信息安全保障人员认证
信息安全风险管理培训课程
第6课 信息安全风险评估标准GB/T20984

目录

一、我国信息安全风险评估
二、GB/T 20984设计思想
三、风险评估框架及流程
四、风险评估实施
五、被评估对象生命周期不同阶段的风险评估

一、我国信息安全风险评估

内容提要：我国信息安全风险评估发展史、与风险管理相关的国家标准。

GB/T 20984出版前的工作

调查研究

成立课题组
完成三份报告

标准编制

两个国标草案

试点工作

国信办[2006]
5号文

GB/T 20984的发展

GB/T 20984:2007

《网络安全法》

GB/T 20984:2019（报批稿）

GB/T 31509 标准

GB/T 31509《信息安全技术 信息安全风险评估实施指南》

为指导信息安全风险评估工作的开展，本标准依据GB/T 20984《信息安全技术 信息安全风险评估规范》，从风险评估工作开展的组织、管理、流程、文档、审核等几个方面提出了相关要求，是操作性指导标准。

风险评估原则

- 标准性原则
- 关键业务原则
- 可控性原则

（服务、人员信息、过程、工具）

- 最小影响原则

例题1

多选题：依据《GB/T 31509 信息安全技术 信息安全风险评估实施指南》，开展风险评估要遵循的原则包括（ ）。

√ A. 标准性原则

B. 可操作性原则

√ C. 关键业务原则

√ D. 可控性原则

二、GB/T 20984设计思想

内容提要：OCTAVE方法、GB/T 20984的结构。

OCTAVE概述

美国卡耐基梅隆大学
软件工程研究所
CMU/SEI

O：可操作性 C：关键性 T：威胁

Operationally Critical Threat Asset Vulnerability Evaluation

A：资产 V：脆弱性 E：评估

三个阶段八个过程

第一阶段
建立基于资产的威胁概要文件
OCTAVE Phase 1, Build Enterprise-Wide Security Requirements

过程1
标识高层管理部门的知识
OCTAVE Process 1, Identify Enterprise Knowledge

过程2
标识业务区域管理部门的知识
OCTAVE Process 2, Identify Operational Area Knowledge

过程3
标识员工的知识
OCTAVE Process 3, Identify Staff Knowledge

过程4
建立威胁配置文件
OCTAVE Process 4, Establish Security Requirements

第二阶段
识别基础设施的脆弱点
OCTAVE Phase 2, Identify Infrastructure Vulnerabilities

过程5
标识重要资产的关键组件
OCTAVE Process 5, Map High-Priority Information Assets to Information Infrastructure

