

关于《网络安全等级保护基本要求 第一部分：安全通用要求》标准解析

上海安言信息技术有限公司
上海市长宁区长宁路855号8楼B座
021-62101209

关于我们

上海安言信息技术有限公司

安言咨询，始建于2004年，是国内最早也是最大的信息安全专业咨询机构。总部上海，业务涉及北上广多地，面向金融、电力、通讯、央企、全球五百强等重点行业和企业。专注为客户提供信息安全意识培训、产品解决方案及技术服务、管理体系建设、IT风险管治、IT战略发展规划等专业化的咨询服务。

第一张世界500强BS7799证书

第一张银行业ISO27001证书

第一张运营商ISO27001证书

第一张电力ISO27001及ISO20000双体系证书

首家CISSP注册信息系统安全师认证培训机构

数据安全、应用安全、基础设施安全服务提供者

信息安全意识提升推动者

信息安全产业发展见证者

公司资质

中国信息安全测评中心信息安全服务资质证书

中国信息安全认证中心信息安全服务资质证书

国家信息安全测评授权培训机构资质证书

计算机软件著作权等级证书

高新企业认定证书

公司荣誉

上海市信息服务行业协会会员单位

上海市信息安全行业协会会员单位

上海市信息安全服务推荐单位

第三届上海市信息安全活动周优秀组织单位

2012年信息安全技能竞赛优秀技术支持单位

荣获上海市诚信创建企业称号

荣获2007年中国信息安全优秀管理咨询奖

认证咨询服务

ISO27001管理体系建设及认证咨询
ISO20000管理体系建设及认证咨询
ISO22301管理体系建设及认证咨询
PCI-DSS评估及认证咨询

管理咨询服务

数据全生命周期防护咨询
信息安全风险审计及合规检查咨询
信息安全管理体系优化咨询
IT多管理体系融合咨询
信息安全有效性测量咨询
信息安全合规管理咨询
IT风险管理整体规划咨询
信息安全风险管理及流程优化咨询

IT风险管理平台

IT-GRC风险管理
IT-GRC合规管理
IT-GRC制度管理
IT-GRC审计检查管理
IT-GRC意识培训

意识培训服务

信息安全意识导入服务
信息安全意识培训服务
信息安全意识材料定制服务
信息安全技术能力提升培训服务



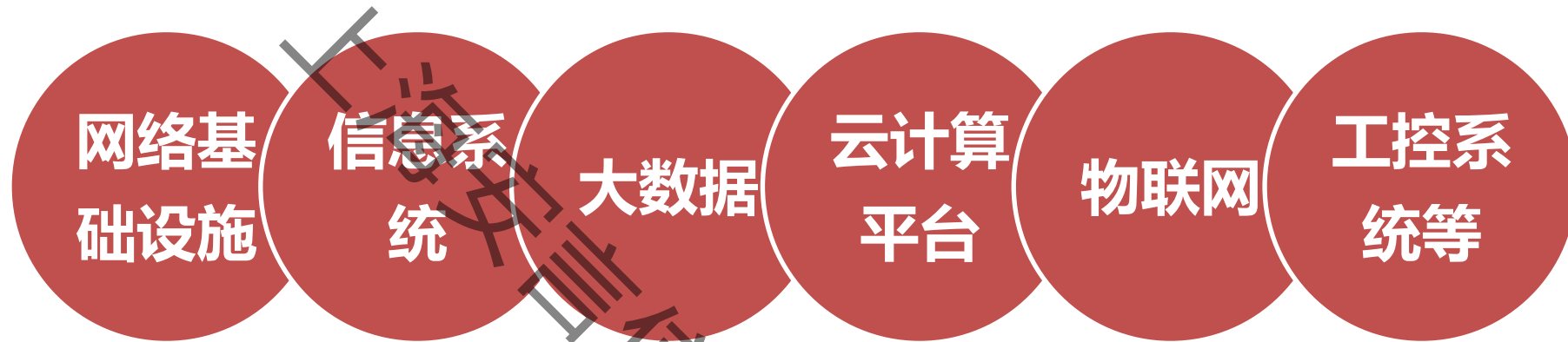
目录

CONTENTS

- [1] 概述
- [2] 技术要求和管理要求
- [3] 升版变化
- [4] 云计算安全扩要求
- [5] 移动互联安全扩展要求
- [6] 物联网安全扩展要求
- [7] 工业控制系统安全扩展要求

