

ICS 35.40

L80



中华人民共和国国家标准

GB/T 28448—20XX

代替 GB/T 28448-2012

信息安全技术 网络安全等级保护测评要求

Information security technology-

Evaluation requirement for classified cybersecurity protection

(试行稿)

(本稿完成日期：2017 年 10 月 26 日)

XXXX - XX - XX 发布

XXXX - XX - XX 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	XVII
引言	XVIII
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	4
5 等级测评概述	4
5.1 等级测评方法	4
5.2 单项测评和整体测评	4
6 第一级测评要求	5
6.1 安全测评通用要求	5
6.1.1 物理和环境安全	5
6.1.1.1 物理访问控制	5
6.1.1.2 防盗窃和防破坏	5
6.1.1.3 防雷击	5
6.1.1.4 防火	5
6.1.1.5 防水和防潮	6
6.1.1.6 温湿度控制	6
6.1.1.7 电力供应	6
6.1.2 网络和通信安全	6
6.1.2.1 网络架构	6
6.1.2.2 通信传输	7
6.1.2.3 边界防护	7
6.1.2.4 访问控制	7
6.1.3 设备和计算安全	8
6.1.3.1 身份鉴别	8
6.1.3.2 访问控制	9
6.1.3.3 入侵防范	10
6.1.3.4 恶意代码防范	10
6.1.4 应用和数据安全	11
6.1.4.1 身份鉴别	11
6.1.4.2 访问控制	11
6.1.4.3 软件容错	12
6.1.4.4 数据完整性	12
6.1.4.5 数据备份恢复	12

6.1.5	安全策略和管理制度	13
6.1.5.1	管理制度	13
6.1.6	安全管理机构和人员	13
6.1.6.1	岗位设置	13
6.1.6.2	人员配备	13
6.1.6.3	授权和审批	14
6.1.6.4	人员录用	14
6.1.6.5	人员离岗	14
6.1.6.6	安全意识教育和培训	14
6.1.6.7	外部人员访问管理	15
6.1.7	安全建设管理	15
6.1.7.1	定级	15
6.1.7.2	安全方案设计	15
6.1.7.3	产品采购和使用	16
6.1.7.4	工程实施	16
6.1.7.5	测试验收	16
6.1.7.6	系统交付	16
6.1.7.7	服务供应商管理	17
6.1.8	安全运维管理	17
6.1.8.1	环境管理	17
6.1.8.2	介质管理	18
6.1.8.3	设备维护管理	18
6.1.8.4	漏洞和风险管理	18
6.1.8.5	网络和系统安全管理	19
6.1.8.6	恶意代码防范管理	19
6.1.8.7	备份与恢复管理	20
6.1.8.8	安全事件处置	20
6.2	云计算安全测评扩展要求	21
6.2.1	网络和通信安全	21
6.2.1.1	网络架构	21
6.2.1.2	访问控制	21
6.2.2	设备和计算安全	22
6.2.2.1	镜像和快照保护	22
6.2.3	应用和数据安全	22
6.2.3.1	数据完整性	22
6.2.3.2	数据备份恢复	23
6.2.4	安全建设管理	23
6.2.4.1	云服务商选择	23
6.2.4.2	供应链管理	24
6.3	移动互联安全测评扩展要求	24
6.3.1	物理和环境安全	24
6.3.1.1	无线接入点的物理位置	24
6.3.2	网络和通信安全	24

6.3.2.1	边界防护	24
6.3.2.2	访问控制	24
6.3.3	设备和计算安全	25
6.3.3.1	移动应用管控	25
6.3.4	安全建设管理	25
6.3.4.1	移动应用软件采购	25
6.4	物联网安全测评扩展要求	25
6.4.1	物理和环境安全	25
6.4.1.1	感知节点设备物理防护	25
6.4.2	网络和通信安全	26
6.4.2.1	接入控制	26
6.4.3	安全运维管理	26
6.4.3.1	感知节点管理	26
6.5	工业控制系统安全测评扩展要求	28
6.5.1	物理和环境安全	28
6.5.1.1	室外控制设备物理防护	28
6.5.2	网络和通信安全	28
6.5.2.1	网络架构	28
6.5.2.2	访问控制	29
6.5.2.3	无线使用控制	29
6.5.3	设备和计算安全	30
6.5.3.1	控制设备安全	30
6.5.4	安全运维管理	30
6.5.4.1	漏洞和风险管理	30
7	第二级测评要求	31
7.1	安全测评通用要求	31
7.1.1	物理和环境安全	31
7.1.1.1	物理位置选择	31
7.1.1.2	物理访问控制	31
7.1.1.3	防盗窃和防破坏	32
7.1.1.4	防雷击	32
7.1.1.5	防火	32
7.1.1.6	防水和防潮	33
7.1.1.7	防静电	33
7.1.1.8	温湿度控制	33
7.1.1.9	电力供应	34
7.1.1.10	电磁防护	34
7.1.2	网络和通信安全	34
7.1.2.1	网络架构	34
7.1.2.2	通信传输	35
7.1.2.3	边界防护	36
7.1.2.4	访问控制	36

