决定组织持续发展的资源，再分析资源的潜在威胁，再评估每种威胁的可能性和对业务的影响。BIA 的定量分析、定性分析在第一域 I.2 章节里讲过了。（相关内容在第六域 C.6 章节和第七域 N 章节里面也有涉及）。

BIA 的标准流程是 4 步：

①收集信息。Gathering information。识别和列举组织的所有业务。

②评估脆弱性。Performing a vulnerability assessment。

③分析业务影响。Analyzing the information。

④拟制并呈报分析报告。Documenting the results and presenting the recommendations。

1.确定业务优先级

BIA 的第一个任务是确定业务优先级，就是当灾难发生时，哪个业务最重要，最先被恢复。

这里涉及几个常用概念：

①最大允许中断时间（MTD）Maximum Tolerable Degradation，也称为最大容忍中断时间（MTO），指的是某个业务功能出现故障但是不会对业务产生无法弥补的损害所允许的最大时间长度（底线）。

②恢复时间目标（RTO）recovery time objective，就是当中断事件发生时，实际恢复功能的时间期望。

BCP 过程的目标是确保你的 RTOs 小于 MTDs。

很明显，MTD 最短的业务，其优先级就越高！

2.识别风险

识别风险是一个纯粹的定性分析的过程，就是列出可能的各种风险。自然或人为的风险。

3.业务影响评估

这里要考虑到所谓的云服务的可靠性，当企业的某个服务外包给第三方公司时，它的中断风险一定要考虑到。

4.可能性评估

就是要算出年发生比率(ARO)。

5.影响评估

这里要定义暴露因子 EF，计算单损 SLE，计算年损 ALE。当然，也可以用定性的方法，只评级，不量化计算。

6.资源优先级划分 Resource prioritization

BIA 的最后一个步骤，因是针对各种不同风险，确定分配业务连续性资源的优先级。如果生成了一个所有风险的列表，那么年损最大的风险优先级就最高。

前面只是做了影响分析，下面要开始写 BCP 计划了

7.策略开发 strategy development

BCP 团队现在根据风险优先级列表，确定采取什么应对措施（减轻、转移、接受和拒绝）。这是衔接业务影响分析 BIA 和业务连续计划拟制工作的环节！这个策略的主要内容包括:范围、任务说明、原则、指南和标准。

8. 预备和处理 Provisions and processes

有了 BCP 策略，就要研究怎么保护人、建筑物与设备、基础设施等，采取什么措施缓解（mitigate）不可按受的风险。这里就要研究实际的风险消减机制、方法、手段了。

9. 计划批准

一旦 BCP 团队完成了 BCP 文档的设计，那么就该呈上审批了。高层的决策是最关键的。

10. 计划实现

计划被批准了，就要落实了，包括资源分配、计划维护什么的。

11. 培训和教育

培训和教育是落实 BCP 计划的一项重要内容，确保人员在灾难发生时能够有效地完成其任务，人员还要有所冗余。

12. BCP 文档化

成体系的，持续的修订、完善和保存 BCP 文档，确保该项工作有序开展。

现在算是完成业务连续性的计划的研究拟制和预备实施工作了，有些具体的执行和维护工作在第七域的灾难恢复里讲。

H. 促进人员安全策略

雇用新的职员涉及几个明确的步骤：①创建工作描述、②设置工作分类、③筛选候选人、④雇用和培训最适合这项工作的人。

1. 员工管理方面的重要元素包括责任分离、工作职责和岗位轮换

①职责分离（Separation of Duties）

职责分离属于安全概念，是指把关键的、重要的和敏感的工作任务分配给若干不同的管理员或高级执行者，是将最小权限原则应用到管理员身上。这样做能避免一个人能够独自干成一件坏事，也能防止共谋 collusion。共谋指的是几个人的团伙一起干成一件坏事。

②工作职责（Job Responsibilities）

工作职责是要求员工在常规的基础上执行特定工作任务。这个概念主要用来确定员工的最小访问权限。

③岗位轮换（Job Rotation）

让员工在不同的工作岗位中轮换职位，从而提高整体的安全性。岗位轮换有两种功能：一是提供知识和人员的冗余，缺谁都照样运转；二是提供了一种同级审计形式，减少伪造、篡改、偷窃、破坏和信息滥用的风险，也能够防止共谋。

