



# 中华人民共和国国家标准化指导性技术文件

GB/Z 30286—2013

---

## 信息安全技术 信息系统保护轮廓和信息系统安全目标 产生指南

Information security technology—  
Guide for the production of information system  
protect profile and information system security target

2013-12-31 发布

2014-07-15 实施

---

中华人民共和国国家质量监督检验检疫总局  
中国国家标准化管理委员会 发布

## 目 次

前言 .....	III
引言 .....	IV
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 ISPP 和 ISST 概述 .....	1
4.1 ISPP 和 ISST 的用途 .....	1
4.2 ISPP 和 ISST 的内容 .....	1
4.3 ISPP 和 ISST 的目标读者 .....	4
5 ISPP 和 ISST 的产生过程 .....	4
6 ISPP 和 ISST 的描述部分 .....	5
6.1 概述 .....	5
6.2 ISPP 和 ISST 标识 .....	5
6.3 ISPP 和 ISST 概述 .....	5
6.4 ISPP 应用注解 .....	6
7 信息系统描述 .....	6
7.1 概述 .....	6
7.2 信息系统使命描述 .....	6
7.3 信息系统概要描述 .....	6
7.4 信息系统详细描述 .....	6
8 安全保障需求 .....	7
8.1 概述 .....	7
8.2 识别和说明假设 .....	7
8.3 识别和说明威胁 .....	8
8.4 识别和确定组织安全策略 .....	11
8.5 明确安全保障需求定义 .....	12
9 安全保障目的 .....	12
9.1 概述 .....	12
9.2 威胁、假设和组织安全策略的列表 .....	13
9.3 信息系统环境保障目的 .....	13
9.4 信息系统安全保障目的 .....	13
10 安全保障要求 .....	13
10.1 概述 .....	13
10.2 安全技术保障要求 .....	15
10.3 安全管理保障要求 .....	19

10.4	ISPP 或 ISST 中的安全工程保障要求 .....	20
11	信息系统概要规范 .....	22
11.1	概述 .....	22
11.2	信息系统概要规范概述 .....	22
11.3	安全保障措施的选择 .....	23
12	ISPP 声明 .....	24
12.1	概述 .....	24
12.2	ISPP 引用 .....	24
12.3	ISPP 裁剪 .....	24
12.4	ISPP 附加项 .....	24
13	符合性声明 .....	25
13.1	概述 .....	25
13.2	安全保障目的的符合性声明 .....	25
13.3	安全保障要求的符合性声明 .....	27
附录 A (资料性附录)	从 GB/T 20274.2—2008 选取 STRs .....	29
附录 B (资料性附录)	从 GB/T 20274.3—2008 选取 SMRs .....	33
附录 C (资料性附录)	从 GB/T 20274.4—2008 选取 SERs .....	36
参考文献	.....	37

## 前 言

本指导性技术文件按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本指导性技术文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本指导性技术文件主要起草单位：中国信息安全测评中心、中国信息安全测评中心华中测评中心、华北计算技术研究所。

本指导性技术文件主要起草人：江常青、张利、姚轶焱、佟鑫、彭勇、陆丽、胡卫华、付敏、周瑾。

## 引 言

本指导性技术文件是 GB/T 20274《信息安全技术 信息系统安全保障评估框架》系列标准的配套指南文件,为信息系统保护轮廓(Information System Protect Profile, ISPP)和信息系统安全目标(Information System Security Target, ISST)的编制提供指导。

本指导性技术文件的使用者应熟悉 GB/T 20274 系列标准。

# 信息安全技术

## 信息系统保护轮廓和信息系统安全目标 产生指南

### 1 范围

本指导性技术文件给出了编制信息系统保护轮廓(ISPP)和信息系统安全目标(ISST)的过程,为编写 ISPP 和 ISST 提供指导。

本指导性技术文件适用于应用 GB/T 20274 系列标准进行信息系统安全性保障评估的评估者和确认评估者行为的认证者、系统开发者等。

### 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 20274.1—2006	信息安全技术	信息系统安全保障评估框架	第 1 部分:简介和一般模型
GB/T 20274.2—2008	信息安全技术	信息系统安全保障评估框架	第 2 部分:技术保障
GB/T 20274.3—2008	信息安全技术	信息系统安全保障评估框架	第 3 部分:管理保障
GB/T 20274.4—2008	信息安全技术	信息系统安全保障评估框架	第 4 部分:工程保障
GB/T 20984—2007	信息安全技术	信息安全风险评估规范	

### 3 术语和定义

GB/T 20274.1—2006、GB/T 20274.2—2008、GB/T 20274.3—2008、GB/T 20274.4—2008 界定的术语和定义适用于本文件。

### 4 ISPP 和 ISST 概述

#### 4.1 ISPP 和 ISST 的用途

GB/T 20274 系列标准的主要用途是表达信息系统的安全保障要求。信息系统有许多不同的种类,每个信息系统运行于特定的现实环境中,受到来自于组织内部与外部环境的约束。因此对于不同的信息系统,通常有不同的安全保障要求。

GB/T 20274.1—2006 中用 ISPP 和 ISST 来表达某一类信息系统和某一个特定信息系统的安全保障要求。信息系统的所有者运用 ISPP 来描述某一类信息系统标准化、结构化和规范化的安全保障需求。信息系统的开发者依据 ISPP 针对特定的信息系统编制相应的 ISST,描述其特定用户系统的安全保障需求以及对 ISPP 的满足情况。

#### 4.2 ISPP 和 ISST 的内容

GB/T 20274.1—2006 的图 A.1 描述了 ISPP 中所要求的内容条目。表 1 是推荐使用的 ISPP 样本