上海安言信息技术有限公司

【1】 概述



受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

技术类安全要求与提供的技术安全机制有关，主要通过部署软硬件并正确的配置其安全功能来实现

管理类安全要求与各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现

技术要求

管理要求

安全保护能力

第一级:用户自主保护级

第二级:系统审计保护级

第三级:安全标记保护级

第四级:结构化保护级

第五级:访问验证保护级

G的级别与系统级别一致

S和A的级别根据对象不同、关注重点不同可以适当降低级别要求

保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改的信息安全类要求（简记为S）

保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保障类要求（简记为A）

其他通用安全保护类要求（简记为G）

行业要求

安全保护等级	定级结果的组合
第一级	S1A1G1
第二级	S1A2G2 , S2A2G2 , S2A1G2
第三级	S1A3G3 , S2A3G3 , S3A3G3 , S3A2G3 , S3A1G3
第四级	S1A4G4 , S2A4G4 , S3A4G4 , S4A4G4 , S4A3G4 , S4A2G4 , S4A1G4
第五级	S1A5G5 , S2A5G5 , S3A5G5 , S4A5G5 , S5A4G5 , S5A3G5 , S5A2G5 , S5A1G5

技术/管理	分类	安全控制点	属性标识
安全技术要求	物理和环境安全	物理位置选择	G
		物理访问控制	G
		防盗窃和防破坏	G
		防雷击	G
		防火	G
		防水和防潮	G
		防静电	G
		温湿度控制	G
		电力供应	A
	电磁防护	S	
	网络和通信安全	网络架构	G
		通信传输	G
		边界防护	G
		访问控制	G
		入侵防范	G
		恶意代码防范	G
		安全审计	G
集中管控		G	

技术/管理	分类	安全控制点	属性标识
安全技术要求	设备和计算安全	身份鉴别	S
		访问控制	S
		安全审计	G
		入侵防范	G
		恶意代码防范	G
		资源控制	A
	应用和数据安全	身份鉴别	S
		访问控制	S
		安全审计	G
		软件容错	A
		资源控制	A
		数据完整性	S
		数据保密性	S
		数据备份恢复	A
		剩余信息保护	S
		个人信息保护	S

技术/管理	分类	安全控制点	属性标识
安全管理要求	安全策略和管理制度	安全策略	G
		管理制度	G
		制定和发布	G
		评审和修订	G
	安全管理机构和人员	岗位设置	G
		人员配备	G
		授权和审批	G
		沟通和合作	G
		审核和检查	G
		人员录用	G
		人员离岗	G
		安全意识教育和培训	G
		外部人员访问管理	G

技术/管理	分类	安全控制点	属性标识
安全管理要求	安全建设管理	定级和备案	G
		安全方案设计	G
		产品采购和使用	G
		自行软件开发	G
		外包软件开发	G
		工程实施	G
		测试验收	G
		系统交付	G
		等级测评	G
		服务供应商管理	G

技术/管理	分类	安全控制点	属性标识
安全管理要求	安全运维管理	环境管理	G
		资产管理	G
		介质管理	G
		设备维护管理	G
		漏洞和风险管理	G
		网络与系统安全管理	G
		恶意代码防范管理	G
		配置管理	G
		密码管理	G
		变更管理	G
		备份与恢复管理	G
		安全事件处置	G
应急预案管理	G		

[2] **技术要求和
管理要求**

上海安言信息技术有限公司

	技术要求	第一级	第二级	第三级	第四级
物理和环境安全	地理位置选择	0	2	2	2
	物理访问控制	1	1	1	2
	防盗窃和防破坏	1	2	3	3
	防雷击	1	1	2	2
	防火	1	2	3	3
	防水和防潮	1	2	3	3
	防静电	0	1	2	2
	温湿度控制	1	1	1	1
	电力供应	1	2	3	4
	电磁防护	0	1	2	2
网络和通信安全	网络架构	2	4	5	6
	通信传输	1	1	2	4
	边界防护	1	1	4	5
	访问控制	3	4	5	3
	入侵防范	0	1	4	4
	恶意代码防范	0	0	2	2
	安全审计	0	3	5	4
	集中管控	0	0	6	6

技术要求		第一级	第二级	第三级	第四级
设备和计算安全	身份鉴别	2	3	4	4
	访问控制	3	4	7	7
	安全审计	0	3	5	5
	入侵防范	2	4	5	5
	恶意代码防范	1	1	1	1
	资源控制	0	1	4	4
应用和数据安全	身份鉴别	2	4	5	6
	访问控制	3	3	7	7
	安全审计	0	3	5	5
	软件容错	1	2	3	3
	资源控制	0	3	4	4
	数据完整性	1	1	2	3
	数据保密性	0	0	2	3
	数据备份恢复	1	2	3	4
	剩余信息保护	0	1	2	2
	个人信息保护	0	2	2	2