④交叉训练（Cross-training）

是工作轮换的另一种形式，员工不换岗位，只是跟班学习或者临时顶替一下，是一种应急预案。

上面的①、②、③都是经常考的。

H.1 求职人员甄选 （例如：证明人核实、教育背景查证）

要确保任职人员的安全性，必须做背景调查和安全检查。

背景调查

背景调查包括：获得候选人的工作和教育历史记录，检查证明材料，与候选人的同事、邻居和朋友进行面谈，向警察局和政府机关调查候选人的拘捕或违法活动记录，通过指纹、驾驶执照和出生证明来认证身份，还要进行面试。如有必要，也可以采用测谎仪、药检、性格测试/评估等形式。很多公司还要对申请人进行在线背景调查和社交网络账号复审。

重要的安全岗位对人的道德素养要求很高，所以别用自己的身份证去乱开房，还有手机号、银行账户都会被查的。

H.2 雇佣协议与政策

新员工入职，要签署雇佣协议和保密协议。

1. 雇佣协议

协议文档说明了组织的规则和限制、安全策略、可接受的使用和行为准则、详细的工作描述、破坏活动及其后果、要求员工胜任工作所需的时间。

2. 保密协议（NDA）

NDA 用来保护组织的机密信息不会被的员工泄漏。

3. 竞业禁止协议（NCA）

NCA 通常与 NDA 同时存在。NCA（竞业禁止协议）防止了解公司核心秘密的员工进入另一个存在竞争关系的组织机构，也能防止员工因为高薪而跳槽到另外的公司。通常，NCA 具有时间限制，例如半年、一年甚至三年。

强制执行 NCA 是有一定困难的，法律上认可员工为了保障自己和家庭的生活，允许使用所具备的技能和知识谋取工作，NCA 不能妨碍员工获得适当的收入。但是它的威慑作用和保密作用还是明显的。

4. 强制休假

强制员工休假，可以提供与岗位轮换类似的好处。代班的人员可以审计发现他的过失。

H.3 劳动合同解除流程

解雇 1 个员工时，应该：

①采取不公开的和尊重人的方式。

②终止合同时应该至少有一位证人在场，证人最好是高层经理或保安人员。

③一旦员工被告知离职，应该被立刻护送离开，并且不允许通过任何理由返回办公地点。

④在员工被解雇离开之前，所有组织特有的身份证件、访问权限或员工安全标志以及门卡、钥匙和出入证都应该被收回。还必须在通知员工被解雇的同时或之前，就禁止或删除此员工对系统的访问权限。

解雇员工的最佳时间是员工轮班结束的时候。一方面，留给时间去寻找新的就业机会；另一方面，换班时解雇更加自然，可以减少压力。解雇员工时，根据员工的心理状态，视情进行一次离职面谈，目的是：根据之前签署的雇用协议和保密协议来审查其责任和约束条件。

H.4 供应商、顾问与承包商的控制

在使用任何类型的第三方服务提供商时，服务级别协议(SLA)尤为重要。

H.5 合规

详见 C 章节。

H.6 隐私

隐私性的定义多种多样，大概意思就是：

①防止对个人重要信息的未授权访问。

②防止未被同意或知晓情况下，检查、监控其行为。

个人身份信息（PII）personally identifiable information

PII 是可以追溯到源头的人的任何数据项。如：一个电话号码、电子邮件地址、邮寄地址、社会保障号、名字、信用卡账号、银行账号等；没有代表性的个人信息不是 PII，如：一个 MAC 地址、IP 地址、操作系统类型、最喜欢的度假地点、高中吉祥物的名字等等。

I.理解与应用风险管理的概念

理解风险管理的概念是 CISSP 考试的重点（必考）。

风险管理的主要目的是要将风险降低到一个可以接受的级别。达到风险管理主要目标的过程被称为风险分析（risk analysis）。风险评估（Risk Assessment）是对信息资产及其价值、面临的威胁、存在的弱点，以及三者综合作用而带来风险的大小或水平的评估。

信息风险管理 IRM (lnfonnation Risk Management)是识别并评估风险、将风险降低至可接受级别、执行适当机制来维护这种级别的过程。

风险分析提供了一种成本/收益比(costl-benefit comparison)，也就是用来保护公司免受威胁的防护措施的费用与预料中的损失所需要付出的代价之间的比值。在大多数情况下，如果损失的代价没有超过防护措施本身的费用，那么就不应该实行该防护措施。风险分析有下列 4 个主要目标：

①标识资产和它们对于组织机构的价值。

②识别脆弱性和威胁。

③量化潜在威胁的可能性及其对业务的影响。

④在威胁的影响和对策的成本之间达到预算的平衡。

1.重要术语

我们常常使用术语“脆弱性”、“威胁”、“风险”和“暴露”来表示同样的事情，然而，它们实际上有不同的含义，相互之间也有不同的关系。理解每一个术语的定义是非常重要的，但更重要的是应当理解它们彼此之间的关系。