过程6
评估选定的组件
OCTAVE Process 6, Perform Infrastructure Vulnerability Evaluation

第三阶段
开发安全策略和计划
OCTAVE Phase 3, Determine Security Risk Management Strategy

过程7
执行风险分析
OCTAVE Process 7, Conduct Multi-Dimensional Risk Analysis

过程8
开发保护策略
OCTAVE Process 8, Develop Protection Strategy

GB/T 20984的结构

生命周期各阶段的风险评估
- 规划阶段
- 设计阶段
- 实施阶段
- 运行阶段
- 废弃阶段

工作形式
- 自评估
- 检查评估

框架及流程
- 风险要素关系
- 风险分析原理
- 风险评估流程

风险评估实施
- 风险评估准备
- 风险识别
- 风险分析和计算
- 风险评价
- 风险沟通
- 风险评估文档记录

风险处理
- 《GB/T 33132-2016》

例题2

单选题：卡内基梅隆 OCTAVE 评估方法，以下描述错误的是（ ）。

A. 包括3个阶段8个子过程

B. O代表可操作性

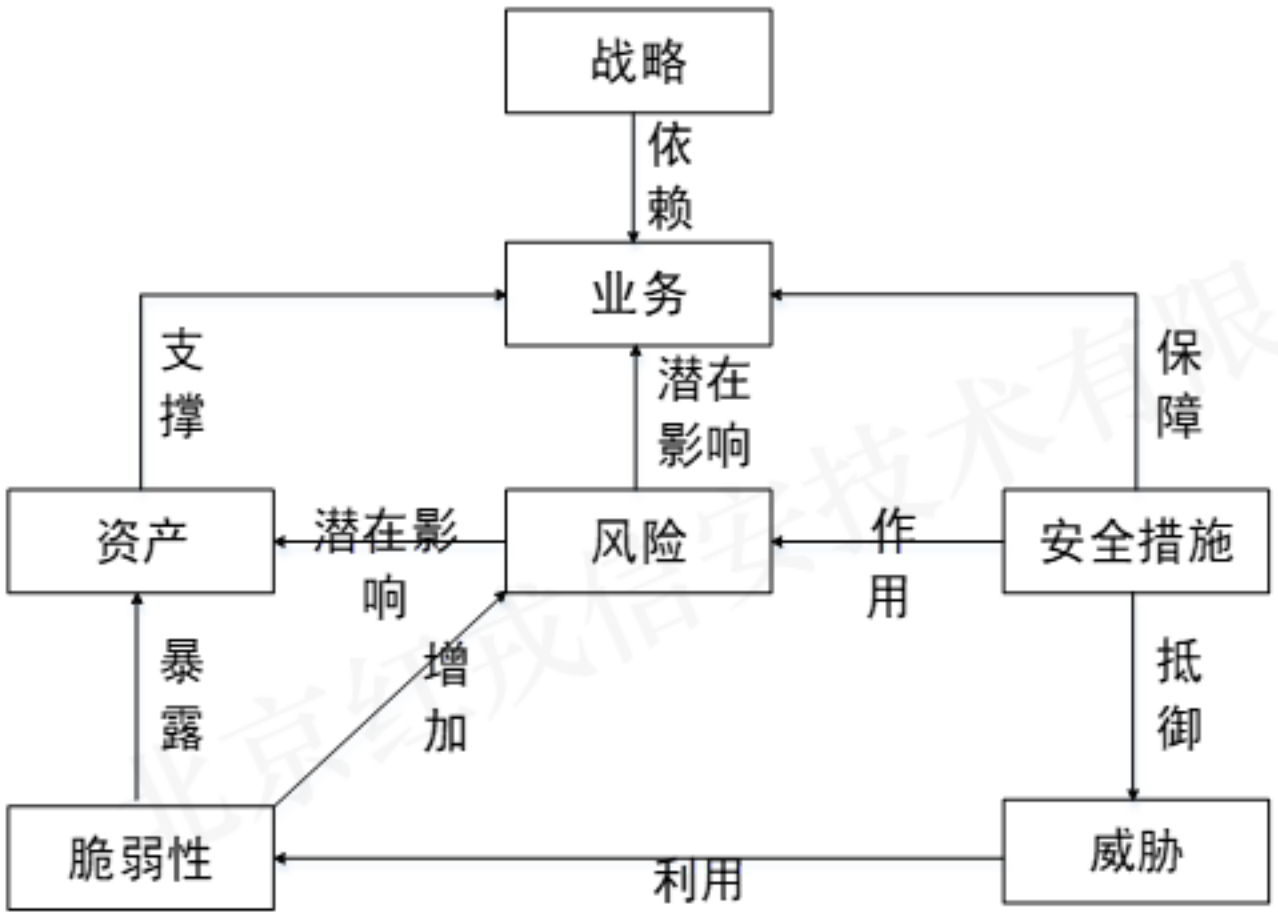
