# 中国通信企业协会网络安全人员能力认证考试知识点大纲

# 技术类基础级(CACE-CPAC-BLT)

**中国通信企业协会网络安全人员能力认证中心**

**2017 年 3 月**

# 目录

# 第一部分综述

# 第1章 政策法规及道德规范

## 1.1 国家网络安全相关法律法规

了解国家安全委员会和中央网络安全和信息化领导小组，重点领会总书记“419”讲话内容和精神。

### 1.1.1我国网络安全管理体制

了解我国各级网络安全管理部门之间的关系和各自职责。

### 1.1.2网络安全相关法律法规

了解“国家网络空间主权”提法的出处，了解维护网络和信息安全的核心任务。了解《网络安全法》基本内容。了解《电信条例》基本内容。

### 1.1.3信息安全等级保护相关法规政策

了解《关于信息安全等级保护工作的实施意见》和《信息安全等级保护管理办法》的基本内容和要求。

## 1.2 电信和互联网行业网络安全管理政策

### 1.2.1通信网络安全相关法规政策

了解《通信网络安全防护办法》的基本内容和要求；了解《电信和互联网用户个人信息保护规定》基本内容和要求；了解《关于加强电信和互联网行业网络安全工作的指导意见》的八项工作任务。

### 1.2.2网络安全防护

了解安全防护的原则、方针和理念；了解定级备案的要求，了解符合性评测和风险评估的要求。了解网络安全防护监督检查工作内容。

### 1.2.3网络安全威胁治理

了解网络安全威胁治理相关的技术手段建设和管理情况。

### 1.2.4网络安全应急保障

了解《公共互联网网络安全应急预案》基本内容，了解预警分级、监测上报、应急响应的基本流程和要求。

## 1.3 道德规范

主要了解网络安全从业人员应当遵守的相关道德规范。相关道德规范具体可以分为通行道德规范和职业道德规范，无论通行道德规范和职业道德规范，网络安全从业人员都应遵守，道德规范是对网络安全从业人员的基本要求。

# 第2章 安全管理标准及体系

## 2.1 国际主要标准介绍

### 2.1.1ISO 27000 系列标准简介

1) 了解 ISO 27000 系列重要标准的编号及名称
2) 了解 ISO 27000 系列各标准之间的关系

### 2.1.2NIST SP 800 系列标准简介

了解 NIST SP 800 系列标准的基本内容

### 2.1.3ISO/IEC 15408 简介

1) ISO/IEC 15408 标准的主要目的以及使用场景。

2) 了解 CC 标准的安全功能要求。

3) 熟悉 cc 标准的主要控制项。

## 2.2 国内主要安全标准介绍

### 2.2.1通信网络安全防护标准简介

1. 电信网和互联网安全防护管理指南

    1) 了解该标准的适用范围

    2) 理解电信网和互联网安全防护体系的构成

    3) 了解安全等级保护实施的基本过程

    4) 了解安全风险评估实施的基本过程

    5) 了解灾难备份及恢复实施的基本过程

    6) 理解电信网和互联网安全防护体系中的安全等级保护、安全风险评估、灾难备份及恢复三者之间的关系

2. 电信网和互联网安全风险评估实施指南

    1) 了解标准的主要内容和目的

    2) 了解对于电信网和互联网相关系统生命周期中的风险要素

    3) 熟悉风险实施的流程

3. 电信网和互联网灾难备份以及恢复实施指南

    1) 理解该标准的目的和主要的内容

    2) 了解灾难备份及恢复定级的 5 个等级的主要内容

    3) 了解不同级别对应有的技术和管理支持的要求

4. 电信网和互联网安全等级保护实施指南

    1) 了解实施指南的主要内容与结构

    2) 熟悉实施指南的安全等级保护对象

    3) 熟悉安全等级保护实施的基本过程

4) 熟悉电信网和互联网及相关系统定级方法

## 2.2.2其他网络安全相关标准简介

1. 信息系统等级保护相关标准
   1) 了解信息系统安全等级保护标准体系的组成结构
   2) 了解信息系统安全等级保护的关键环节
   3) 熟悉信息安全等级保护实施过程与方法
2. GB/Z 20985-2007 信息技术安全技术信息安全事件管理指南
   1) 了解标准的结构
   2) 掌握标准核心思想和主要内容
3. GB/Z 20986-2007 信息安全技术信息安全事件分类分级指南
   1) 了解标准的结构
   2) 掌握标准核心思想和主要内容
4. GB/T 24363-2009 信息安全技术信息安全应急响应计划规范
   1) 了解标准的结构
   2) 掌握标准核心思想和主要内容

