

The background of the slide is a light gray gradient with several realistic water droplets of various sizes scattered across it. The droplets have highlights and shadows, giving them a three-dimensional appearance. The main text is centered in the middle of the slide.

CISSP 备考经验分享

@JINXU FANG

ABOUT ME

基本信息

姓名：方锦旭 / Fang JinXu

从业经历

超过5年的安全从业经验

2014 ~ 2018 计算机科学与技术专业，白帽黑客

2018 ~ 2022 国内某云厂商安全工程师，从事攻防技术和安全自动化研究。

2022 ~ NOW 加入某云厂商，安全运营工程师（乙方->甲方）。

目录

- CISSP 考试介绍
- 对准备CISSP认证的三条建议
 - 建议1：找到支持自己通过认证的核心动力
 - 建议2：把握复习节奏，我的复习记录供参考
 - 建议3：独家秘诀，用好考纲，心中不慌
- 通过CISSP后，还可以做这些...

1. CISSP 认证介绍

The background of the slide is a light gray gradient. It is decorated with several realistic water droplets of various sizes, scattered across the right and top portions of the frame. The droplets have highlights and shadows, giving them a three-dimensional appearance.

CISSP 认证介绍

- 全称：CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL / (ISC)²注册信息系统安全专家
- 持证者数量：全球约15万人，国内约4千位（2022年数据）。
- 认证特点：综合素质要求较高、知识面广、信息量大、考试时间长、与实践经验紧密结合，无官方题库。
- 含金量高、雇主认可。

Number of CISSP members as of July, 2022 is 156,054.^[1]

Top 15 countries by CISSP
Member Counts as at July 2022

#	Country (Top 15)	Count
1	United States	95,243
2	United Kingdom	8,486
3	Canada	6,842
4	China	4,136
5	Japan	3,699
6	India	3,364
7	Australia	3,305
8	The Netherlands	2,983
9	Singapore	2,963
10	Germany	2,856
11	Korea	2,090
12	Hong Kong	1,968
13	France	1,277
14	Switzerland	1,127
15	Spain	847

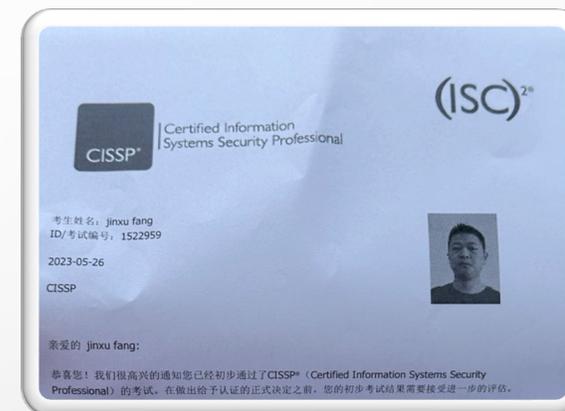
CISSP 认证前提条件

- 在8个DOMAIN中有2个或多个的5年全职工作经验。
- 本科或持ISC2 其他证书可减1年。

如果不满足条件，可先申请成为associate，满足条件之后可转为正式会员（member）

考试、认证流程

- 1. 缴费、预约考试：考试费用\$749.
- 2. 线下考试，携带身份证、信用卡（信用卡需在有效期内
!!）
- 3. 考试通过，现场发放通过成绩单。



- 4. 登录网站，提交工作经历，需要现有会员背书（或ISC2自己审核，不推荐）。
- 5. 等待CISSP审核，下证。（实测从考试通过到下证大约1个月）

考试规则

- 一共250道单选题(中英文对照), 总分为1000分, 700分即为通过。
- 考试时长: 6个小时, 实际上时间完全够用, 4个小时左右即可。
 - 我实际的考试时间: 上午8点开始考试, 中午12点出来。
- 可以吃东西: 牛奶、巧克力等, 补充战斗力。
- 建议:
 - 放缓做题速度, 做题太快可能提高被抽中重考的概率。
 - 把握节奏, 中间可以休息休息(我休息了三次), 需要举手示意即可。

2. 对准备CISSP认证的 三条建议



The background features a light gray gradient with several realistic water droplets of various sizes scattered across the right side and top. The droplets have highlights and shadows, giving them a three-dimensional appearance.