C. C代表关键性

√ D. T代表资产

三、风险评估框架及流程

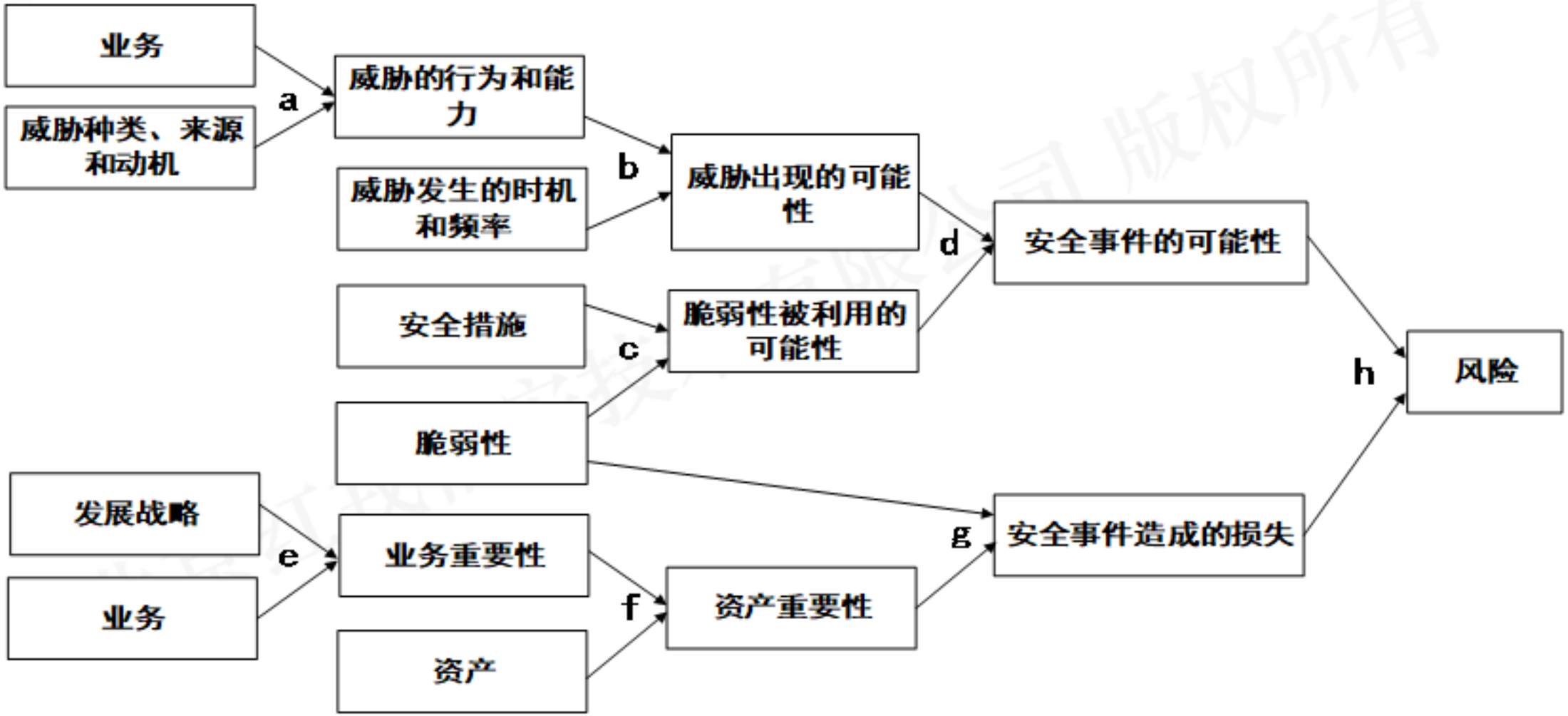
内容提要：要素及要素间关系、风险分析原理、风险评估实施流程。

要素及要素间关系

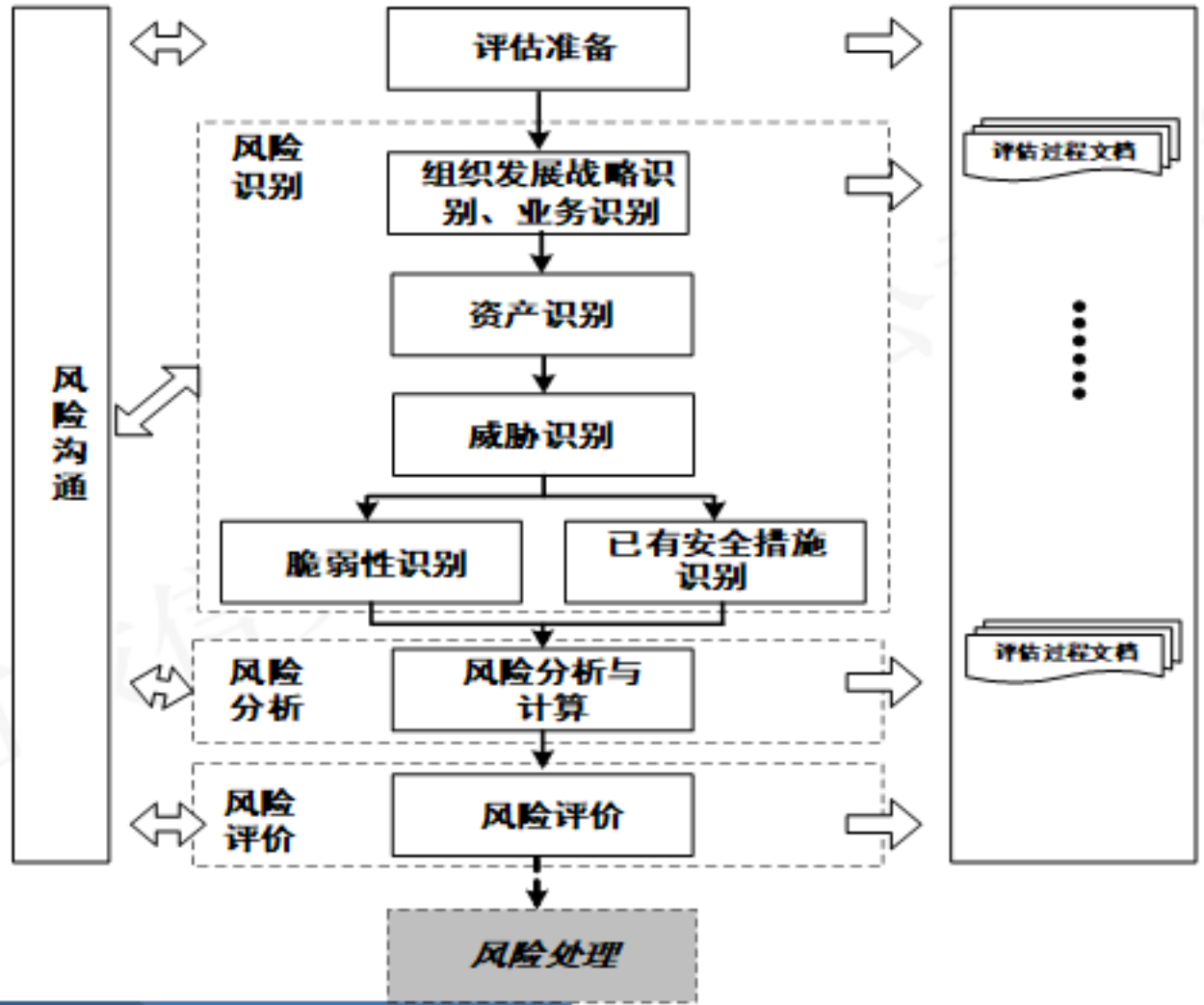


- 风险评估框架的内容：构成风险的要素及其相关关系
- 风险评估7要素：战略、业务、资产、威胁、脆弱性、安全措施和风险
- 在对这7个基本要素评估过程中，要考虑战略、安全需求、安全事件、残余风险、业务重要性和资产价值等与这些基本要素相关的各类属性。