管理要求		第一级	第二级	第三级	第四级
安全策略和管理制度	安全策略	0	0	1	1
	管理制度	1	2	3	3
	制定和发布	0	2	2	2
	评审和修订	0	1	1	1
安全管理机构和人员	岗位设置	1	2	3	3
	人员配备	1	1	2	3
	授权和审批	1	2	3	3
	沟通和合作	0	3	3	2
	审核和检查	0	1	3	3
	人员录用	1	2	3	4
	人员离岗	1	1	2	2
	安全意识教育和培训	1	1	2	2
	外部人员访问管理	1	3	4	5

管理要求		第一级	第二级	第三级	第四级
安全建设管理	定级和备案	1	4	4	4
	安全方案设计	1	3	3	3
	产品采购和使用	1	2	3	4
	自行软件开发	0	2	7	7
	外包软件开发	0	0	3	3
	工程实施	1	2	3	3
	测试验收	1	2	2	2
	系统交付	2	3	3	3
	等级测评	0	3	3	3
	服务供应商选择	2	2	3	3
	安全运维管理	环境管理	2	3	3
资产管理		0	1	3	3
介质管理		1	2	2	2
设备维护管理		1	2	4	4
漏洞和风险管理		1	1	2	2
网络和系统安全管理		2	5	9	9
恶意代码防范管理		2	2	3	3
配置管理		0	1	2	2
密码管理		0	2	1	1
变更管理		0	1	3	3
备份与恢复管理		2	3	3	3
安全事件处置		2	3	4	4
应急预案管理		0	3	4	4
外包运维管理		0	2	4	4

[3] 升版变化

上海安言信息技术有限公司

GB/T 22239-2008
信息安全技术 信息系统
安全等级保护基本要求

GB/T 22239.1-2017 信息安全技术 网络安全等级保护基本要求 第1部分 安全通用要求



GB/T 22239.2-2017 信息安全技术 网络安全等级保护基本要求 第2部分 云计算安全扩展要求

GB/T 22239.3-2017 信息安全技术 网络安全等级保护基本要求 第3部分 移动互联安全扩展要求

GB/T 22239.4-2017 信息安全技术 网络安全等级保护基本要求 第4部分 物联网安全扩展要求

GB/T 22239.5-2017 信息安全技术 网络安全等级保护基本要求 第5部分 工业控制安全扩展要求

GB/T 22239.6-2017 信息安全技术 网络安全等级保护基本要求 第6部分 大数据安全扩展要求

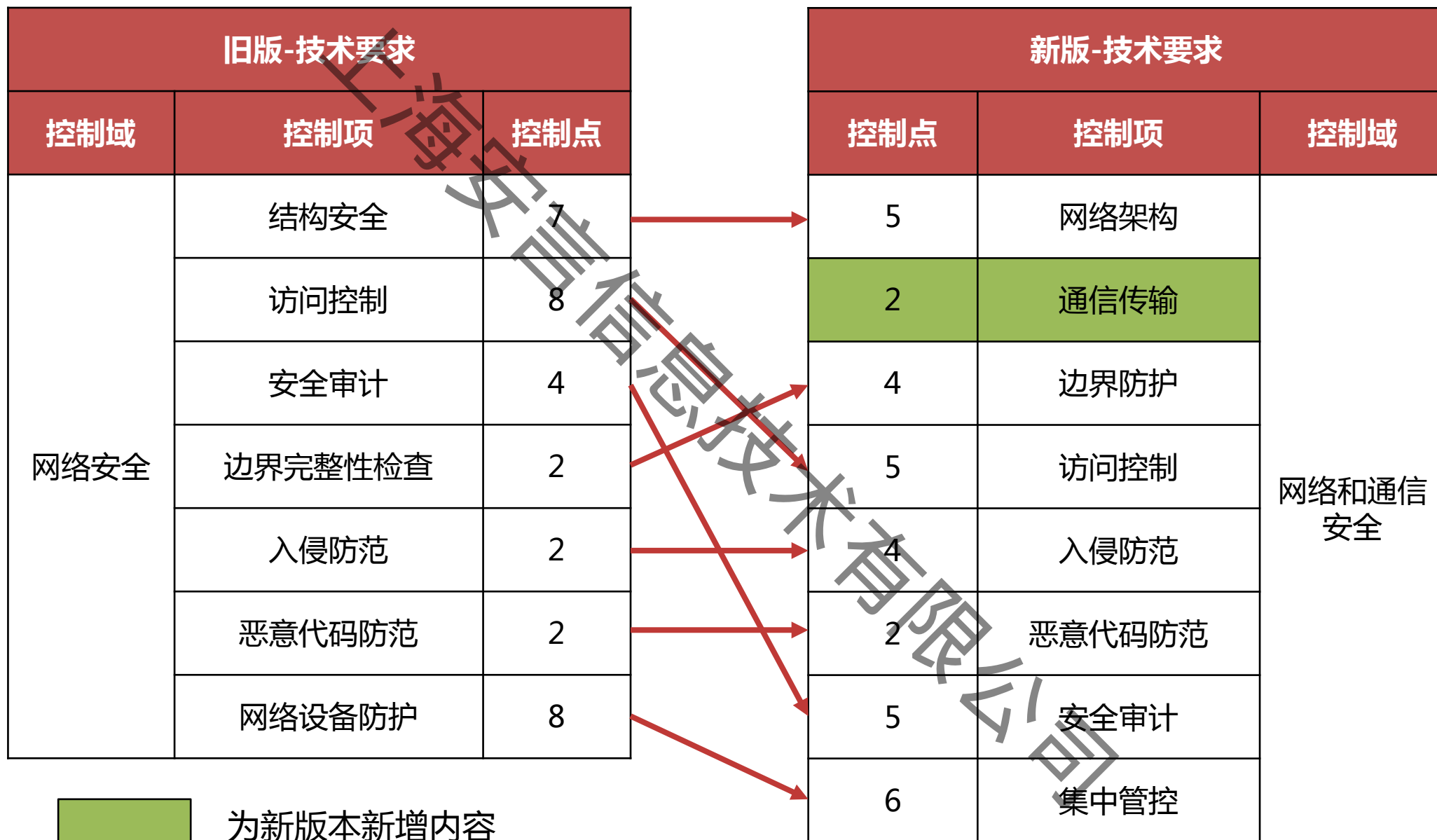
旧版	
技术要求	物理安全
	网络安全
	主机安全
	应用安全
	数据安全及备份恢复
管理要求	安全管理制度
	安全管理机构
	人员安全管理
	系统建设管理
	系统运维管理