①资产（Asset）

资产是指环境中应该加以保护的任何事物。如：计算机文件、网络服务、系统资源、进程、程序、产品、IT 基础架构、数据库、硬件设备、家具、产品秘方/配方、人员、软件和设施等。。

②资产估值（Asset Valuation）AV

就是资产具备的货币价值。包括开发、维护、管理、宣传、支持、维修和替换资产的所有

成本，还包括公众信心、行业支持、生产率增加、知识资产以及所有者权益等无形价值。

③弱点/脆弱性（Vulnerability）

一个资产的弱点（缺少安全措施）、缺陷（安全方面的问题）或者漏洞被称为脆弱性。一旦被利用，就会对资产造成损害。如果没被利用，当然也就没事了。

③威胁（Threats）

前面讲了脆弱性，那么一个弱点有多个大可能会被利用，并产生破坏呢？

威胁就是利用脆弱性的行为，它会带来危险：即某人或某个软件识别出特定的脆弱性，并利用其来危害公司或个人。任何可能发生的、造成资产价值损失的事情都被称为威胁。威胁主体通常是人，不过也可能是程序、硬件或系统。威胁事件包括火灾、地震、水灾、系统故障和人为错误(一般是因为缺少培训或无知)和断电等等。

⑤风险（Risk）

脆弱性、威胁都是客观可能存在的东西或者事件，而风险就是一个量化的指标（百分比或者经济损失的价值），代表了是某种威胁事件利用了脆弱性，并导致资产损害的可能性。它是 1 个概率性的评估。可能性越大，风险就越大，损失就越大。

风险=（威胁+脆弱性）×100%=潜在影响

会考到风险相关的三要素：威胁、脆弱性和消减措施。

⑥暴露（Exposure）

显示脆弱性，把组织暴露在威胁之下。暴露就是存在可利用的脆弱性。暴露并不是指威胁事件实际发生了，而是存在漏洞被利用的潜在可能性，或者是资产被迫害的可能性。也就是说，没暴露前，没人知道系统有脆弱性、威胁和风险，一切都是安全的；只有真实暴露了，才会发生实际的安全事件，一切才变得不安全。

⑦防护措施（Safeguards）

防护措施就是安防对策，是指能消除脆弱性或应对一种或多种特定威胁的任何方法，包括技术的、物理的、管理的。当然，一切的目的是为了消减风险（mitigate risk），包括控制(control)、对策（countmeasure）和防护措施（safeguard）。