# 第二部分通用网络安全技术知识

# 第3章 密码技术

## 3.1 密码技术基础知识概述

### 3.1.1密码学与信息安全

1) 了解密码学的概念
2) 掌握密码学和信息安全之间的内在关系

### 3.1.2基本术语和概念

1) 了解密码学的含义
2) 掌握密钥的含义及分类
3) 掌握明文和密文的概念及区别
4) 掌握加、解密的概念及关系
5) 掌握密码算法的概念和分类

### 3.1.3密码技术发展历史

1) 了解密码技术发展历史的四个不同时期
2) 了解古代加密方法表现形式
3) 了解古典密码的加密方式
4) 了解近代密码的形成时期及方法
5) 了解现代密码的形成时期及特点

# 3.2 密码技术标准

## 3.2.1标准化组织

了解使密码技术标准化的国际组织

## 3.2.2开放系统

了解现存的各个标准化密码学开放系统

## 3.2.3因特网标准与 RFC

1) 了解因特网标准的概念
2) 掌握两种关于密码学技术的两种 RFC

## 3.2.4我国密码学的安全标准

1) 了解我国形成密码学安全标准的时间
2) 掌握我国密码学标准的特点及地位

# 3.3 常见密码技术

## 3.3.1密码学分析

1) 了解密码学分析的概念
2) 掌握五种密码学分析的方法

## 3.3.2古典密码

1) 了解移位密码的概念及基本方法
2) 了解替换密码的概念及基本方法

### 3.3.3现代密码

1) 了解私钥密码的基本方法

2) 掌握公钥密码的核心思想、基本方法

## 3.4 资产管理

### 3.4.1资产管理概述

了解资产管理的基本概念、条件及对企业管理的作用。

### 3.4.2保密性与认证标准

1) 了解保密性的基本概念及含义

2) 掌握在资产管理的过程中实行保密性的必要性。

### 3.4.3信息数据生命周期

1) 了解信息生命周期的概念

2) 掌握信息生命周期从开始到结束所包含的六个阶段

### 3.4.4鉴权技术分类与实现

1) 了解鉴权技术的基本概念

2) 掌握八种常见的鉴权技术分类形式

## 3.5 数字签名技术

### 3.5.1数字签名概述

1) 了解数字签名的概念

2) 掌握数字签名在密码学中的作用性

### 3.5.2数字签名标准

了解数字签名标准的概念及形成

### 3.5.3RSA 数字签名生成方案

1) 了解 RSA 数字签名生成的过程
2) 掌握 RSA 数字签名在生成过程中需要满足的四个基本条件

### 3.5.4一次性签名方案

1) 了解一次性签名方案的概念
2) 掌握一次性签名性需要满足的条件

### 3.5.5群体数字签名方案

1) 了解不同于传统数字签名的特点
2) 掌握群体数字签名的概念及常见签名类型

## 3.6 哈希函数

### 3.6.1哈希函数的概念

了解哈希函数基本概念及含义

### 3.6.2哈希函数的性质与分类

1) 了解哈希函数五种基本性质
2) 掌握哈希函数的三种基本分类形式

### 3.6.3消息摘要的构造方法

1) 了解消息摘要的概念

2) 掌握消息摘要采用的基本构造方法

### 3.6.4数据完整性及数据源认证的实现

1) 了解数据完整性的含义

2) 掌握数据源的两层含义以及据源认证的实现方法

## 3.7 密钥管理技术

### 3.7.1密钥建立的模式

了解密钥建立过程需要考虑的两个条件

### 3.7.2密钥协商

了解密钥协商的概念

### 3.7.3密钥分配模型

了解钥分配模型所包括的四种基本方案

### 3.7.4密钥期限和加密密钥的层次结构

1) 了解密钥期限的概念和作用

2) 掌握按照 ANSI X.17 将密钥分成的三个层次

### 3.7.5公钥分配技术

1) 了解公钥分配技术的概念

2) 掌握公钥分配技术与对称密码体制密钥分配的本质性差别所在

### 3.7.6密钥生存期

1) 了解密钥生存期的概念
2) 掌握从两个方面阐述密钥生存期存在的必要性

## 3.8 身份识别

### 3.8.1身份识别的概念

1) 了解身份识别的含义
2) 掌握身份识别的实现方法

### 3.8.2弱身份识别

了解弱身份识别的概念

### 3.8.3强身份识别

了解强身份识别的概念

### 3.8.4身份识别协议

1) 了解身份识别协议的概念
2) 掌握一个安全的身份识别协议至少应满足的两个条件

### 3.8.5对身份识别协议的攻击

1) 掌握针对身份识别协议的六种攻击方式的含义
2) 掌握六种攻击方式的表现形式及方法

# 第4章 安全协议

## 4.1 安全协议概述

### 4.1.1安全协议说明

1) 了解安全协议的基本概念
2) 了解安全协议如何在各类信息系统中的应用和不安全协议使用的危险
3) 了解了解安全协议的运行原理和安全协议本身的特点

### 4.1.2网络安全与安全协议

1) 了解安全协议在网络安全中的重要作用
2) 了解网络安全面向用户、系统和数据等不同方面的重要性
3) 了解如何通过诸多安全手段提升信息系统安全性，做好信息安全工作，保护重要的信息系统。

### 4.1.3密码与安全协议

1) 了解“密码和安全协议是网络安全的核心”这一重要观点
2) 了解密码算法和逻辑协议在安全协议中的作用
3) 了解一个不安全的安全协议会带来怎样的危害

### 4.1.4安全协议分类

1) 了解应用层安全协议
2) 了解运输层安全协议
3) 了解网络层安全协议
4) 了解数据链路层安全协议

# 4.2 TCP/IP 协议概述

## 4.2.1TCP/IP 协议的发展

1) 了解 TCP/IP 协议的发展历史
2) 了解 TCP/IP 协议参考模型以及该模型与 OSI 模型对应的层次划分
3) 了解 TCP/IP 协议族本身的独特特点