建议1：找到支持自己
通过认证的核心动力

世界很大，大家很忙，没有动力，容易熄火



很忙
忙着可爱
忙着长大



通过CISSP认证的常见动力

提升收入潜力

持证人员的平均年薪为131,030美元

发挥职业潜力

市场需求旺盛，提升职业发展的最好时机

同行中脱颖而出

可为组织提供有效的网络安全领导和指导

了解网安领域各方面

CISSP涵盖了整个网络安全领域的基本要素

展示网安实际经验

(ISC)²持证会员背书证明网安相关工作经验

脱颖而出成为专业人才

持证很有价值，多年发展和研究的产物

成为网安协会会员

获得(ISC)²会员资格福利继续提供专业教育

知乎 @沙子

问：思来想去之后，还是没有找到动力来源

有两种可能性：

1. 世界很广阔，有其他事情更值得我关注，不用考认证。
(完全没问题！)

2. 没动力，但是想用考证逼自己一把，锦旭我该怎么办？请帮助我

非常规动力：把报名费换算成喜欢的东西...

先报名，报名后可以把 \$749 报名费换算成很多很多东西, for example...



一趟旅行



2瓶好酒

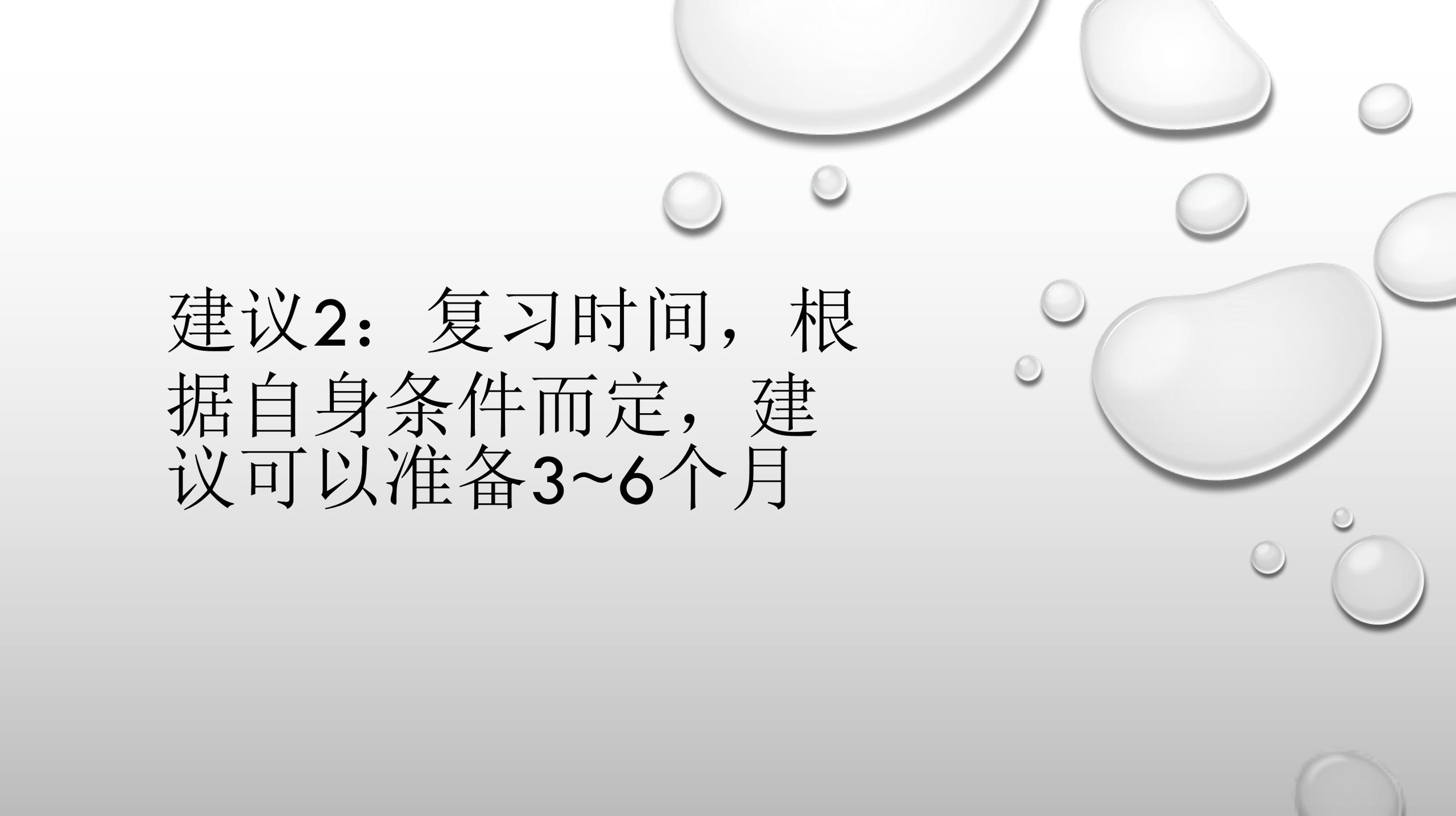


一个游戏机和很多很多卡带....