7.1.2.5	入侵防范	37
7.1.2.6	安全审计	37
7.1.3	设备和计算安全	38
7.1.3.1	身份鉴别	38
7.1.3.2	访问控制	39
7.1.3.3	安全审计	40
7.1.3.4	入侵防范	41
7.1.3.5	恶意代码防范	42
7.1.3.6	资源控制	42
7.1.4	应用和数据安全	43
7.1.4.1	身份鉴别	43
7.1.4.2	访问控制	44
7.1.4.3	安全审计	45
7.1.4.4	软件容错	46
7.1.4.5	资源控制	46
7.1.4.6	数据完整性	47
7.1.4.7	数据备份恢复	47
7.1.4.8	剩余信息保护	48
7.1.4.9	个人信息保护	48
7.1.5	安全策略和管理制度	48
7.1.5.1	安全策略（L2-PSS1-01）	48
7.1.5.2	管理制度	49
7.1.5.3	制定和发布	49
7.1.5.4	评审和修订	50
7.1.6	安全管理机构和人员	50
7.1.6.1	岗位设置	50
7.1.6.2	人员配备	50
7.1.6.3	授权和审批	51
7.1.6.4	沟通和合作	51
7.1.6.5	审核和检查	52
7.1.6.6	人员录用	52
7.1.6.7	人员离岗	53
7.1.6.8	安全意识教育和培训	53
7.1.6.9	外部人员访问管理	54
7.1.7	安全建设管理	54
7.1.7.1	定级和备案	54
7.1.7.2	安全方案设计	55
7.1.7.3	产品采购和使用	56
7.1.7.4	自行软件开发	56
7.1.7.5	外包软件开发	57
7.1.7.6	工程实施	57
7.1.7.7	测试验收	58
7.1.7.8	系统交付	58

7.1.7.9	等级测评	59
7.1.7.10	服务供应商管理	60
7.1.8	安全运维管理	60
7.1.8.1	环境管理	60
7.1.8.2	资产管理	61
7.1.8.3	介质管理	61
7.1.8.4	设备维护管理	62
7.1.8.5	漏洞和风险管理	63
7.1.8.6	网络和系统安全管理	63
7.1.8.7	恶意代码防范管理	64
7.1.8.8	配置管理	65
7.1.8.9	密码管理	65
7.1.8.10	变更管理	65
7.1.8.11	备份与恢复管理	66
7.1.8.12	安全事件处置	66
7.1.8.13	应急预案管理	67
7.1.8.14	外包运维管理	68
7.2	云计算安全测评扩展要求	68
7.2.1	物理和环境安全	68
7.2.1.1	物理位置选择	68
7.2.2	网络和通信安全	69
7.2.2.1	网络架构	69
7.2.2.2	访问控制	70
7.2.2.3	入侵防范	71
7.2.2.4	安全审计	72
7.2.3	设备和计算安全	72
7.2.3.1	身份鉴别	72
7.2.3.2	访问控制	73
7.2.3.3	安全审计	73
7.2.3.4	资源控制	73
7.2.3.5	镜像和快照保护	74
7.2.4	应用和数据安全	75
7.2.4.1	数据完整性	75
7.2.4.2	数据备份恢复	75
7.2.4.3	剩余信息保护	76
7.2.4.4	个人信息保护	76
7.2.5	安全建设管理	77
7.2.5.1	云服务商选择	77
7.2.5.2	供应链管理	78
7.2.6	安全运维管理	78
7.2.6.1	云计算环境管理	78
7.3	移动互联安全测评扩展要求	79
7.3.1	物理和环境安全	79