## 4.2.2网络接口层协议特征说明

1) 了解物理层中物理介质的特性
2) 了解数据链路层中 ARP 正向地址解析协议与 RARP 反向地址解析协议
3) 了解常见接口协议的种类

## 4.2.3网络层协议特征说明

1) 了解处理传输层分组发送请求
2) 了解处理输入数据包
3) 了解处理路径、流控、拥塞
4) 掌握网路层 IP 协议、ICMP 协议等知识

## 4.2.4传输层协议特征说明

1) 了解格式化信息流、提供可靠传输等应用程序间通信的特点
2) 了解“三次握手”过程
3) 了解传输控制协议 TCP 和用户数据报协议 UDP

## 4.2.5应用层协议特征说明

1) 了解 FTP 文件传输协议
2) 了解 Telnet 用户远程登录服务
3) 了解 DNS 域名解析服务

4) 了解 SMTP 简单邮件传输协议

5) 了解 NFS 网络文件系统

6) 了解 HTTP 超文本传输协议

# 4.3 网络接口层协议

## 4.3.1网络接口层常见攻击方式

了解无线密码破解等网络接口层常见攻击方法

## 4.3.2网络接口层常见安全协议

了解 PPTP、WEP、WPA 等网络接口层常见安全协议

## 4.3.3PPTP 协议分析说明

1) 了解 PPTP 点对点隧道协议的概述

2) 掌握 PTP 协议的原理

## 4.3.4WEP 协议分析说明

1) 了解数据安全性、接入控制、数据完整性等方面 WEP 协议的特性

2) 了解 WEP 协议的工作原理

## 4.3.5WPA 协议分析说明

1) 了解生成 MSDU

2) 了解生成 WEP 种子

3) 了解封装 WEP

# 4.4 网际层协议--虚拟专用网络协议（IPSEC）

## 4.4.1网际层常见攻击方式

1) 了解 MAC 地址泛滥攻击
2) 了解 DHCP 服务器欺骗攻击
3) 了解 ARP 欺骗
4) 了解 IP/MAC 地址欺骗

## 4.4.2网际层常见安全协议

了解 IPSEC 协议等网际层常见安全协议的基础知识

## 4.4.3IPSEC 协议分析说明

1) 了解 IPSEC 协议的特性
2) 了解 IPSec 提供的两种安全机制：认证（采用 ipsec 的 AH）和加密（采用 ipsec 的 ESP）

# 4.5 传输层安全（TLS/SSL、Socks）协议

## 4.5.1传输层常见攻击方式

1) 了解异常包
2) 了解 LAND 攻击
3) 了解 Flood 攻击
4) 了解端口扫描

## 4.5.2传输层常见安全协议

1) 了解 TLS/SSL 协议
2) 了解 Socks 协议

### 4.5.3TLS/SSL 协议分析

1) 了解 SSL 安全套接层协议的基本知识
2) 了解 SSL 协议的秘密性、完整性、认证性
3) 了解 SSL 的强化版本 TLS 协议格式
4) 了解 TLS/SSL 这类协议的运行原理，安全性

### 4.5.4SOCKS 协议分析说明

1) 了解 SOCKS 协议的基本概念
2) 了解 Socks 服务器和 Socks 客户库两个组件，以及它们的运行原理。