信息安全风险分析原理



风险评估实施流程



例题3

单选题：在GB/T 20984的风险评估7个要素中，“战略”要素与“脆弱性”要素没有直接关联，但是通过（ ）关联起来。

A. 安全措施、威胁

B. 安全措施、风险

√ C. 业务、资产

D. 风险、威胁

例题4

单选题：依据《GB/T 20984 》，在确定评估对象风险时，需要先计算得到（　）和安全事件造成的损失。

A. 业务重要性

B. 威胁出现可能性

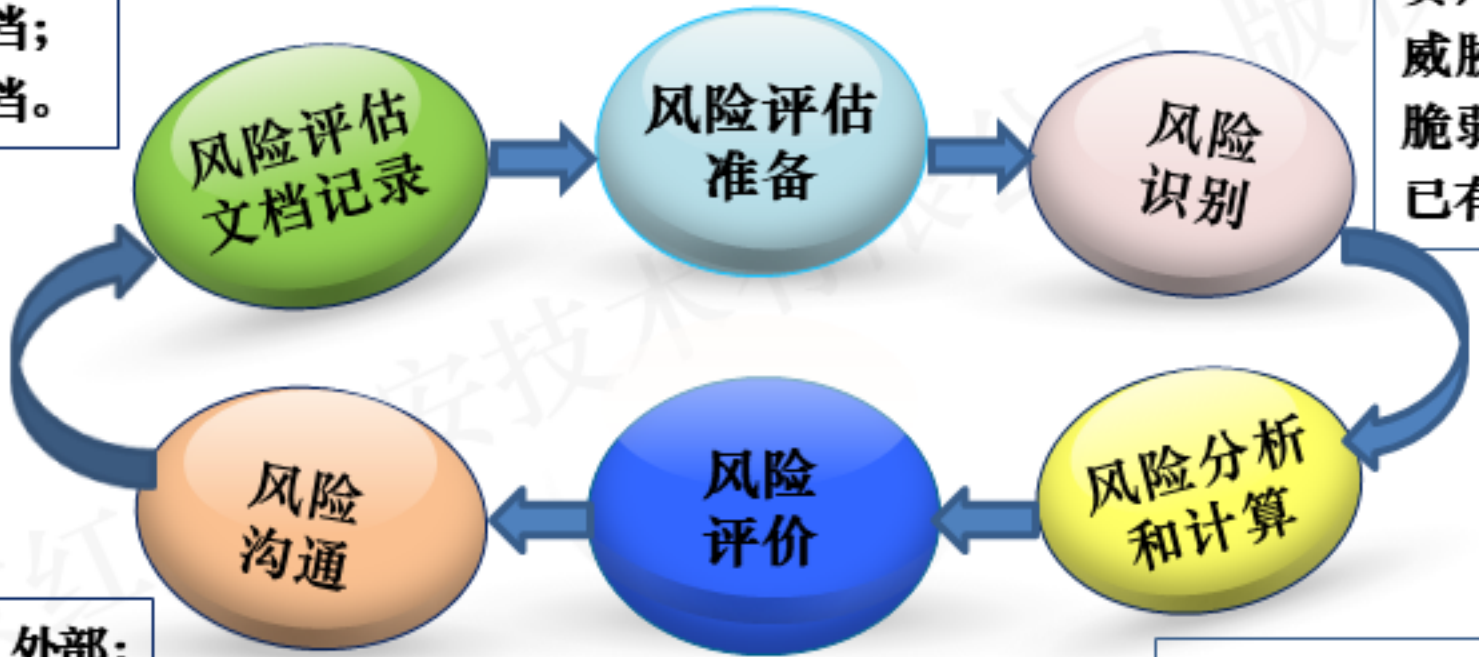
C. 脆弱性被威胁利用的可能性

√ D. 安全事件出现可能性

四、风险评估实施

内容提要：风险评估准备、风险识别、风险分析和计算、风险评价、风险沟通、风险评估文档记录、风险评估的工作形式。

风险评估实施



确定目标；组建团队；前期调研；
确定依据；制定方案；获得支持。

发展战略识别；
业务识别；
资产识别；
威胁识别；
脆弱性识别；
已有安全措施识别。

风险分析：可能性、损失、风险；
风险计算：方法、工具。

资产风险等级；业务风险等级。

内部；外部；
及时记录。

过程文档；
结果文档。

风险评估的工作形式

检查评估（上级or监管）

由信息安全主管机构或业务主管机构主导并实施的依据已经颁布的法规及标准进行的风险评估活动

委托

第三方

信息系统拥有者委托具有评估能力的专业评估机构（国家认证的风险评估机构或企业）实施的评估活动

自评估（被评估方）

自评估是信息系统拥有者依靠自身力量，对自有的信息系统进行评估的活动

委托

例题5

单选题：风险评估的工作形式有两种，即检查评估和（ ）。

A. 上级评估

B. 第三方评估

C. 监督评估

√ D. 自评估

例题6

单选题：依据《GB/T 20984》，在风险评估实施过程中，“制定评估方案”是（　）阶段的工作。。

√ A. 风险评估准备

B. 环境建立

C. 风险分析

D. 沟通与咨询

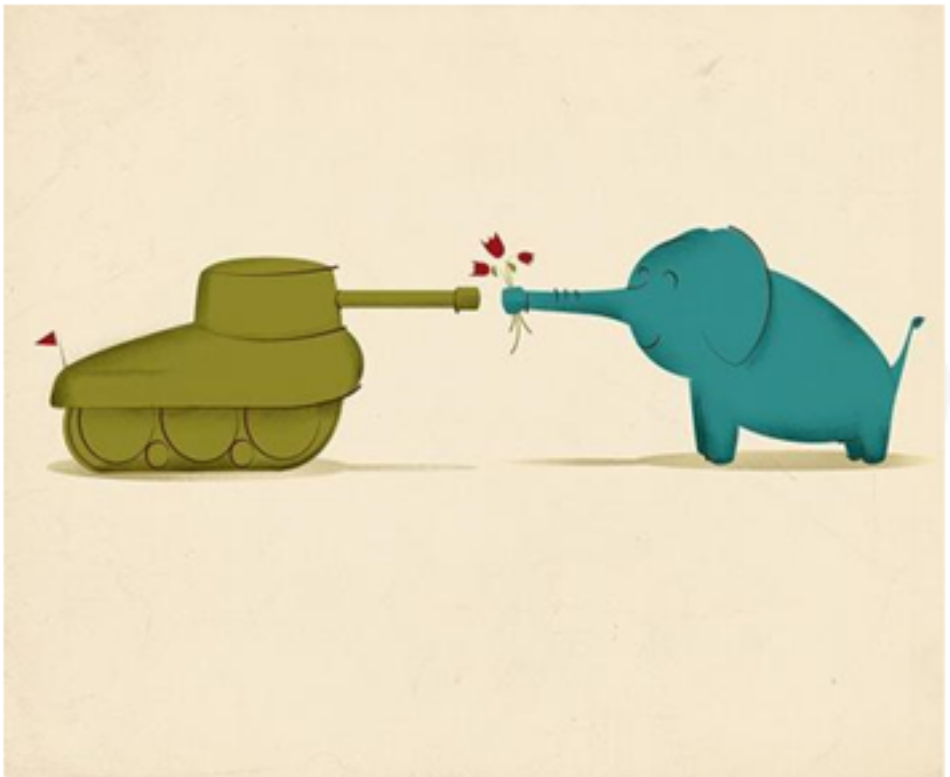
五、被评估对象生命周期不同阶段的风险评估

内容提要：规划阶段、设计阶段、实施阶段、运行阶段、废弃阶段的风险评估。