换算完之后:



动力满满，完全睡不着觉

The background of the slide is a light gray gradient with several realistic water droplets of various sizes scattered across it. The droplets have highlights and shadows, giving them a three-dimensional appearance. The text is centered on the left side of the slide.

建议2：复习时间，根据自身条件而定，建议可以准备3~6个月

我的备考经历：大约3个月（看书自学）

2月底：报名，报名了5月底的考试。



3月-奋斗月：早起不堵车，来公司学习，冲冲冲，动力十足。



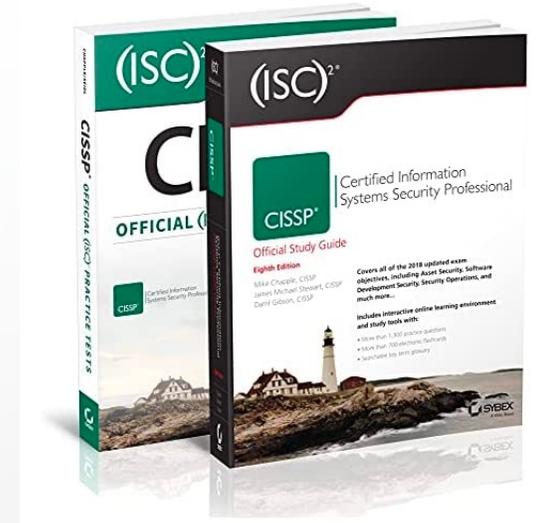
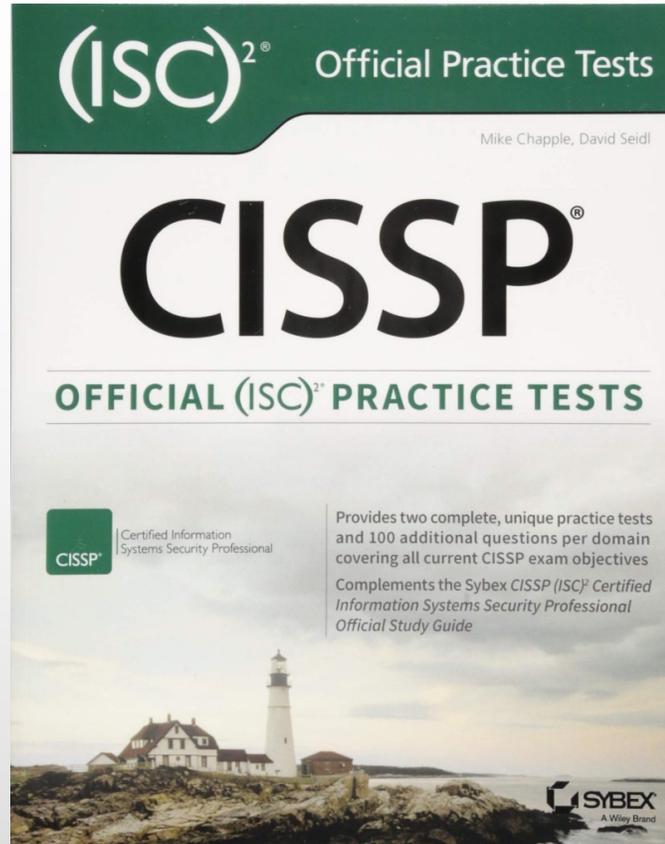
4月-懈怠月：清明节出去踏青好好玩啊 / 五一假期



5月-冲刺月：DDL来了，紧张激动，开始冲刺，下班之后自习室冲冲冲。

复习三件套

1. CISSP复习时候的问题：中文资料少。
2. 我尝试过的一些其他选项：
 - 1) 一些网上的中文题 -> 翻译有问题，答案还不准确
 - 2) ISC2 的 IOS APP -> 都挺好就是看英文效率太低了
 - 3) 一些已经总结好了的复习纲要 -> 都挺好就是过目就忘...
3. 建议：以官方的中文材料（书本）为主，以官方的习题册作为检验手段，以考纲来指导最后冲刺。