## 4.6 应用层协议（SSH、SET、kerberos 等）

### 4.6.1应用层常见攻击方式

1) 了解应用软件（如 SQL Server、Sendmail、PostScript 和 FTP）缺陷
2) 了解应用层方面详细列出常见攻击方式和原理

### 4.6.2应用城常见安全协议

1) 了解 SSH 协议
2) 了解 SET 协议
3) 了解 Kerberos 协议
4) 了解 HTTP 协议

### 4.6.3SSH 协议分析

1) 了解 SSH 协议定义、以及传输加密方式，
2) 了解 SSH 通道模式
3) 了解 SSH 协议框架中的三个主要协议传输层协议、用户认证协议、连接协议
4) 掌握每层协议之间的层次关系

5) 掌握 SSH 的应用。

### 4.6.4SET 协议分析

1) 了解 SET 协议的概念
2) 了解 SET 协议的安全性
3) 了解 SET 协议在网上银行等方面的应用

### 4.6.5kerberos 协议分析

1) 了解 Kerberos 协议的基本概念
2) 了解 Kerberos 协议的历史
3) 了解 Kerberos 协议的基本描述
4) 了解 Kerberos 协议的具体流程。

# 第5章 网络安全攻击技术

## 5.1 网络攻击技术概述

### 5.1.1网络攻击技术概念

1) 了解网络攻击事件的诸多产生因素
2) 了解网络攻击行为的危害性
3) 掌握网络攻击保密性、完整性等特点，并能说明其技术的重要性

### 5.1.2网络攻击技术类型

1) 了解从被动攻击、主动攻击、邻近物理攻击、内部人员攻击等方面进行阐述网络攻击技术的主要攻击形式
2) 掌握网络攻击技术的主要类型

### 5.1.3网络攻击技术一般流程

1) 了解网络攻击的大致步骤分析
2) 掌握寻找找目标、进入目标，获取登录权限、获取控制权限、保留后门、网络隐身等方面着手的网络攻击一般流程

### 5.1.4网络管理与攻防常用命令

1) 掌握 ping 命令的主要内容，能够进行实例操作
2) 掌握 Pathping 命令，能够进行实例操作
3) 掌握 Tracert（Traceroute）命令，能够进行实例操作
4) 掌握 netstat 命令，能够进行实例操作
5) 掌握 nbtstat 命令，能够进行实例操作
6) 了解其他的命令以及主要的利用方式

## 5.2 黑客与攻击技术

### 5.2.1漏洞扫描技术

1) 了解其硬件、软件等领域说明其危害性
2) 了解漏洞扫描的概念、意义和实施步骤
3) 掌握漏洞扫描的基本技术

### 5.2.2网络嗅探技术

1) 了解嗅探技术的概念、局限性等基础知识
2) 了解嗅探技术的实现原理

### 5.2.3口令破解技术

1) 了解口令破解技术定义等基础知识
2) 掌握口令破解的清除密码、后门密码、网络窃听、社会工程、暴力破解、MD5 破解等常见

技术

### 5.2.4计算机病毒及特洛伊木马

1) 了解病毒的定义、简史、危害、以及一些具有代表性的特性，如：隐蔽性、传染性、表现性或破坏性等。
2) 掌握病毒的分类，和主要的分类内容
3) 掌握计算机病毒的逻辑结构、工作原理

