



国际标准

**ISO/IEC 27017**

信息技术 安全技术 基于 ISO/IEC 27002  
的云服务信息安全控制实施规范  
(Information technology—Security  
techniques—Code of practice for  
information security controls based on  
ISO/IEC 27002 for cloud services)

第一版  
2015-12

## 目录

引言 .....	3
1. 范围 .....	4
2. 规范性引用文件 .....	4
2.1 等同建议/国际标准 .....	4
2.2 补充引用文件 .....	4
3. 术语和定义 .....	4
3.1 其他文件中定义的术语 .....	4
3.2 缩写 .....	5
4. 云领域特定概念 .....	5
4.1 概述 .....	5
4.2 云服务中的供应商关系 .....	5
4.3 云服务客户与云服务提供商之间的关系 .....	6
4.4 云服务中的信息安全风险管理 .....	6
4.5 本标准的结构 .....	6
5. 信息安全策略 .....	7
5.1 信息安全管理方向 .....	7
6. 信息安全组织 .....	8
6.1 内部组织 .....	8
6.2 移动设备和远程办公 .....	9
7. 人力资源安全 .....	9
7.1 入职前 .....	9
7.2 在职期间 .....	9
7.3 离职和岗位变动 .....	10
8. 资产管理 .....	10
8.1 资产责任 .....	10
8.2 信息分类 .....	11
8.3 介质处理 .....	11
9. 访问控制 .....	11
9.1 访问控制的业务要求 .....	11
9.2 用户访问管理 .....	12
9.3 用户职责 .....	13
9.4 系统和应用程序访问控制 .....	13
10. 密码学 .....	14
10.1 密码控制 .....	14
11. 物理和环境安全 .....	15
11.1 安全区域 .....	15
11.2 设备 .....	15
12. 运行安全 .....	16
12.1 运行程序和职责 .....	16
12.2 恶意软件防护 .....	17
12.3 备份 .....	17
12.4 日志记录和监控 .....	17
12.5 运行软件控制 .....	18

12.6 技术漏洞管理 .....	19
12.7 信息系统审核考虑 .....	19
13. 通信安全 .....	19
13.1 网络安全管理 .....	19
13.2 信息传输 .....	20
14 系统获取、开发和维护 .....	20
14.1 信息系统的安全要求 .....	20
14.2 开发与支持流程中的安全 .....	20
14.3 测试数据 .....	21
15 供应商关系 .....	21
15.1 供应商关系中的信息安全 .....	21
15.2 供应商服务交付管理 .....	22
16 信息安全事件管理 .....	23
16.1 信息安全事件管理与改进 .....	23
17 业务连续性管理 .....	24
17.1 信息安全连续性 .....	24
17.2 冗余 .....	24
18 合规性 .....	24
18.1 遵守法律法规和合同要求 .....	24
18.2 信息安全评审 .....	26
附录 A .....	27
附录 B .....	30
参考文献 .....	32