⑧攻击（Attack）

攻击是 1 个威胁主体利用脆弱性的行为，前面几个概念都是纸上谈兵，只有攻击发生了，才产生实际的、真正的破坏性影响。搞攻击就是搞破坏，搞破坏就是

⑨破坏（Breach）

破坏就是破解了或者绕过了安防系统，也就是实现了非法进入。搞成了破坏，就能搞攻击了。当破坏与攻击结合时，就会发生渗透事件或入侵事件。

⑩残留风险（Residual Risk）

在实施安全措施之后仍然存在的风险。

最后用一个图来描述关系：

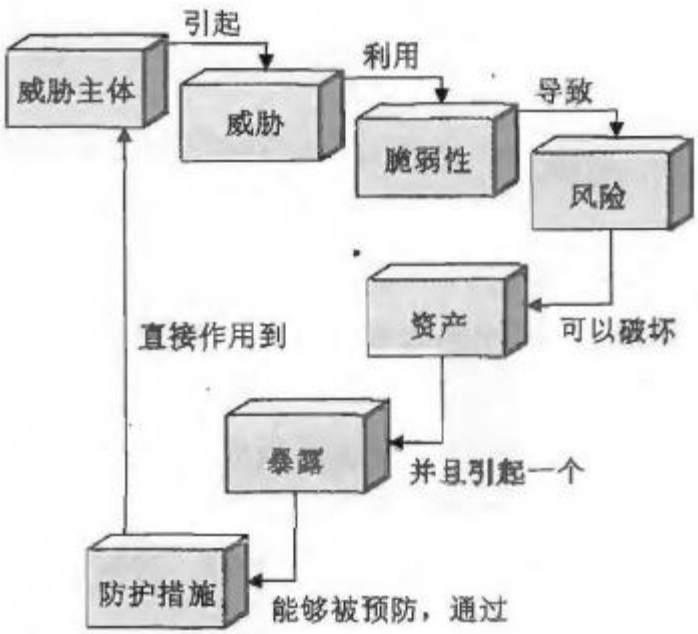


图 2-2 各种安全组件之间的关系

表 2-5 威胁和脆弱性之间的关系

威 胁 主 体	可能利用的脆弱性	导致的风险
恶意软件	缺少防病毒软件	病毒感染
黑客	服务器上运行的功能强大的服务	对机密信息的未授权访问
用户	操作系统中配置错误的参数	系统故障
火灾	缺少灭火器材	设施和计算机受到破坏，可能付出生命代价
雇员	缺少训练或实施标准 缺少审计	共享至关重要的信息 在数据处理应用程序中更改输入和输出
承包商	松懈的访问控制机制	窃取商业秘密
攻击者	编写较差的应用程序 缺少严格的防火墙设置	造成缓冲区溢出 进行拒绝服务攻击
入侵者	缺少保安	打破窗户，盗窃计算机和设备

2. 美国 NIST 的风险评估过程

NIST 开发了一套风险方法，出版在 SP 800-30 文档中。这套 NIST 方法叫做信息技术体系风险管理指南(Risk Management Guide for Information Technology System)，被认为是美国联邦政府标准。

①准备评估。

目标是搞清背景。

*确定评估的目的，*确定评估范围，*识别与评估有关的假定与约束，*识别评估的输入，*识别评估期间使用的风险模型和分析方法。

②进行评估。

目标是生成信息安全风险列表，从而根据风险水平区分优先级，并通知风险响应决策。

*识别与组织相关的威胁源，识别这些源可能产生的威胁事件，

*识别组织内可被威胁源利用的脆弱性，

*确定威胁源会引发的特定威胁事件的可能性，以及威胁事件成功的可能性，

*确定威胁事件产生的负面影响

*确定威胁负面影响的信息安全风险。

③沟通评估结果和分享风险的相关信息。

目的是确保决策者了解掌握风险相关的信息，指导风险决策沟通，共享信息。

*沟通风险评估结果，*在风险评估的执行阶段共享相关信息，支持其他的风险管理活动

④维护评估。

目的是跟踪掌握风险变化情况。

*监控风险评估中识别的风险因素，掌握后续变化，*更新风险评估报告。

3. ISO/IEC 27005

一个国际标准，规定在 ISMS 框架内如何进行风险管理。

I.1 识别威胁与脆弱性

对 IT 的威胁并不只限制在 IT 源，也有自然灾害、人和管理的因素。脆弱性评估需要一个技术团队，也需要非专业的人员来提高全面性。

通过常使用微软的 STRIDE 威胁分类方案（6 个首字母）。即：

①电子欺骗(Spoofing)——通过使用伪造身份获得对目标系统访问权限的攻击行为。可使用 IP 地址、MAC 地址、用户名、系统名称、无线网络名称、电子邮件地址以及许多其它类型的逻辑标识来欺骗。

②篡改(Tampering)——任何对数据进行未授权的更改或操纵的行为，包括在传输中的和被存储的数据。这种攻击主要侵害完整性和可用性。

③否认(Repudiation)——用户或攻击者否认执行了一个动作或行为的能力。也就是抵赖、不承认有过非法行为。

④信息披露(Information disclosure)——将私人、机密或受控信息揭露、传播给外部或未授权实体的行为。

⑤拒绝服务(DOS)——指攻击试图阻止对资源的授权使用。这可以通过缺陷开发、连接重载或流量泛滥实现。DOS 攻击并不一定会导致对一个资源的完全中断；而是会减少吞吐量或造成延迟，以阻碍对资源的有效利用。

⑥权限提升(Elevation of privilege)——此攻击是指有限的用户帐号被转换成一个拥有更大特权、权力和访问权的帐户。

一骗二改三抵赖；窃密瘫痪提权限。

I.2 风险评估/分析 （定性分析、定量分析、混合分析）

要搞清 2 种风险分析的区别：

①项目风险分析 project risk analysis：团队针对项目实施的分析，为了避免项目失败。

②安全风险分析 security risk analysis：仅针对某个信息系统的分析，为了找其漏洞。

1. 风险评估的任务包括：

①识别构成风险的各种因素；

②评估风险发生的可能性和造成的影响，并最终评价风险水平或大小；

③确定组织承受风险的能力；

④确定风险消减和控制的策略、目标和优先顺序；

⑤推荐风险消减对策以供实施。

2.风险评估的内容：

①资产面临的威胁。Threats to its assets

②当前环境中存在的脆弱性。Vulnerabilities present in the environment

③威胁真实发生的概率（定量评估的频次）。The likelihood that a threat will be realized by taking advantage of an exposure (probability and frequency when dealing with quantitative assessment)