## 5.3 网络入侵技术

### 5.3.1网络后门技术

1) 了解后门技术的发展历程、分类等方面介绍其相关内容
2) 掌握后门程序的分类
3) 掌握后门程序的具体设置方法和运用的相关工具

### 5.3.2网络隐身技术

1) 了解网络隐身技术的具体实施过程
2) 掌握系统日志的相关基础知识，掌握日志文件存放位置
3) 掌握清楚攻击痕迹的方法

## 5.4 网络安全攻击事件

### 5.4.1海康威视被黑客植入代码

1) 了解该事件的起因和发展经过
2) 掌握黑客植入代码技术的原理和防御方法

## 5.4.2支付宝机房电缆被挖断

1) 了解该事件的起因和事件发展经过
2) 了解该事件的影响和其危害性
3) 掌握该事件的防御方法

## 5.4.3DDOS 攻击事件-运营商

1. DDOS
    1) 了解 DDOS 基础知识
    2) 掌握 DDOS 攻击原理
2. DDOS 攻击事件
    1) 了解该事件的起因和事情经过
    2) 掌握 DDOS 攻击事件的防御措施

## 5.4.4电信网络诈骗

1) 了解电信网络诈骗概念
2) 了解类似事件发生的起因和事情经过
3) 掌握类似事件的防范措施

## 5.4.5德国核电站因恶意程序被迫关闭

1. 恶意程序
    1) 了解恶意程序基础知识：定义、危害性等
    2) 掌握恶意程序攻击原理
2. 恶意程序事件
    1) 了解德国核电站因恶意程序被迫关闭事件的起因和事情经过
    2) 了解该事件的危害性和

# 5.5 网络安全攻击防范

## 5.5.1加强对安全防范的重视

掌握安全防范的主要措施

## 5.5.2及时使用防毒、防黑等防火墙保护软件

1) 了解及时使用防毒、防黑等防火墙保护软件的重要性

2) 掌握防毒、防黑等防火墙保护软件的使用方法

## 5.5.3及时进行系统升级、打补丁

1) 了解及时进行系统升级、打补丁的重要性

2) 掌握系统升级、打补丁的方法

# 第三部分网络安全防护

# 第6章 系统自身安全防护技术

## 6.1 Windows 安全防护技术

### 6.1.1Windows 操作系统的基本结构

1) 了解 windowsNT 内核的体系结构
2) 了解系统的关键进程和文件

### 6.1.2Windows 操作系统安全体系结构

1) 了解安全操作系统的标准
2) 理解 windowsserver2008 的安全标识符
3) 理解 windowsserver2008 的 ACL
4) 理解 windowsserver2008 的注册表与安全
5) 了解 windowsserver2008 的启动过程