新版	
物理和环境安全	技术要求
网络和通信安全	
设备和计算安全	
应用和数据安全	
安全策略和管理制度	
安全管理机构和人员	
安全建设管理	
安全运维管理	

旧版-技术要求			新版-技术要求		
控制域	控制项	控制点	控制点	控制项	控制域
物理安全	物理位置的选择	2	→	2	物理和环境安全
	物理访问控制	4	→	1	
	防盗窃和防破坏	6	→	3	
	防雷击	3	→	2	
	防火	3	→	3	
	防水和防潮	4	→	3	
	防静电	2	→	2	
	温湿度控制	1	→	1	
	电力供应	4	→	3	
	电磁防护	3	→	2	

控制项内容发生变化

控制项内容未发生变化



旧版-技术要求			新版-技术要求		
控制域	控制项	控制点	控制点	控制项	控制域
主机安全	身份鉴别	7	4	身份鉴别	设备和计算安全
	访问控制	7	7	访问控制	
	安全审计	6	5	安全审计	
	剩余信息保护	2	5	入侵防范	
	入侵防范	3	1	恶意代码防范	
	恶意代码防范	3	4	资源控制	
	资源控制	5			

 为旧版删除控制项

旧版-技术要求			新版-技术要求		
控制域	控制项	控制点	控制点	控制项	控制域
应用安全	身份鉴别	5	5	身份鉴别	应用和数据安全
	访问控制	6	7	访问控制	
	安全审计	4	5	安全审计	
	剩余信息保护	2	3	软件容错	
	通信完整性	1	4	资源控制	
	通信保密性	2	2	数据完整性	
	抗抵赖	2	2	数据保密性	
	软件容错	2	3	备份和恢复	
	资源控制	7	2	剩余信息保护	
数据安全及备份恢复	数据完整性	2	2	个人信息保护	
	数据保密性	2			
	备份和恢复	4			

为新版本新增内容

旧版-管理要求			新版-管理要求		
控制域	控制项	控制点	控制点	控制项	控制域
安全管理制度	管理制度	4	→	1	安全策略和 管理制度
	制定和发布	5		3	
	评审和修订	2		2	
安全管理机构	岗位设置	4	→	1	安全管理机 构和人员
	人员配备	3		3	
	授权和审批	4		2	
	沟通和合作	5		3	
	审核和检查	4		3	
人员安全管理	人员录用	4	→	3	安全管理机 构和人员
	人员离岗	3		3	
	人员考核	3		2	
	安全意识教育和培训	4		2	
	外部人员访问管理	2		4	

旧版-管理要求			新版-管理要求		
控制域	控制项	控制点	控制点	控制项	控制域
系统建设管理	系统定级	4	4	定级和备案	安全建设管理
	安全方案设计	5	3	安全方案设计	
	产品采购和使用	4	3	产品采购和使用	
	自行软件开发	5	7	自行软件开发	
	外包软件开发	4	3	外包软件开发	
	工程实施	3	3	工程实施	
	测试验收	5	2	测试验收	
	系统交付	5	3	系统交付	
	系统备案	3	3	等级测评	
	等级测评	4	3	服务供应商选择	
	安全服务商选择	3			