④威胁发生带来的影响。The impact that the exposure being realized will have on the organization

⑤消减措施。Countermeasures available that can reduce the threat’s ability to exploit the exposure or that can lessen the impact to the organization when a threat is able to exploit a vulnerability

⑥剩余风险。The residual risk (e.g., the amount of risk that is left over when appropriate controls are properly applied to lessen or remove the vulnerability)

3.定量风险分析/必考

要计算出具体的概率百分比，用货币形式表示每个资产和威胁。虽然，纯粹的、精准的定量分析是不可能的，但还是能用的。下面是定量风险分析的六个主要步骤或阶段，都不难理解：

①列出资产清单并分配资产价值，即 AV（asset value）；

②研究生成每个资产所有可能威胁的列表。为每个威胁计算暴露因子 EF（exposure factor）和单一损失期望 SLE（single loss expectancy），就是单损。

EF 也称为潜在损失，是该风险实际发生时，可能损失的资产价值的百分比。

SLE 就是该风险实际发生 1 次时，可能损失的资产价值，也就是损失多少钱。

SLE=AV×EF

③计算每种风险的年发生概率 ARO（annualized rate of occurrence）。

ARO 就是该风险每年可能发生几次，值从 0 到无穷大，越大越危险。如果风险每年发生很多次，它带来的损失可以远远超出相关资产的价值。

④计算每个风险的年度损失期望 ALE（annualized loss expectancy），就得到每个威胁可能的总损失。

ALE=SLE×ARO

⑤研究每个威胁的对策，然后基于对策，计算采取措施后的 ARO 和 ALE。

不管有没有采取措施，EF 是不变的，也就是不管攻击搞没搞成，反正只要搞成了，你就会损失这么多。安防措施的目的应是减少 ARO，就不让风险实际发生。

⑥针对每个资产的每个威胁的每个对策执行成本/效益分析。选择对最适用的对策。

这里要先计算每个威胁采取某种防护措施的年度成本 ACS（annual cost of safeguard），

部署安防系统的价值就是：施策前的 ALE—施策后的 ALE—ACS，可以让高层看到安防系统实现了多大的效益。SLE 和 ALE 的区别要搞清楚，经常考。

当然，除了算清楚钱，也要考虑法律因素、社会效益等，要采取“应尽关注”的态度，有些安防开支可以适度增加，不能只管赚钱。

4. 定性的风险分析

不算钱，只是评估其风险、成本和影响，可以使用很多统筹学里用到的技术，如头脑风暴、得尔非（Delphi）、问卷调查、各种开会等。

①场景（Scenarios）

就是用一页纸讲清楚 1 个风险案例，用高、中、低或者 A、B、C 什么的表示影响程度。

②Delphi 技术

学过统筹学就知道，Delphi 技术就是一个简单的匿名反馈和响应过程。参与者通常被集中在一间会议室中，对每项意见或问题匿名反馈自己的想法；然后组织者修改完善这个报告或方案，再进行匿名反馈；最后所有参与者都答成一致，没有意见了。

③风险评估矩阵

横轴是风险影响，一般分 5 级；纵轴是风险发生的可能性，一般分 5 级。然后就得到了每个风险的评级。

5. 其它

风险评估的方法论（模型）有：

①FRAP(Facilitated Risk Analysis Process)：专用的定量方法，先进行预筛选以节省时间和金钱。

②OCTAVE(Operationally Critical Tbreat, Asset and Vulnerability Evaluation)：面向团队的方法，通过组织研讨会来评估组织风险和 IT 风险。

③AS/NZS 4360：澳大利亚和新西兰的一种业务风险管理评估方法。

④FMEA(Failure Modes and Effect Analysis)，失效模式和影响分析：利用组件的基本功能来识别缺陷及其影响的一种方法。

⑤**故障树分析**：分析具体缺陷在复杂系统中出现的根本原因的一种方法。

⑥CRAMM 中央计算和电信机构风险分析管理方法：Central Computing and Telecommunications Agency Risk Analysis and Management Method。

