ICS 35.020
L 01

中华人民共和国国家标准

GB/T 19668.4—2017
代替 GB/T 19668.6—2007

信息技术服务　监理
第4部分:信息安全监理规范

Information technology service—Surveillance—
Part 4:Information security surveillance specification

2017-07-31 发布　　2018-02-01 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

GB/T 19668《信息技术服务　监理》分为六部分：

——第1部分：总则；

——第2部分：基础设施工程监理规范；

——第3部分：运行维护监理规范；

——第4部分：信息安全监理规范；

——第5部分：软件工程监理规范；

——第6部分：应用系统：数据中心工程监理规范。

本部分为GB/T 19668的第4部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 19668.6—2007《信息化工程监理规范　第6部分：信息化工程安全监理规范》，与GB/T 19668.6—2007相比，主要技术变化如下：

——术语中增加了“信息安全、信息安全监理”、“安全工程”、“风险评估”、“安全需求”、“等级保护”、“安全控制措施”、“合规性”和“安全策略”，共9条定义（见3.2～3.9）；

——删除了术语中的信息化工程安全监理；

——新增规划设计部分，包括目标、内容、要点（见第5章）；

——将原标准中工程招标阶段、工程设计阶段、工程实施阶段和工程验收阶段纳入部署实施部分（见第6章）；

——修改了工程招标阶段的监理目标、监理内容、监理要点（见6.1.1、6.1.2和6.1.3）；

——修改了工程设计阶段的监理目标、监理内容、监理要点（见6.2.1、6.2.2和6.2.3）；

——将原标准工程设计阶段监理要点中的“安全需求分析”删除，将原“工程设计方案”细分为“体系结构设计”和“详细设计”（见6.2.3.1和6.2.3.2）；

——修改了工程实施阶段的监理目标、监理内容、监理要点（见6.3.1、6.3.2和6.3.3）；

——工程实施阶段监理要点中的“工程实施方案和工程实施组织方案”修改为“工程实施方案”（见6.3.3.1），增加了“安全控制措施”（见6.3.3.2），修改了“安全设备验收”具体内容（见6.3.3.3），将“工程实验管理”修改为“工程实施中的安全管理”（见6.3.3.4）；

——修改了工程验收阶段的监理目标、监理内容、监理要点（见6.4.1、6.4.2和6.4.3）；

——工程验收阶段监理要点中删除了“信息系统安全测评”，增加“工程验收方案”（见6.4.3.2），将“工程验收”修改为“工程验收管理”（见6.4.3.3）；

——删除了原标准中“各类信息化工程的安全监理要点”；

——增加了规范性附录信息系统工程安全合规性要求（见附录A）；

——增加了规范性附录信息系统工程安全技术要求（见附录B）；

——增加了资料性附录信息系统工程安全监理工作表单（见附录C）。

请注意本文件的某些内容可能涉及的专利。本文件的发布机构不承担标识这些专利的责任。

本部分由全国信息技术标准化技术委员会（SAC/TC 28）提出并归口。

本部分主要起草单位：中国电子技术标准化研究院、上海三零卫士信息安全有限公司、北京交通大学、成都安美勤信息技术股份有限公司、山东正中计算机网络技术咨询有限公司、北京中百信工程咨询有限公司、武汉实为咨询监理有限公司、大连鸿润信息系统工程监理有限公司、北京希达建设监理有限责任公司、惠州市亿信通信息技术服务有限公司、新疆天衡信息系统咨询管理有限公司、北京联海信息

系统有限公司、北京中保天和信息科技有限公司、北京中宏信科技有限公司、深圳市艾泰克工程咨询监理有限公司。

本部分主要起草人：邬敏华、朱卫东、卓兰、曹铁舰、于惊涛、李阳、郭锐、邹晓光、杨涛、王丽、钟平、王智斌、王平、李强、葛倓、温廷祥、周筱来、李歆丽、张硕、于锋、杜晓东、黄红、祁文君、董晓杰、朱晓娟、贾卓生、葛迺康。

本部分所代替标准版本的历次发布情况为：

——GB/T 19668.6—2007。

信息技术服务　监理
第4部分:信息安全监理规范

1　范围

GB/T 19668的本部分规定了信息系统工程新建、升级、改造过程中各阶段信息安全监理工作的主要目标、内容和要点。

本部分适用于在信息系统工程建设规划设计、招标、设计、实施和验收阶段中提供有关信息安全的监督管理。

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 9361—2011　计算机场地安全要求

GB/T 19668.1—2014　信息技术服务　监理　第1部分:总则

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 19668.1—2014界定的以及下列术语和定义适用于本文件。

3.1

信息安全　information security

保持信息的保密性、完整性、可用性;另外也可包括诸如真实性、可核查性、不可否认性和可靠性等。

[GB/T 22081—2008,定义2.5]

3.2

信息安全监理　information security surveillance

依据信息安全方面的标准和要求,在工程建设各阶段向业主单位提供相关咨询,并协助业主单位对承建单位在工程建设中的信息安全实施服务,实施控制和管理的一种专业化服务活动。信息安全监理还可以包括对信息系统运维阶段的其他信息安全实施服务进行监理。

[GB/T 30283—2013,定义6.13]

3.3

安全工程　security engineering

为确保信息系统的保密性、完整性、可用性等目标而进行的系统工程过程。

[GB/T 20282—2006,定义3.1]

注:安全工程的例子包括信息系统工程(含云服务类的信息系统)建设和运维阶段的安全集成。

3.4

风险评估　risk assessment

依据有关信息安全技术与管理标准,对信息系统及其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可