旧版-管理要求			新版-管理要求			
控制域	控制项	控制点	控制点	控制项	控制域	
系统运维管理	环境管理	4	→	3	环境管理	安全运维管理
	资产管理	4	→	3	资产管理	
	介质管理	6	→	2	介质管理	
	设备管理	5	→	4	设备维护管理	
	监控管理和安全管理中心	3	→	2	漏洞和风险管理	
	网络安全管理	8	→	9	网络和系统安全管理	
	系统安全管理	7	→	3	恶意代码防范管理	
	恶意代码防范管理	4	→	2	配置管理	
	密码管理	1	→	1	密码管理	
	变更管理	4	→	3	变更管理	
	备份与恢复管理	5	→	3	备份与恢复管理	
	安全事件处置	6	→	4	安全事件处置	
	应急预案管理	5	→	4	应急预案管理	
				→	4	

云计算

物联网

大数据

移动互联

工业控制

安全通用要求

[4]

云计算安全扩展要求

上海安言信息技术有限公司



类	子类	第一级	第二级	第三级	第四级
物理和环境安全	物理位置选择	/	扩展	扩展	扩展
	物理访问控制	继承	继承	继承	继承
	防盗窃和防破坏	继承	继承	继承	继承
	防雷击	继承	继承	继承	继承
	防火	继承	继承	继承	继承
	防水和防潮	继承	继承	继承	继承
	防静电	/	继承	继承	继承
	温湿度控制	继承	继承	继承	继承
	电力供应	继承	继承	继承	继承
	电磁防护	/	继承	继承	继承
网络和通信安全	网络架构	继承	扩展	扩展	扩展
	通信传输	继承	继承	继承	继承
	边界防护	继承	继承	继承	继承
	访问控制	继承	扩展	扩展	扩展
	入侵防范	/	扩展	扩展	扩展
	恶意代码防范	/	/	继承	继承
	安全审计	/	继承	扩展	扩展
	集中管控	/	/	继承	继承
设备和计算安全	身份鉴别	继承	扩展	扩展	扩展
	访问控制	继承	扩展	扩展	扩展
	安全审计	/	扩展	扩展	扩展
	入侵防范	继承	扩展	扩展	扩展
	恶意代码防范	继承	继承	扩展	扩展
	资源控制	/	扩展	扩展	扩展
	镜像和快照保护	/	增加	增加	增加

注：“/”代表此级别的控制点没有要求项；“继承”代表此级别的控制点要求项完全继承22239.1；“扩展”代表此级别的控制点要求项对于22239.1有扩展；“增加”代表此级别的控制点对于22239.1为新增控制点。



类	子类	第一级	第二级	第三级	第四级
应用和数据安全	身份鉴别	继承	继承	继承	继承
	访问控制	继承	继承	继承	继承
	安全审计	/	扩展	扩展	扩展
	软件容错	继承	继承	继承	继承
	资源控制	/	扩展	扩展	扩展
	接口安全	/	增加	增加	增加
	数据完整性	继承	扩展	扩展	扩展
	数据保密性	/	/	扩展	扩展
	数据备份恢复	继承	扩展	扩展	扩展
	剩余信息保护	/	继承	扩展	扩展
	个人信息保护	/	继承	继承	继承
	安全策略和管理制度	安全策略	/	/	继承
管理制度		继承	继承	继承	继承
制定和发布		继承	继承	继承	继承
评审和修订		/	继承	继承	继承
安全管理机构和人员	岗位设置	继承	继承	继承	继承
	人员配备	继承	继承	继承	继承
	授权和审批	继承	扩展	扩展	扩展
	沟通和合作	/	继承	继承	继承
	审核和检查	/	继承	继承	继承
	人员录用	继承	继承	继承	继承
	人员离岗	继承	继承	继承	继承
	安全意识教育和培训	继承	继承	继承	继承
外部人员访问管理	继承	继承	继承	继承	