I.3 风险分配/接受 （例如：系统授权）

1. 风险分析的结果有：

①所有资产的完整和详细的评估。

②所有威胁、风险、发生概率和一旦发生的损失的详细列表。

③针对特定威胁的防护措施和对策列表，并且标识出其有效性与 ALE（年损）。

④每种防护措施的成本/效益分析。

2. 对风险的应对策略有四种：

①降低风险（Reduce or mitigate），就是风险**消减**，采取最佳性价比的安防措施。

②转移风险（Assign or transfer），就是买**保险**或外包，自己不干有风险的事。

③接受风险（Accept），组织机构**书面**说明对某风险不采取任何措施，比如容忍地震。

④拒绝风险（Reject or ignore），最消极的态度，就当风险不存在，无视，**不管**它。

3. 剩余风险

实施并实现了安防措施，仍然继续存在的风险被称为剩余风险，也是高层管理部门选择接受的风险。这也表明通过成本/效益分析，发现某些防护措施并不划算。

首先算个总风险：就是在没有任务防护措施的情况下，组织将要面对的风险数量，与威胁、脆弱性和资产价值有关。

然后算个控制间隙(controls gap)：就是通过采取防护措施被减少的风险数量。总风险和剩余风险之间的差值被称为控制间隙。代表了安防系统的效益，也就是可控制风险。

总风险-控制间隙(可控风险)=剩余风险。

I.4 风险应对策略选择

选择风险应对措施的原则主要有以下几个：

①措施的成本要小于资产价值。为办公室修个地下防空洞肯定是没必要的。

②措施的成本要小于措施的效益。雇用 1 个中南海保镖做公司门卫也是没必要的。

③措施的结果应当使攻击成本大于攻击获得的效益。压缩包加密就行了，要十年才能破解。

其它的原则就不列举了，自己看着办。

I.5 实施

就三类应对措施：

1. 技术

包括：用户名、密码、智能卡和生物识别、加密、受限接口、访问控制列表、协议、防火墙、路由器、入侵检测系统（IDS）以及阈值级别。

2. 管理

主要关注人员与业务，包括：策略、过程、雇用准则、背景调查、数据分类和标签、安全意识和培训效果、休假记录、报告和回顾、工作监督、人员控制以及测试。

3. 物理

防止最直接访问和接触，包括：保安、围墙、移动探测器、闭锁的门、密封窗、灯光、线缆保护、笔记本电脑锁、磁条卡、看门狗、摄像机、陷阱以及报警器。

I.6 控制措施的类型 （预防措施、 检测措施、 纠正措施等）

1. 访问控制的 7 个主要类型/安全控制功能种类：

①管理（Directive）/指引：指令性、强制性的规定，如：安全策略需求或标准、张贴通告、疏散路线出口标志、监控、监督、工作任务过程。

②威慑（Deterrent）：旨在打击潜在的攻击者。吓唬人别搞坏事，如：策略、安全意识培训、锁、围墙、安全标识、保安、陷阱、安全摄像机。

③预防（Preventive）：旨在避免发生事件。阻止非法进入，如：围墙、锁、生物测定学、陷阱、灯光、警报系统、责任分离、工作轮换、数据分类、渗透测试、访问控制方法、加密、审计、使用安全摄像机或闭路电视(CCTV) 、智能卡、回叫、安全策略、安全意识培训、反病毒软件、防火墙和入侵防御系统。

④补偿（Compensating）：提供可替代控制措施。增加访问控制措施，如：对 PII（个人信息）加密。

⑤检测（Detective）/监测：确认事件的活动和潜在的入侵者。发现非法进入，如：保安、移动探测器、记录和检查安全摄像机或闭路电视捕获的事件(CCTV) 、工作轮换、强制休假、审计跟踪、蜜罐或蜜网、IDS、违规报告、对用户的监管和检查、事故调查。

⑥纠正（Corrective）/矫正：事件发生后，修复部件或系统。发生非法访问后，将系统还原至正常的状态，如：终止恶意行为或重启系统、删除或隔离病毒。

⑦恢复（Recovery）：目的是使环境恢复正常运作。比纠正性控制更高级、更复杂，如：备份和还原、容错驱动系统、系统镜像、服务器群集、反病毒软件以及虚拟机影像。

很多安全措施是同时符合以上多种类型的，如果问 CCTV 是预防、还是威慑、还是检测？就要看题目中的场景了，它发挥的实际作用是什么就选最佳答案。

I.7 控制措施评估

看看第六域就行了。

I.8 风险监控与测量

安全控制措施必须是可以监测和度量的，否则并提供任何安全性。也就是安防系统的功能有效性和好处要能被看到。

I.9 资产评估

没什么要考的内容。

I.10 汇报

一个风险报告应该是准确、及时、全面的，能为整个组织提供清晰和准确的决策支持，并且定期的更新。例如，美国政府机构被要求在发现个人信息泄露的 1 小时内，向美国计算机应急小组(US-CERT)汇报。