7.3.1.1 无线接入点的物理位置	79
7.3.2 网络和通信安全	79
7.3.2.1 边界防护	79
7.3.2.2 访问控制	79
7.3.2.3 入侵防范	80
7.3.3 设备和计算安全	81
7.3.3.1 移动应用管控	81
7.3.3.2 资源控制	82
7.3.4 安全建设管理	82
7.3.4.1 移动应用软件采购	82
7.3.4.2 移动应用软件开发	83
7.4 物联网安全测评扩展要求	83
7.4.1 物理和环境安全	83
7.4.1.1 感知节点设备物理防护	83
7.4.2 网络和通信安全	84
7.4.2.1 入侵防范	84
7.4.2.2 接入控制	85
7.4.3 安全运维管理	85
7.4.3.1 感知节点管理	85
7.5 工业控制系统安全测评扩展要求	86
7.5.1 物理和环境安全	86
7.5.1.1 室外控制设备物理防护	86
7.5.2 网络和通信安全	87
7.5.2.1 网络架构	87
7.5.2.2 通信传输	88
7.5.2.3 访问控制	88
7.5.2.4 拨号使用控制	88
7.5.2.5 无线使用控制	89
7.5.3 设备和计算安全	89
7.5.3.1 控制设备安全	89
7.5.4 安全建设管理	90
7.5.4.1 产品采购和使用	90
7.5.4.2 外包软件开发	90
7.5.5 安全运维管理	91
7.5.5.1 漏洞和风险管理	91
7.5.5.2 恶意代码防范管理	91
7.5.5.3 安全事件处置	91
8 第三级测评要求	92
8.1 安全测评通用要求	92
8.1.1 物理和环境安全	92
8.1.1.1 物理位置选择	92
8.1.1.2 物理访问控制	92

8.1.1.3	防盗窃和防破坏	93
8.1.1.4	防雷击	93
8.1.1.5	防火	94
8.1.1.6	防水和防潮	94
8.1.1.7	防静电	95
8.1.1.8	温湿度控制	96
8.1.1.9	电力供应	96
8.1.1.10	电磁防护	97
8.1.2	网络和通信安全	97
8.1.2.1	网络架构	97
8.1.2.2	通信传输	98
8.1.2.3	边界防护	99
8.1.2.4	访问控制	100
8.1.2.5	入侵防范	101
8.1.2.6	恶意代码防范	102
8.1.2.7	安全审计	103
8.1.2.8	集中管控	104
8.1.3	设备和计算安全	105
8.1.3.1	身份鉴别	105
8.1.3.2	访问控制	107
8.1.3.3	安全审计	108
8.1.3.4	入侵防范	110
8.1.3.5	恶意代码防范	111
8.1.3.6	资源控制	111
8.1.4	应用和数据安全	112
8.1.4.1	身份鉴别	112
8.1.4.2	访问控制	114
8.1.4.3	安全审计	115
8.1.4.4	软件容错	116
8.1.4.5	资源控制	117
8.1.4.6	数据完整性	118
8.1.4.7	数据保密性	119
8.1.4.8	数据备份恢复	119
8.1.4.9	剩余信息保护	120
8.1.4.10	个人信息保护	121
8.1.5	安全策略和管理制度	121
8.1.5.1	安全策略	121
8.1.5.2	管理制度	121
8.1.5.3	制定和发布	122
8.1.5.4	评审和修订	122
8.1.6	安全管理机构和人员	123
8.1.6.1	岗位设置	123
8.1.6.2	人员配备	124

8.1.6.3	授权和审批	124
8.1.6.4	沟通和合作	125
8.1.6.5	审核和检查	126
8.1.6.6	人员录用	127
8.1.6.7	人员离岗	127
8.1.6.8	安全意识教育和培训	128
8.1.6.9	外部人员访问管理	129
8.1.7	安全建设管理	130
8.1.7.1	定级和备案	130
8.1.7.2	安全方案设计	131
8.1.7.3	产品采购和使用	131
8.1.7.4	自行软件开发	132
8.1.7.5	外包软件开发	134
8.1.7.6	工程实施	134
8.1.7.7	测试验收	135
8.1.7.8	系统交付	135
8.1.7.9	等级测评	136
8.1.7.10	服务供应商管理	137
8.1.8	安全运维管理	138
8.1.8.1	环境管理	138
8.1.8.2	资产管理	139
8.1.8.3	介质管理	139
8.1.8.4	设备维护管理	140
8.1.8.5	漏洞和风险管理	141
8.1.8.6	网络和系统安全管理	142
8.1.8.7	恶意代码防范管理	144
8.1.8.8	配置管理	145
8.1.8.9	密码管理	146
8.1.8.10	变更管理	146
8.1.8.11	备份与恢复管理	147
8.1.8.12	安全事件处置	148
8.1.8.13	应急预案管理	149
8.1.8.14	外包运维管理	149
8.2	云计算安全测评扩展要求	150
8.2.1	物理和环境安全	150
8.2.1.1	物理位置选择	150
8.2.2	网络和通信安全	151
8.2.2.1	网络架构	151
8.2.2.2	访问控制	153
8.2.2.3	入侵防范	154
8.2.2.4	安全审计	156
8.2.2.5	集中管控	157
8.2.3	设备和计算安全	157