类	子类	第一级	第二级	第三级	第四级
系统安全建设管理	系统定级和备案	继承	继承	继承	继承
	安全方案设计	继承	继承	扩展	扩展
	产品采购和使用	继承	继承	继承	继承
	自行软件开发	/	继承	继承	继承
	外包软件开发	/	继承	继承	继承
	工程实施	继承	继承	继承	继承
	测试验收	继承	扩展	扩展	扩展
	系统交付	继承	继承	继承	继承
	等级测评	/	继承	继承	继承
	服务供应商选择	继承	继承	继承	继承
	云服务商选择	/	增加	增加	增加
	供应链管理	/	增加	增加	增加
	系统安全运维管理	环境管理	继承	继承	继承
资产管理		/	继承	继承	继承
介质管理		继承	继承	继承	继承
设备维护管理		继承	继承	继承	继承
漏洞和风险管理		继承	继承	继承	继承
网络和系统安全管理		继承	继承	继承	继承
恶意代码防范管理		继承	继承	继承	继承
配置管理		/	继承	继承	继承
密码管理		/	继承	继承	继承
变更管理		/	继承	继承	继承
备份与恢复管理		继承	继承	继承	继承
安全事件处置		继承	继承	继承	继承
应急预案管理		/	继承	继承	继承
外包运维管理		/	继承	继承	继承
监控和审计管理		/	/	增加	增加

[5]

移动互联安全扩展要求

上海安言信息技术有限公司

类	子类	第一级	第二级	第三级	第四级
物理和环境安全	物理位置选择	扩展	扩展	扩展	扩展
	物理访问控制	继承	继承	继承	继承
	防盗窃和防破坏	继承	继承	继承	继承
	防雷击	继承	继承	继承	继承
	防火	继承	继承	继承	继承
	防水和防潮	继承	继承	继承	继承
	防静电	继承	继承	继承	继承
	温湿度控制	继承	继承	继承	继承
	电力供应	继承	继承	继承	继承
	电磁防护	继承	继承	继承	继承
	网络架构	扩展	扩展	扩展	扩展
网络和通信安全	通信传输	扩展	扩展	扩展	扩展
	边界防护	扩展	扩展	扩展	扩展
	访问控制	扩展	扩展	扩展	扩展
	入侵防范	继承	扩展	扩展	扩展
	恶意代码防范	继承	继承	继承	继承
	安全审计	继承	扩展	扩展	扩展
	集中管控	继承	继承	继承	继承
	网络设备防护	---	增加	增加	增加
设备和计算安全	身份鉴别	扩展	扩展	扩展	扩展
	移动终端管控	---	---	增加	增加
	应用管控	增加	增加	增加	增加
	访问控制	继承	继承	继承	继承
	安全审计	继承	继承	扩展	扩展
	入侵防范	扩展	扩展	扩展	扩展
	恶意代码防范	扩展	扩展	扩展	扩展
	资源控制	继承	扩展	扩展	扩展

类	子类	第一级	第二级	第三级	第四级
应用和数据安全	身份鉴别	继承	扩展	扩展	扩展
	软件审核与检测	---	增加	增加	增加
	访问控制	继承	继承	继承	继承
	安全审计	继承	继承	继承	继承
	软件容错	继承	继承	继承	继承
	资源控制	继承	继承	继承	继承
	数据完整性	扩展	扩展	扩展	扩展
	数据保密性	继承	扩展	扩展	扩展
	数据备份恢复	继承	继承	扩展	扩展
	剩余信息保护	继承	继承	继承	继承
	个人信息保护	继承	继承	继承	继承
	安全策略和管理制度	安全策略	继承	继承	继承
管理制度		扩展	扩展	扩展	扩展
制定和发布		继承	继承	继承	继承
评审和修订		继承	继承	继承	继承
安全管理机构和人员	岗位设置	扩展	扩展	扩展	扩展
	人员配备	继承	继承	扩展	扩展
	授权和审批	继承	扩展	扩展	扩展
	沟通和合作	继承	继承	继承	继承
	审核和检查	继承	继承	继承	继承
	人员录用	继承	继承	继承	继承
	人员离岗	继承	继承	继承	继承
	安全意识教育和培训	扩展	扩展	扩展	扩展
	外部人员访问管理	继承	继承	继承	继承

类	子类	第一级	第二级	第三级	第四级
安全管理机构和人员	系统定级和备案	继承	继承	继承	继承
	安全方案设计	扩展	扩展	扩展	扩展
	产品采购和使用	扩展	扩展	扩展	扩展
	自行软件开发	继承	继承	继承	继承
	移动应用软件开发	---	增加	增加	增加
	外包软件开发	继承	继承	继承	继承
	工程实施	扩展	扩展	扩展	扩展
	测试验收	扩展	扩展	扩展	扩展
	系统交付	扩展	扩展	扩展	扩展
	等级测评	继承	继承	继承	继承
	服务供应商选择	扩展	扩展	扩展	扩展
安全运维管理	环境管理	继承	继承	继承	继承
	资产管理	继承	继承	扩展	扩展
	介质管理	继承	继承	继承	继承
	设备维护管理	扩展	扩展	扩展	扩展
	漏洞和风险管理	扩展	扩展	扩展	扩展
	网络和系统安全管理	继承	继承	继承	继承
	应用软件来源管理	---	增加	增加	增加
	恶意代码防范管理	扩展	扩展	扩展	扩展
	配置管理	继承	继承	扩展	扩展
	监控和审计管理	继承	继承	增加	增加
	密码管理	继承	继承	继承	继承
	变更管理	继承	继承	继承	继承
	备份与恢复管理	扩展	扩展	扩展	扩展
	安全事件处置	继承	扩展	扩展	扩展
	应急预案管理	继承	继承	继承	继承
	外包运维管理	继承	继承	继承	继承