I.11 持续改进

持续改进广泛使用的工具是四步质量模型，PDCA（计划——执行—评估—行动），也称为戴明环或休哈特环，这个在各种领域用的太多了：

①计划：识别时机并计划改变

②执行：小范围内实施改变

③检查：用数据分析改变的结果，确定是否有差别

④行动：如果改变是成功的，在更大范围内实施它和持续评估结果；如果这个改变无效，再次开始循环。

其他广泛使用的持续改进方法有：六西格玛，Lean 等。

I.12 风险框架

风险框架是关于如何评估风险、解决风险和监管风险的指导或方法。CISSP 考试主要考美国国家标准技术研究所(NIST) 在 800-37 专业出版中的定义。其它的企业风险管理（ERM）框架有：

1. COSO：2013

2. ISO 27005：2008
3. AS/NZS and 31000：2009
4. ISO Guide 73：2009
5. NIST Special Publications 800-37 and 800-39
6. ISACA (2009) Risk IT Framework

详细看第 9 域。

J. 理解与运用威胁建模

威胁建模是指潜在威胁被识别、分类和分析的安全流程。它通过寻找系统潜在的威胁以建立对抗的策略和安全的系统，使您可以对最可能影响系统的威胁进行识别和评价。

①威胁建模的**主动式方法**发生于系统开发的早期阶段，也被称为防御方法。事先集成安全解决方案更符合成本效益，比后面硬塞的方案更成功。但是，并不是所有的威胁都可以在设计阶段预测出来，所以仍然需要被动式威胁建模来解决不可预见的问题。

②威胁建模的**被动式方法**发生在产品被创建和部署之后，也被称为对抗的方法。通常需要在部署后精心制作产品的更新或补丁，有可能会牺牲一些功能性和用户友好性。

J.1 识别威胁 （例如：竞争对手、承包商、员工和可信合作伙伴）

1. 识别威胁的结构化方法主要有：

①关注资产

对资产进行估值，并试图识别对于宝贵资产的威胁。

②关注攻击

假设有潜在的攻击者，并基于攻击者的目标识别他们所代表的威胁。

③关注软件

主要考虑企业内部各种软件系统的潜在威胁。

2. 对威胁进行分类

通过常使用微软的 STRIDE 威胁分类方案（6 个首字母）。即：

①电子欺骗（Spoofing）——通过使用伪造身份获得对目标系统访问权限的攻击行为。可使用 IP 地址、MAC 地址、用户名、系统名称、无线网络名称、电子邮件地址以及许多其它类型的逻辑标识来欺骗。

②篡改（ Tampering ）——任何对数据进行未授权的更改或操纵的行为，包括在传输中的和被存储的数据。这种攻击主要侵害完整性和可用性。

③否认（ Repudiation ）——用户或攻击者否认执行了一个动作或行为的能力。也就是抵赖、不承认有过非法行为。

④信息披露（ Information disclosure ）——将私人、机密或受控信息揭露、传播给外部或未授权实体的行为。

⑤拒绝服务(DOS) ——指攻击试图阻止对资源的授权使用。这可以通过缺陷开发、连接重载或流量泛滥实现。DOS 攻击并不一定会导致对一个资源的完全中断；而是会减少吞吐量或造成延迟，以阻碍对资源的有效利用。

⑥权限提升(Elevation of privilege) ——此攻击是指有限的用户帐号被转换成一个拥有更大特权、权力和访问权的帐户。

一骗二改三抵赖；窃密瘫痪提权限。

3.威胁的优化级排序

对威胁进行排序或定级，可以利用 3 种技术来完成：

①概率×潜在

使用一个代表风险严重程序的编号，编号值从 1 到 100，100 是最严重的；概率和损失的值从 1 到 10 。

②高/中/低

很简单，每个威胁都被标注为三种优先级标签中的一种。高优先级的需要立即解决。

③DREAD 评级系统

对每种威胁问五个问题，根据回答情况来评级：

1. 潜在破坏——如果威胁成真，可能造成的损失有多严重?
2. 再现性——攻击者重复利用这一漏洞有多复杂?
3. 可利用性——实施攻击有多难?
4. 受影响用户——多少用户可能受到攻击影响？(百分比)
5. 可发现性——攻击者发现该弱点有多难?