8.2.3.1	身份鉴别	157
8.2.3.2	访问控制	158
8.2.3.3	安全审计	159
8.2.3.4	入侵防范	159
8.2.3.5	资源控制	160
8.2.3.6	镜像和快照保护	161
8.2.4	应用和数据安全	162
8.2.4.1	数据完整性	162
8.2.4.2	数据保密性	162
8.2.4.3	数据备份恢复	163
8.2.4.4	剩余信息保护	164
8.2.4.5	个人信息保护	165
8.2.5	安全建设管理	165
8.2.5.1	云服务商选择	165
8.2.5.2	供应链管理	167
8.2.6	安全运维管理	168
8.2.6.1	云计算环境管理	168
8.3	移动互联安全测评扩展要求	168
8.3.1	物理和环境安全	168
8.3.1.1	无线接入点的物理位置	168
8.3.2	网络和通信安全	169
8.3.2.1	边界防护	169
8.3.2.2	访问控制	169
8.3.2.3	入侵防范	169
8.3.3	设备和计算安全	171
8.3.3.1	移动终端管控	171
8.3.3.2	移动应用管控	171
8.3.3.3	资源控制	172
8.3.4	安全建设管理	173
8.3.4.1	移动应用软件采购	173
8.3.4.2	移动应用软件开发	173
8.3.5	安全运维管理	174
8.3.5.1	配置管理	174
8.4	物联网安全测评扩展要求	174
8.4.1	物理和环境安全	174
8.4.1.1	感知节点设备物理防护	174
8.4.2	网络和通信安全	175
8.4.2.1	入侵防范	175
8.4.2.2	接入控制	176
8.4.3	设备和计算安全	176
8.4.3.1	感知节点设备安全	176
8.4.3.2	网关节点设备安全	177
8.4.4	应用和数据安全	178

8.4.4.1	抗数据重放	178
8.4.4.2	数据融合处理	179
8.4.5	安全运维管理	179
8.4.5.1	感知节点管理	179
8.5	工业控制系统安全测评扩展要求	181
8.5.1	物理和环境安全	181
8.5.1.1	室外控制设备物理防护	181
8.5.2	网络和通信安全	182
8.5.2.1	网络架构	182
8.5.2.2	通信传输	182
8.5.2.3	访问控制	183
8.5.2.4	拨号使用控制	183
8.5.2.5	无线使用控制	184
8.5.3	设备和计算安全	185
8.5.3.1	控制设备安全	185
8.5.4	安全建设管理	186
8.5.4.1	产品采购和使用	186
8.5.4.2	外包软件开发	186
8.5.5	安全运维管理	187
8.5.5.1	漏洞和风险管理	187
8.5.5.2	恶意代码防范管理	187
8.5.5.3	安全事件处置	188
9	第四级测评要求	188
9.1	安全测评通用要求	188
9.1.1	物理和环境安全	188
9.1.1.1	物理位置选择	188
9.1.1.2	物理访问控制	189
9.1.1.3	防盗窃和防破坏	190
9.1.1.4	防雷击	190
9.1.1.5	防火	191
9.1.1.6	防水和防潮	191
9.1.1.7	防静电	192
9.1.1.8	温湿度控制	192
9.1.1.9	电力供应	193
9.1.1.10	电磁防护	194
9.1.2	网络和通信安全	194
9.1.2.1	网络架构	194
9.1.2.2	通信传输	196
9.1.2.3	边界防护	196
9.1.2.4	访问控制	198
9.1.2.5	入侵防范	199
9.1.2.6	恶意代码防范	200