[6]

物联网安全扩展要求

上海安言信息技术有限公司



类	子类	第一级	第二级	第三级	第四级
物理和环境安全	物理位置选择	/	继承	继承	继承
	物理访问控制	继承	继承	继承	继承
	防盗窃和防破坏	继承	继承	继承	继承
	防雷击	继承	继承	继承	继承
	防火	继承	继承	继承	继承
	防水和防潮	继承	继承	继承	继承
	防静电	/	继承	继承	继承
	温湿度控制	继承	继承	继承	继承
	电力供应	继承	继承	继承	继承
	电磁防护	/	继承	继承	继承
	终端感知节点（包括RFID标签）	增加	增加	增加	增加
	感知层网关节点（包括RFID读写器）	增加	增加	增加	增加
网络和通信安全	网络架构	继承	继承	继承	继承
	通信传输	继承	继承	继承	继承
	边界防护	继承	继承	继承	继承
	访问控制	继承	继承	继承	继承
	入侵防范	/	继承	继承	继承
	恶意代码防范	/	/	继承	继承
	安全审计	/	继承	继承	继承
	集中管控	/	/	继承	继承
	数据源认证	增加	增加	增加	增加
	异构网安全接入	增加	增加	增加	增加
	感知设备访问控制	/	增加	增加	增加
	组认证	/	/	增加	增加
设备和计算安全	身份鉴别	继承	继承	继承	继承
	访问控制	继承	继承	继承	继承
	安全审计	/	继承	继承	继承
	剩余信息保护	/	/	继承	继承
	入侵防范	继承	继承	继承	继承
	恶意代码防范	继承	继承	继承	继承
	资源控制	/	继承	继承	继承



类	子类	第一级	第二级	第三级	第四级
设备和计算安全	集中管控	/	/	继承	继承
	终端感知节点(包括RFID标签)的设备安全	/	/	增加	增加
	感知网关节点(包括RFID读写器)的设备安全	/	/	增加	增加
应用和数据安全	访问控制	增加	增加	增加	增加
	安全审计	/	继承	继承	继承
	软件容错	继承	继承	继承	继承
	资源控制	/	继承	增加	增加
	数据完整性	增加	增加	增加	增加
	数据保密性	/	增加	增加	增加
	数据备份恢复	继承	继承	继承	继承
	剩余信息保护	/	继承	继承	继承
	个人信息保护	/	继承	继承	继承
	数据生命周期保护	/	继承	继承	继承
	数据可用性	增加	增加	增加	增加
	数据可用性	增加	增加	增加	增加
安全策略和管理制度	安全策略	/	/	继承	继承
	管理制度	继承	继承	继承	继承
	制定和发布	继承	继承	继承	继承
	评审和修订	/	继承	继承	继承
安全管理机构和人员	岗位设置	继承	继承	继承	继承
	人员配备	继承	继承	继承	继承
	授权和审批	继承	继承	继承	继承
	沟通和合作	/	继承	继承	继承
	审核和检查	/	继承	继承	继承
	人员录用	继承	继承	继承	继承
	人员离岗	继承	继承	继承	继承
	安全意识教育和培训	继承	继承	继承	继承
	外部人员访问管理	继承	继承	继承	继承



类	子类	第一级	第二级	第三级	第四级	
系统安全建设管理	安全方案设计	继承	继承	继承	继承	
	产品采购和使用	继承	继承	继承	继承	
	自行软件开发	/	继承	继承	继承	
	外包软件开发	继承	继承	继承	继承	
	工程实施	继承	继承	继承	继承	
	测试验收	继承	继承	继承	继承	
	系统交付	继承	继承	继承	继承	
	等级测评	/	继承	继承	继承	
	服务供应商选择	继承	继承	继承	继承	
	供应链管理	/	继承	继承	继承	
	自行研发感知设备 (包括RFID)	增加	增加	增加	增加	
	外包研发感知设备 (包括RFID)	增加	增加	增加	增加	
	系统安全运维管理	环境管理	继承	继承	继承	继承
		资产管理	/	继承	继承	继承
介质管理		继承	继承	继承	继承	
设备维护管理		继承	继承	继承	继承	
漏洞和风险管理		继承	继承	继承	继承	
网络和系统安全管理		继承	继承	继承	继承	
恶意代码防范管理		继承	继承	继承	继承	
配置管理		/	继承	继承	继承	
密码管理		/	继承	继承	继承	
变更管理		/	继承	继承	继承	
备份与恢复管理		继承	继承	继承	继承	
安全事件处置		继承	继承	继承	继承	
应急预案管理		/	继承	继承	继承	
外包运维管理		/	继承	继承	继承	
监控和审计管理		/	继承	继承	继承	
感知设备 (包括RFID) 环境管理		增加	增加	增加	增加	
感知设备 (包括RFID) 监控管理和安全管理中心		/	增加	增加	增加	
感知设备 (包括RFID) 备份与恢复管理		增加	增加	增加	增加	