规划阶段的风险评估

- **目的**是识别被评估对象的业务战略，以支撑被评估对象安全需求及安全战略等
- **评估结果**体现在被评估对象整体规划或项目建议书中。

设计阶段的风险评估



- **目的**是对设计方案中所提供的安全功能符合性进行判断，作为实施过程风险控制的依据。
- **评估结果**体现在被评估对象需求分析报告或建设实施方案中。

实施阶段的风险评估

- **目的**是对系统开发、实施过程进行风险识别，对建成后的安全功能进行验证，在实施及验收时进行质量控制。

□开发、技术与产品获取过程

□系统交付实施过程

运行阶段的风险评估

- **目的**是了解和控制运行过程中的安全风险，是一种较为全面的风险评估。
  - 定期执行
  - 重大变更时执行

废弃阶段的风险评估

- **目的**是分析废弃资产对组织的影响，制定处理方式。
  - 处理过程有效监督
  - 人员进行安全教育

例题7

多选题：执行运行阶段的风险评估，触发点可以包括（ ）。

√ A. 定期

√ B. 业务流程发生重大变更

√ C. 发生重大安全事件

√ D. 组织结构发生重大变动

第6课小结

内容提要：本节课需要了解哪些内容？应该掌握哪些知识？

第6课小结

- 了解我国信息安全风险评估的发展史。
- 了解GB/T 20984的设计思想，掌握风险评估原则。
- 理解风险评估的框架和流程。
- 理解风险评估的实施并运用于实际项目中。
- 理解被评估对象生命周期不同阶段的风险评估。

典型例题

简答题：请简要描述信息安全风险的相关要素，以及它们之间的关系。

1. 信息安全风险的要素包括：战略、业务、资产、威胁、脆弱性、安全措施、风险。
2. 要素之间关系：
3. 组织的发展战略依赖业务实现，业务重要性与其在战略中所处的地位相关；
4. 业务的开展需要资产作为支撑，而资产会暴露出脆弱性；
5. 安全措施可抵御威胁、控制风险；
6. 风险会影响资产；
7. 威胁利用脆弱性会危害资产和业务；
8. 风险的分析与计算，应综合考虑业务、资产、脆弱性、威胁和安全措施等基本因素。

谢谢观看！

北京红戎信安技术有限公司
2022年1月