# 实践 1 信息安全风险评估实践

## 1. 实践目标

(1) 掌握信息安全风险评估的流程；
(2) 掌握信息安全风险评估的具体实践方法；
(3) 通过风险评估发现目标信息系统在技术、管理方面的安全漏洞；
(4) 学习制定安全整改方案，并明确如何在安全建设中运用 IBM Tivoli 产品解决某类安全问题；
(5) 学习编写信息安全风险评估的各类文档。

## 2. 环境与工具

(1) 企业、政务、事业单位等机构的信息系统

本实验以企业、政务、事业单位等机构的真实信息系统作为评估对象，涉及与信息系统相关的物理环境安全、网络安全、主机安全（包括数据库系统安全）及安全管理方面。

(2) 信息安全风险评估工具

本实验的风险评估工具主要包括：调查问卷、检查清单、漏洞扫描工具等。

调查问卷——通过问卷形式对组织信息安全的各个方面进行调查，从问卷调查中，评估者能够了解到组织的关键业务、关键资产、主要威胁、管理上的缺陷、采用的控制措施和安全策略的执行情况。

检查清单——检查清单通常是基于特定基准或基线建立的对特定系统进行审查的项目条款，包括物理环境、操作系统、数据库系统、中间件、网络设备和安全设备几个方面。通过检查列表，操作者可以快速定位系统目前的安全状况与基线要求之间的差距。调查表和检查清单列表见附录 1。

漏洞扫描工具——漏洞扫描通常是指基于漏洞数据库，通过扫描等手段，对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用的漏洞的一种安全检测（渗透攻击）行为。漏洞扫描器可以对信息系统中存在的技术性漏洞（弱点）进行检测，给出已发现漏洞的严重性和风险值。当前主流的工具有 Nessus、X-Scan、Nmap、极光、天镜等。

(3) 评估报告模板

本实验为方便学生编写报告，提供了部分评估报告模板，学生可根据需要采用或改进。评估保护模板列表见附件 2。

## 3. 组织方式

4-6 人一组，分工合作。人员分工情况大致如下：

(1) 设组长 1 名，作为与实践教师、实践单位的接口人。组长负责制定项目实施方案，分配实践任务，控制项目进度，并对报告编写任务进行合理分配。
(2) 由 1~2 人负责信息系统前期调研，了解组织关键业务情况、资产情况，及采取的技术和管理措施现状。
(3) 根据人员知识侧重点不同，可分为技术评估和管理评估人员，技术评估人员按照检查清单分别对物理环境、操作系统（包括 Windows, Unix, Linux）、数据库系统（SQL Server, Oracle, DB2, Sybase, MySQL 等）、中间件（Tomcat, Apache, IIS, Weblogic, WebShpere 等）、网络设备（路由器、交换机等）、安全设备（防火墙，IPS，IDS 等）等进行检查并完成相应的检查报告；管理评估人员主要负责安全管理方面的访谈工作，并完成相应的评估报告。

(4) 安排人员负责安全整改方案的具体制定工作。

## 4. 关键环节

### 4.1 准备阶段

(1) 成立风险评估项目组，明确组织领导及协调人员，确定项目组织结构及相关各方职责；
(2) 收集被评估单位及信息系统相关资料文档；
(3) 确定项目实施具体范围、工作要求及工作安排；
(4) 准备项目实施现场的实施环境。

### 4.2 实施阶段

#### 4.2.1 资产识别

对被评估信息系统的关键资产进行识别，并合理分类；在资产识别过程中，需要详细识别核心资产的安全属性，重点识别出资产在遭受泄密、中断、损害等破坏时所遭受的影响，为资产影响分析及综合风险分析提供参考数据。

工作方式：资产识别会议、相关调查表填写、相关资料的审查确认。

#### 4.2.2 威胁识别

威胁评估涉及管理、技术等多个方面。通过威胁调查、取样等手段识别被评估信息系统的关键资产所面临的威胁源，及其威胁所常采用的威胁方法，对资产所产生的影响，并为后续威胁分析及综合风险分析提供参考数据。

工作方式：问卷调查、人工问询、IDS 取样、日志分析（操作系统，网络设备和防火墙的日志）。

#### 4.2.3 脆弱性识别

◆ 基础环境脆弱性识别

基础环境脆弱性主要是对信息系统所处的物理环境即机房、线路、客户端的支撑设施等进行脆弱性识别，为后续脆弱性分析及综合风险分析提供参考数据。

工作方式：问卷调查、现场检查。

◆ 安全管理脆弱性识别

主要从以下几方面分析被评估信息系统：策略、组织架构、企业人员、安全控制、资产分类与控制、系统接入控制、网络与系统管理、业务可持续性发展计划、应用开发与维护及可适应性。同时为后续脆弱性分析及综合风险分析提供参考数据。

工作方式：人工问询、调查问卷、现场查看。

◆ 技术脆弱性识别

依据检查清单，对评估工作范围内的网络设备、操作系统和数据库、信息系统进行系统脆弱性评估，评估方式又分为手工检查评估和远程脆弱性识别。同时为后续脆弱性分析及综合风险分析提供参考数据。

工作方式：安全扫描、手动检查、问卷调查、人工问询。

◆ 安全措施识别

识别被评估信息系统的有效对抗风险的防护措施（包含技术手段和管理手段），同时为后续安全措施有效性分析及综合风险分析提供参考数据。

工作方式：问卷调查、人工检查。

### 4.3 分析阶段

#### 4.3.1 资产影响分析

在资产识别的基础上，进一步分析被评估信息系统及其关键资产在遭受泄密、中断、损害等破坏时对系统所承载的业务系统所产生的影响，并进行赋值量化，从而为最后综合风险分析提供参考数据。资产的保密性、完整性、可用性赋值可参照我国《信息安全风险评估指