## 6.2 Linux 安全防护技术

### 6.2.1Linux 系统概述

了解 Linux 系统的由来

### 6.2.2Linux 系统安全基础

1) 了解 Linux 系统加固要点
2) 了解 Linux 系统常用命令

### 6.2.3Linux 系统安全防范

1) 了解 Linux 系统安装安全
2) 理解 Linux 系统物理安全与登录安全
3) 理解 Linux 账户安全

## 6.3 数据安全防护技术

### 6.3.1数据库安全防护

1) 了解数据库面临的威胁
2) 了解数据库安全防护
3) 了解数据库安全防护过程

### 6.3.2事前安全防护

1) 理解事前安全防护的内容
2) 了解数据库产品的选择
3) 了解数据库运行配置的检测

### 6.3.3事中监控

1) 理解事中监控的内容
2) 了解纵深防御思想在事中监控阶段的影响

### 6.3.4事后审计

1) 了解事后审计的作用
2) 了解事后审计的方法

## 6.4 中间件安全防护技术

### 6.4.1Web 中间件防护

1) 理解 web 中间件加固要点

2) 了解 apache、IIS 等加固方法

# 第7章 网络安全设备

## 7.1 防火墙

1) 理解防火墙的作用

2) 理解包过滤技术、状态检测技术和应用代理技术的原理和优缺点

## 7.2 IDS 与 IPS

1. IDS
    1) 理解入侵检测基本概念和工作原理
    2) 理解入侵检测的分类
2. IPS
    1) 理解 IPS 的基本概念和工作原理
    2) 理解 IDS 与 IPS 的区别

## 7.3 防病毒

### 7.3.1防病毒技术原理

1) 了解病毒检测的方法

2) 理解特征码技术的原理

3) 了解虚拟化环境下的防病毒解决方案

### 7.3.2传统桌面防病毒软件的工作机制

1) 了解防病毒软件的部署方式
2) 了解防病毒软件的工作机制

### 7.3.3传统防病毒软件在虚拟化环境下面临的问题

了解虚拟化环境下的防病毒软件面临的问题

## 7.4 DDOS 防护设备

### 7.4.1DDOS 防护技术原理

1) 理解 DDOS 攻击的原理
2) 理解 DDOS 攻击的防护手段

### 7.4.2大规模异常流量（DDOS、蠕虫等）监测技术原理

1) 了解监测、流量清洗技术的原理
2) 理解监测、流量清洗设备的部署方式

# 第8章 网络安全系统与平台

## 8.1 4A

1) 了解 4A 的概念
2) 了解账户管理的内容
3) 了解认证管理的内容
4) 了解权限管理的内容
5) 了解 4A 系统的部署

## 8.2 ISMP

1) 了解 ISMP 原理
2) 了解 ISMP 的部署

## 8.3 SOC

1) 了解 SOC 的概念与发展
2) 了解 SOC 技术原理
3) 了解 SOC 的部署
4) 了解 SOC 的解决方案

## 8.4 态势感知

### 8.4.1态势感知概念

1) 了解态势感知的概念
2) 了解态势感知的作用

### 8.4.2态势感知现状与发展趋势

了解态势感知的发展趋势

# 第四部分风险评估

# 第9章 风险评估实施流程

## 9.1 风险评估准备工作

### 9.1.1组建风险评估项目团队

1) 了解直接或间接参与风险评估的角色
2) 理解参与风险评估人员的工作职责
3) 了解参与风险评估人员的关系

### 9.1.2制定风险评估计划

1) 掌握风险评估计划的内容
2) 掌握风险评估的过程

## 9.2 风险评估实施流程

### 9.2.1风险要素识别

1) 理解风险的基本要素
2) 理解风险要素之间的关系
3) 理解风险要素识别的内容

### 9.2.2风险分析

1) 理解风险计算模型
2) 理解可能性计算
3) 理解影响计算

4) 理解风险计算

### 9.2.3风险处置

1) 理解风险处理的方式

2) 理解每种方式的具体措施

## 9.3 建立风险评估工作长效机制

1) 理解风险评估是一个动态的过程

2) 理解建立风险评估的长效机制

# 第10章 风险识别与评价

## 10.1 风险要素

### 10.1.1 资产

1) 理解资产的分类

2) 理解如何识别资产

3) 理解识别资产的重要性

### 10.1.2 威胁

1) 理解威胁的概念

2) 掌握威胁的分类

3) 掌握威胁度量的属性

4) 掌握威胁的获取

5) 理解识别威胁的过程

### 10.1.3 脆弱性

1) 理解脆弱性的概念
2) 掌握脆弱性识别的内容
3) 掌握脆弱性识别的手段
4) 理解脆弱性识别的过程
5) 掌握脆弱性的度量

### 10.1.4 已有安全措施

1) 理解安全措施的分类
2) 掌握安全措施识别的方法
3) 理解安全措施识别的过程

## 10.2 风险分析方法

### 10.2.1 定量的风险分析

1) 理解定量风险计算的要素
2) 理解定量风险计算的公式

### 10.2.2 定性的风险分析

1) 理解定性风险分析的方式
2) 理解定性风险分析的过程

### 10.2.3 半定量风险分析

1) 理解定性与定量风险分析的区别
2) 理解为什么使用半定量风险分析

# 第11章 扫描、渗透及常用工具

## 11.1 安全基线检测

1) 了解扫描、渗透工具在风险评估中的作用

2) 了解安全基线检测的内容

## 11.2 马病毒专项检查

了解木马病毒检查内容

## 11.3 渗透与攻击性专项测试

了解渗透与攻击性测试的内容

## 11.4 关键设备安全性专项测试

1) 了解 web 服务器检查内容

2) 了解操作系统检查内容

3) 了解数据库检查内容

4) 了解网络设备检查内容

# 第12章 风险评估报告

## 12.1 风险评估报告的形式

1) 理解风险评估报告的形式

2) 理解风险评估报告的内容

## 12.2 风险评估结果分析

1) 了解风险控制的方法

2) 了解风险减低的方法

3) 了解风险控制的方式