概述
高级大纲
安全性测试工程师

2016 版本

国际软件测试资质认证委员会

修订历史

版本	日期	备注
2016	2016/03/18	GA 发布

目录

致谢

本文档由国际软件测试资质认证委员会高级工作组的核心团队编写。

核心团队感谢审查小组和所有国家委员会的建议和意见。

在完成本单元的高级课程大纲时，安全性测试高级工作组有以下成员：

本课程大纲的核心团队作者：Randall Rice（主席），HughTazwell Daughtrey（副主席），Frans Dijkman，Joel Oliveira，Alain Ribault。

以下人员参加了本课程大纲的审查，评论和投票
（字母顺序）：Tarun Banga，Hugh Tazwell Daughtrey（副主席），Frans Dijkman（作者），Stefan Karsch 教授，Sebastian Malyska，Satoshi Masuda，Raine Moilanen，Joel Oliveira，Alain Ribault，Randall Rice（主席），Ian Ross，Kwangik Seo，Dave van Stein，Nor Adnan Yahaya 博士，郑文强。

此外，我们承认并感谢专家级工作组的领导和成员提供的初期和持续指导：Graham Bath（专家级工作组主席），Judy McKay（专家级工作组副主席）。

本文件于 2016 年 3 月 18 日由 ISTQB®大会正式发布。

本课程大纲概述中文版翻译参与者（按姓氏拼音排序）
程国青、胡文达、蒲冬梅、腾康、王铁昆、王帅、左平（组长）

本课程大纲概述中文版 QA 评审参与者（按姓氏拼音排序）
李华北、徐文叶

1 引言

本概述文档适用于对 ISTQB®安全性测试师高级认证（CTAL-SEC）大纲感兴趣的任何人。它提供了对大纲主要原则的高层次介绍和内容概述。

本文件定义了 CTAL-SEC 课程大纲所能塑造的业务能力。每项业务能力都是通过特定语句来说明的，这些语句表述了取得 ISTQB® CTAL-SEC 认证的人员的预期能力。它概述了正在考虑开发此级别特定安全性测试技能的公司所能获得的益处。

1.1 测试人员的职业道路

在基础级认证测试员的基础上，高级安全性测试员课程大纲的内容为专业测试人员提供了额外的技能。持有 CTAL-SEC 证书的人员将从基础级上获得的测试认知扩展到安全性测试方面的特定能力，包括方式、方法学和工具。

1.2 准入要求

为了最好地利用本大纲的内容，考生应已掌握基础大纲的学习目标，并将熟悉高级技术考试分析师课程大纲中的安全性测试概念。此外还应具有至少三年的安全性测试或相关技术测试领域的经验。

1.3 结构和课程学时

经认证的安全性测试员高级课程的最短时间为 1,110 分钟，这相当于大约 2 天，4 小时和 30 分钟的培训（基于每天 7 小时）。

1.4 受众

高级安全性测试员认证大纲面向在安全性测试方面有一定经验并希望有所提升的基础级认证测试人员。

1.5 学习目标

一般而言，CTAL-SEC 大纲在 K1 级别进行考查，即要求考生识别、记住和回忆在基础级和 CTAL-SEC 专有课程中提出的术语和概念。

K2、K3 和 K4 级别的相关学习目标在 CTAL-SEC 课程大纲内的每章开头提供。

1.6 认证名称和缩写

本认证的名称是“高级安全性测试员认证”。
首字母缩写是：“CTAL-SEC”。

1.7 标准的适用

本大纲引用了相关标准（IEEE，ISO 等）。这些引用的目的是在阅读者需要时提供额外信息的来源。请注意，只有大纲中特别引用的这些标准中的条目才会被考查。标准文件本身不适用于考查，仅供参考。

2 ISTQB® CTAL-SEC 大纲概述

2.1 业务能力

本节列出了获得 ISTQB® CTAL-SEC 认证的考生的预期业务能力。

已通过“高级安全性测试员”模块考试的高级测试人员应能够完成以下业务目标：
SEC-1 从各种角度规划、执行和评估安全性测试 - 基于策略、基于风险、基于标准、基于需求和基于漏洞。
SEC-2 将安全性测试活动与项目生命周期活动进行对接。
SEC-3 分析特定情况下风险评估技术的有效使用，以确定当前和未来的安全威胁并评估其严重程度。
SEC-4 评估现有的安全性测试套件并确定任何其他安全性测试。
SEC-5 分析一组给定的安全策略和程序以及安全性测试结果，以确定有效性。
SEC-6 对于给定的项目场景，根据功能、技术属性和已知漏洞识别安全性测试目标。
SEC-7 分析一个给定的情况，并确定哪种安全性测试方法最有可能在这种情况下取得成功。
SEC-8 识别可能需要额外或增强安全性测试的领域。
SEC-9 评估安全机制的有效性。
SEC-10 帮助组织建立信息安全意识。
SEC-11 通过发现关于目标的关键信息来展示攻击者的心态，在受保护环境中的测试应用程序上执行恶意人员会执行的操作，并了解攻击的证据如何被删除，。
SEC-12 分析给定的临时安全性测试状态报告，以确定准确性、可理解性和利益相关者适当性。
SEC-13 分析和记录需要通过一个或多个工具来解决的安全性测试。
SEC-14 根据指定的需求为给定的工具搜索分析并选择候选安全性测试工具。
SEC-15 了解使用安全性测试标准的好处以及在哪里可以找到它们。

2.2 内容

请参阅**认证测试人员高级大纲 - 安全性测试人员**文档。

3 与 CTAL-SEC 认证相关的文件

有关 ISTQB® CTAL-SEC 认证的文件如下：

- 总体概述（本文件） - 提供认证的业务能力结果
- 教学大纲 - 详细介绍 ISTQB® CTAL-SEC 的总体教学大纲
- 术语表 - 提供每章中定义的术语的定义
- 样题考试问题 - 为认证提供样例考试。
- 认可规则 - 提供培训机构在申请课程认可时应遵循的认可规则
- 考试指南 - 提供学习认证考试的客观覆盖范围的要求