复习节奏

- **【3月~4月，1.5个月】**刷OSG共21章：一天一个章节 + 练习题，大约1~2小时。4月中旬的时候完成课本的学习。
- **【5月，2周】**随后开始刷PRACTICE LIST的综合题，一天50道题，回头看课本，查漏补缺。初做准确度60%左右，之后70%左右。



别慌 稳住 问题不大



全他妈是问题！
还别慌

- **【5月 第3周】**随后根据官方考纲，整理思维导图，看书回忆知识点。
- 然后怀着忐忑的心情去考试了。

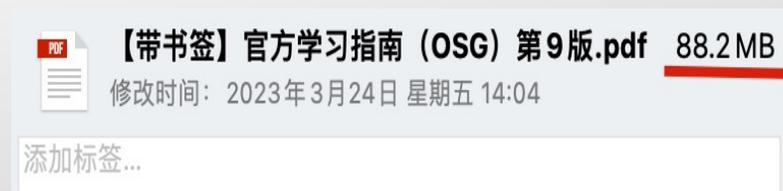
The background features a light gray gradient with several realistic water droplets of various sizes scattered across the right side and top. The droplets have highlights and shadows, giving them a three-dimensional appearance.

建议**3**: 用好考纲，心
中不慌（**独门秘籍**）

经验3:用好考纲，心中不慌

- CISSP特点：一英里宽，一英寸深。
- OSG告诉你CISSP大约有多宽。
- 考纲可以帮助确定，一英寸大约有多深。

据不完全统计：有88.2MB宽，858KB深。



考纲分析，以DOMAIN2: ASSET SECURITY为例

- 根据考纲，使用思维导图，回顾OSG中的内容，细化每个考点

2.1 识别并分类信息和资产

- » 数据分类
- » 资产分类

2.2 制定信息和资产处理要求

2.3 安全配置资源

- » 信息和资产所有权
- » 资产列表（如有形、无形）
- » 资产管理

2.4 管理数据生命周期

- » 数据角色（例如，所有者、控制者、保管员、处理员、用户/对象）
- » 数据采集
- » 数据位置

2.1 识别并分类信息和资产

- 数据分类

常见敏感数据 - PII/PHI(HIPAA法规负责PHI)

政府数据分类: 绝密、秘密、机密、未分类

非政府数据分类: 机密、私有、敏感、公开

- 资产分类: 与数据分类相匹配

资产密级: 处理数据最高级别

数据状态: 静态、传输中、使用中

后续: 定义安全要求并确定安全控制策略能满足安全要求。

2.2 制定信息和资产处理要求

1. 不断地进行数据维护，包括审查数据策略。

2. 使用DLP。网络DLP + 终端DLP

3. 使用标记技术: 如加水印、数字标签、贴上密级类别等

4. 处理(Handling)

5. 数据收集限制: 防止数据丢失的最简单方法之一。

2.4 管理数据生命周期

- 数据角色

数据所有者: 一般是CEO

资产所有者

业务所有者

数据控制者: 数据控制者决定要处理什么数据, 为什么要处理这个数据, 以及如何处理它。

数据托管人员custodian、处理者、用户

- 数据销毁 & 数据残留

擦除(Erasing) - 格式化或致删除文件

清理(Clearing) - 写0

清除(Purging) - 更强烈的清理方式, 重复清理, 无法恢复原始数据

消磁 + 销毁

COMMON QUESTIONS

- 需要报培训班吗？
 - 因人而异，我觉得不需要报名培训班。
 - 我自学的难点：面对考试的不确定性。(希望我的分享能够帮助你减少这个不确定性)
- 教材选择：AIO 还是OSG
 - 建议OSG，AIO 太大太长，不适合作为应试资料。(OSG 700页， AIO 1000页)

考完 CISSP 的感受

- 收获：是一个很好的扩充自己知识面的方式。
- 后续：
 - 1. CISSP中描述的一种完美主义，和现实存在一些差异性，需要裁剪以切合企业的安全需求。
 - 2. 要从认识离合器，成长到HOW TO DRIVE A CAR，需要持续学习和实践。



Easy to Know



Hard to Play

谢谢聆听
(以及祝你好运!)