南》或本课程配套教材、课件的说明。

4.3.2 威胁分析

在威胁识别的基础上，进一步分析被评估信息系统及其关键资产将面临哪一方面的威胁及其所采用的威胁方法，并依据其发生的可能性和成功后所产生的影响进行赋值量化，同时为最后综合风险分析提供参考数据。具体威胁类型及分类方法可参照我国《信息安全风险评估指南》或本课程配套教材、课件的说明。

4.3.3 脆弱性分析

在脆弱性识别的基础上，进一步分析被评估信息系统及其关键资产所存在的各方面脆弱性即基础环境脆弱性、安全管理脆弱性、技术脆弱性。并依据其脆弱性被利用的难易程度和被成功利用后所产生的影响进行赋值量化，从而为最后综合风险分析提供参考数据。具体的脆弱性赋值方法可参照我国《信息安全风险评估指南》或本课程配套教材、课件的说明。

4.3.4 安全措施有效性分析

对安全措施所采取后的有效性进行分析，分析其安全措施对防范威胁、降低脆弱性的有效性，从而为最后综合风险分析提供参考数据。

4.3.5 综合风险分析

在完成以上各项分析工作后，进一步分析被评估信息系统及其关键资产将面临哪一方面的威胁及其所采用的威胁方法、利用了系统的何种脆弱性，对哪一类资产产生了什么样的影响，并描述采取何种对策来防范威胁，减少脆弱性，同时将风险量化。具体的风险计算和结果判定可参照我国《信息安全风险评估指南》或本课程配套教材、课件的说明。

**4.4 规划阶段**

明确组织的安全需求，制定相应的安全规划，形成信息系统安全整改方案。安全整改方案中需对某一安全问题有所侧重，选择相应的 IBM Tivoli 工具进行改进。

**4.5 汇报验收阶段**

对项目依照考核要求进行验收，提交相关评估材料和整改方案。

## 5. 预期成果

本次项目需提交的成果包括：

(1) 《XXX 信息系统风险评估项目实施方案》

详细介绍评估项目流程，需明确的内容至少应包括：

| | |
|---|---|
| 目的 | 介绍本次风险评估的目的。 |
| 参考依据 | 介绍本次风险评估依据的标准及政策。 |
| 项目范围 | 确定本次评估的范围，如评估对象只有一个信息系统，则评估范围为该信息系统及其依赖的主机、网络设备和安全设备以及安全管理等。 |
| 项目成果 | 列出项目预计提交的成果。 |
| 项目组织 | 介绍项目的分工内容。 |
| 项目实施 | 参照本实验第 4 节内容给出项目实施流程，最好能明确各环节参与人员、被测评方人员配合工作及各阶段工作成果。 |
| 项目进度 | 制定项目实施进度。 |

(2) 《XXX 信息系统风险评估报告》

报告中应包含以下内容：

| | |
|---|---|
| 概述 | 简要介绍项目背景、目标、依据及内容。 |
| 风险评估方法和 | 确定本次风险评估的范围、评估实施流程。 |

| 内容 | |
|---|---|
| 现状概述 | 介绍信息系统的整体系统和网络架构。 |
| 资产分析 | 对评估的信息系统网络、服务器、数据、应用软件、安全设备、业务资产进行详细描述，给出资产分析结果。 |
| 威胁分析 | 介绍威胁分析依据的方法，给出分析结果。 |
| 脆弱性分析 | 对物理环境、操作系统、数据库、中间件、网络设备、安全设备和安全管理脆弱性进行分析，给出脆弱点统计结果。操作系统、数据库、中间件的脆弱性评估应包含手工检查和工具评估两部分内容。 |
| 安全措施分析 | 介绍安全措施分析依据的方法，给出分析结果。 |
| 风险分析 | 对各方面风险分析的结果进行分析、提炼。 |
| 安全综述 | 给出评估结论，确定当前信息系统的安全总体水平。如可分为良好、中等偏上、中等、中等偏下等。 |

注：报告中资产分析、威胁分析、脆弱性分析、安全措施分析和风险分析部为报告必须包含的部分，其他部分可根据项目实际情况和报告编写需要进行适当调整。

(3) 《XXX 信息系统安全建设整改方案》
整改方案中通过分析信息系统现状和保护要求，确定系统在技术和管理方面的改进内容。方案中需针对某一类安全问题，采用某种 IBM Tivoli 工具进行改进。

(4) 时间充裕的同学建议提交单独的主机人工检查报告和工具扫描报告，以及网络设备和安全设备检查报告。

**6. 考核要求**

(1) 项目提交报告的完备性和报告的质量。学生需按照上述要求完整提交项目相关报告，报告中内容真实、准确，报告语言通顺、格式统一，无低级错误。

(2) 项目的组织安排合理，项目进度控制良好。相关进度安排、人员安排需在实施方案中明确。

(3) 被评估单位的反馈意见。

**附录 1 调查表和配置检查清单列表**

资产调研表
威胁调查问卷
安全事件调查表
物理安全调查表
管理安全调查表
Windows/Linux/Solaris/AIX/Hp Unix 等操作系统检查清单
SQL Server/Oracle/DB2/Sybase/MySQL 等数据库系统检查清单
Apache/Tomcat/Weblogic/WebShpere 等中间件检查清单
网络设备和安全设备检查清单

**附录 2 评估报告模板**

风险评估项目实施方案
风险评估综合报告
操作系统、数据库、中间件、网络设备和安全设备手工检查报告