每个问题通过 H/M/L 或 3/2/1 的值来回答，从而建立一个详细的威胁优先级表。

J.2 确定和图解潜在攻击（例如：社会工程学攻击、电子欺骗攻击）

进行威胁建模，确定可能发生的潜在攻击，通常通过创建图表来完成，包括元素、数据流指向和特权边界等要素。

J.3 执行风险降低分析

执行风险降低分析，字面上写的是降低，其实是指对程序、系统或环境的细化、分解和分析，就是对风险的详细分析。目的是为了更好地理解产品内部逻辑和与外部的交互关系，并理解输入、处理、安全性、数据管理、存储和输出等详细过程。系统分解的越合理、越细致，就越容易识别威胁。在这个分解流程中，你必须了解五个关键概念：

信任边界——信任或安全等级发生改变的位置

数据流路径——数据在两个位置之间的流动

输入点——接收外部输入的位置

特权操作——比普通用户或流程有更大特权的任何活动，如修改系统参数等

安全立场和方法细节——安全策略、安全基础和安全假设的声明

J.4 风险补救技术和流程（例如：软件架构和运营）

没什么要考的内容。

K 整合安全风险考量至采购策略与实践中

采购流程

采购解决方案通常包括：征求建议书（Request for Proposal, RFP)，RFP 用来针对业务

问题或需求让供应商提供解决方案的，它为采购决策提供了框架，并能让解决方案的风险和收益在前期明确定义。RFP 要传达必要的安全需求，并要求得到有意义的和具体的答复，其中包括供应商将如何满足这些要求。

K.1 硬件、软件和服务

没什么要考的内容。

K.2 第三方评估和监控 （例如： 现场评估、文档交换与审查、过程/策略评审）

很容易。

K.3 最低安全要求

没什么要考的内容。

K.4 服务级别要求

1.服务水平要求(SLR)

服务水平要求的文档包含客户对服务的要求，并演变成安全水平协定草案。它定义了：

①详细的服务水平目标

②共有的责任

③其他的需求尤指一组客户

2.服务水平协定(SLA)

SLA 是一个 IT 服务提供者和客户之间的协定，可以包括多个服务或多个客户。它：

①描述 IT 服务

②描述服务水平目标

③明确说明 IT 服务提供者和客户的责任

3.服务水平报告

服务水平报告是对提供商交付约定的服务质量的能力进行调查并报告。

4.服务水平协议(SLA) VS 保证

SLA 定义供应商和客户间约定的性能级别和赔偿或处罚。然而，有 SLA 并不意味着供应商总能遵守 SLA。

保证只能通过检查、评审、和评估来获得。

L.建立并管理信息安全教育、安全培训与安全意识

L.1 组织内所需的适当安全意识、培训与教育级别

1.意识 Awareness

安全培训的先决条件是意识。培养安全意识的目标是让员工高度重视安全的重要性，站在讲政治的角度把安全放在第一位，充分认识到他们的安全责任和义务，知道能做什么、不能做什么。许多工具都可以被用于培养安全意识，例如海报、通知、时事通讯文章、屏幕保护程序、T 恤衫、经理振奋人心的讲话、告示、演讲、鼠标垫、办公用品、备忘录以及传统的由教师引导的培训课程。

2.培训 Training

教训是教导员工履行工作职责、遵守安全策略并具备基本操作能力。要让新用户知道如何使用 IT 基础架构、数据存储的位置以及如何和为什么要对资源分类。意识和培训往往都是内

部提供的。

3. 教育 Education

往往是由外部提供的，是一项更全面、更细致的工作，对学生或用户进行系统的教学，通常与用户参加认证考试、成为专家或寻求职务晋升关联。

搞清三者的区别，考题会要求选择某活动是属于其中那类？

L.2 定期评审内容相关性

意识、培训和教育必须进行周期性的、适时的评估，以保持与时俱进。

欢迎点击这里的链接进入精彩的Linux公社网站

Linux公社（www.Linuxidc.com）于2006年9月25日注册并开通网站，Linux现在已经成为一种广受关注和支持的一种操作系统，IDC是互联网数据中心，LinuxIDC就是关于Linux的数据中心。

Linux公社是专业的Linux系统门户网站，实时发布最新Linux资讯，包括Linux、Ubuntu、Fedora、RedHat、红旗Linux、Linux教程、Linux认证、SUSE Linux、Android、Oracle、Hadoop、CentOS、MySQL、Apache、Nginx、Tomcat、Python、Java、C语言、OpenStack、集群等技术。

Linux公社（LinuxIDC.com）设置了有一定影响力的Linux专题栏目。

Linux公社 主站网址：www.linuxidc.com 旗下网站：www.linuxidc.net

包括：**Ubuntu 专题** **Fedora 专题** **Android 专题** **Oracle 专题** **Hadoop 专题** **RedHat 专题** **SUSE 专题** **红旗 Linux 专题** **CentOS 专题**

Linux 公社微信公众号：linuxidc_com