[7]

工业控制安全扩展要求

上海安言信息技术有限公司

类	子类	第一级	第二级	第三级	第四级
网络和通信安全	网络架构	/	扩展	扩展	扩展
	通信传输	/	扩展	扩展	扩展
	无线使用控制	增加	增加	增加	增加
	访问控制	扩展	扩展	扩展	扩展
	入侵防范	/	扩展	扩展	扩展
	恶意代码防范	/	/	扩展	扩展
	安全审计	扩展	扩展	扩展	扩展
设备和计算安全	身份鉴别	扩展	扩展	扩展	扩展
	访问控制	扩展	扩展	扩展	扩展
	安全审计	沿用	沿用	沿用	沿用
	入侵防范	沿用	沿用	沿用	沿用
	恶意代码防范	扩展	扩展	扩展	扩展
	资源控制	扩展	扩展	扩展	扩展
应用和数据安全	身份鉴别	沿用	沿用	沿用	沿用
	访问控制	沿用	沿用	沿用	沿用
	安全审计	沿用	沿用	沿用	沿用
	软件容错	沿用	沿用	沿用	沿用
	资源控制	/	沿用	沿用	沿用
	数据完整性	沿用	沿用	沿用	沿用
	数据保密性	扩展	增加	扩展	扩展
	数据备份恢复	沿用	沿用	沿用	沿用
剩余信息保护	/	沿用	沿用	沿用	

类	子类	第一级	第二级	第三级	第四级
网络和通信安全	网络架构	扩展	扩展	扩展	扩展
	通信传输	/	扩展	扩展	扩展
	无线使用控制	增加	增加	增加	增加
	访问控制	扩展	扩展	扩展	扩展
	入侵防范	扩展	扩展	扩展	扩展
	恶意代码防范	/	/	/	/
	安全审计	扩展	扩展	扩展	扩展
设备和计算安全	身份鉴别	扩展	扩展	扩展	扩展
	访问控制	扩展	扩展	扩展	扩展
	安全审计	扩展	扩展	扩展	扩展
	入侵防范	扩展	扩展	扩展	扩展
	恶意代码防范	扩展	扩展	扩展	扩展
	资源控制	扩展	扩展	扩展	扩展
	身份鉴别	扩展	扩展	扩展	扩展
应用和数据安全	访问控制	扩展	扩展	扩展	扩展
	安全审计	扩展	扩展	扩展	扩展
	软件容错	扩展	扩展	扩展	扩展
	资源控制	扩展	扩展	扩展	扩展
	数据完整性	扩展	扩展	扩展	扩展
	数据保密性	增加	增加	扩展	扩展
	数据备份恢复	扩展	扩展	扩展	扩展
剩余信息保护	/	扩展	扩展	扩展	

类	子类	第一级	第二级	第三级	第四级
网络和通信安全	网络架构	扩展	扩展	扩展	扩展
	通信传输	/	扩展	扩展	扩展
	无线使用控制	增加	增加	增加	增加
	访问控制	扩展	扩展	扩展	扩展
	入侵防范	/	扩展	扩展	扩展
	恶意代码防范	/	扩展	扩展	扩展
	安全审计	扩展	扩展	扩展	扩展
设备和计算安全	身份鉴别	/	/	扩展	扩展
	访问控制	/	/	/	/
	安全审计	扩展	扩展	扩展	扩展
	入侵防范	/	扩展	扩展	扩展
	恶意代码防范	/	/	/	/
	资源控制	/	/	扩展	扩展
应用和数据安全	身份鉴别	/	/	/	/
	访问控制	/	/	/	/
	安全审计	/	/	/	/
	软件容错	/	/	/	/
	资源控制	/	/	/	/
	数据完整性	扩展	扩展	扩展	扩展
	数据保密性	/	增加	扩展	扩展
	数据备份恢复	扩展	扩展	扩展	扩展
剩余信息保护	/	/	/	/	

上海安言信信息技术股份有限公司