9.1.2.7	安全审计	200
9.1.2.8	集中管控	201
9.1.3	设备和计算安全	203
9.1.3.1	身份鉴别	203
9.1.3.2	访问控制	204
9.1.3.3	安全审计	206
9.1.3.4	入侵防范	208
9.1.3.5	恶意代码防范	209
9.1.3.6	资源控制	209
9.1.4	应用和数据安全	210
9.1.4.1	身份鉴别	210
9.1.4.2	访问控制	212
9.1.4.3	安全审计	213
9.1.4.4	软件容错	215
9.1.4.5	资源控制	216
9.1.4.6	数据完整性	216
9.1.4.7	数据保密性	217
9.1.4.8	数据备份恢复	218
9.1.4.9	剩余信息保护	219
9.1.4.10	个人信息保护	220
9.1.5	安全策略和管理制度	220
9.1.5.1	安全策略	220
9.1.5.2	管理制度	220
9.1.5.3	制定和发布	221
9.1.5.4	评审和修订	221
9.1.6	安全管理机构和人员	222
9.1.6.1	岗位设置	222
9.1.6.2	人员配备	223
9.1.6.3	授权和审批	223
9.1.6.4	沟通和合作	224
9.1.6.5	审核和检查	225
9.1.6.6	人员录用	226
9.1.6.7	人员离岗	227
9.1.6.8	安全意识教育和培训	227
9.1.6.9	外部人员访问管理	228
9.1.7	安全建设管理	229
9.1.7.1	定级和备案	229
9.1.7.2	安全方案设计	230
9.1.7.3	产品采购和使用	231
9.1.7.4	自行软件开发	232
9.1.7.5	外包软件开发	233
9.1.7.6	工程实施	234
9.1.7.7	测试验收	235

9.1.7.8	系统交付	235
9.1.7.9	等级测评	236
9.1.7.10	服务供应商管理	237
9.1.8	安全运维管理	237
9.1.8.1	环境管理	237
9.1.8.2	资产管理	239
9.1.8.3	介质管理	239
9.1.8.4	设备维护管理	240
9.1.8.5	漏洞和风险管理	241
9.1.8.6	网络和系统安全管理	242
9.1.8.7	恶意代码防范管理	244
9.1.8.8	配置管理	245
9.1.8.9	密码管理	246
9.1.8.10	变更管理	246
9.1.8.11	备份与恢复管理	247
9.1.8.12	安全事件处置	248
9.1.8.13	应急预案管理	249
9.1.8.14	外包运维管理	250
9.2	云计算安全测评扩展要求	251
9.2.1	物理和环境安全	251
9.2.1.1	物理位置选择	251
9.2.2	网络和通信安全	251
9.2.2.1	网络架构	251
9.2.2.2	访问控制	253
9.2.2.3	入侵防范	255
9.2.2.4	安全审计	257
9.2.2.5	集中管控	257
9.2.3	设备和计算安全	258
9.2.3.1	身份鉴别	258
9.2.3.2	访问控制	258
9.2.3.3	安全审计	259
9.2.3.4	入侵防范	259
9.2.3.5	资源控制	260
9.2.3.6	镜像和快照保护	262
9.2.4	应用和数据安全	262
9.2.4.1	数据完整性	263
9.2.4.2	数据保密性	263
9.2.4.3	数据备份恢复	264
9.2.4.4	剩余信息保护	265
9.2.4.5	个人信息保护	266
9.2.5	安全建设管理	266
9.2.5.1	云服务商选择	266
9.2.5.2	供应链管理	267

9.2.6	安全运维管理	268
9.2.6.1	云计算环境管理	268
9.3	移动互联安全测评扩展要求	269
9.3.1	物理和环境安全	269
9.3.1.1	无线接入点的物理位置	269
9.3.2	网络和通信安全	269
9.3.2.1	边界防护	269
9.3.2.2	访问控制	269
9.3.2.3	入侵防范	270
9.3.3	设备和计算安全	271
9.3.3.1	移动终端管控	271
9.3.3.2	移动应用管控	272
9.3.3.3	资源控制	273
9.3.4	安全建设管理	273
9.3.4.1	移动应用软件采购	273
9.3.4.2	移动应用软件开发	274
9.3.5	安全运维管理	274
9.3.5.1	配置管理	274
9.4	物联网安全测评扩展要求	274
9.4.1	物理和环境安全	274
9.4.1.1	感知节点设备物理防护	274
9.4.2	网络和通信安全	276
9.4.2.1	入侵防范	276
9.4.2.2	接入控制	276
9.4.3	设备和计算安全	277
9.4.3.1	感知节点设备安全	277
9.4.3.2	网关节点设备安全	278
9.4.4	应用和数据安全	279
9.4.4.1	抗数据重放	279
9.4.4.2	数据融合处理	279
9.4.5	安全运维管理	280
9.4.5.1	感知节点管理	280
9.5	工业控制系统安全测评扩展要求	282
9.5.1	物理和环境安全	282
9.5.1.1	室外控制设备物理防护	282
9.5.2	网络和通信安全	282
9.5.2.1	网络架构	282
9.5.2.2	通信传输	283
9.5.2.3	访问控制	283
9.5.2.4	拨号使用控制	284
9.5.2.5	无线使用控制	285
9.5.3	设备和计算安全	286
9.5.3.1	控制设备安全	286

9.5.4 安全建设管理	287
9.5.4.1 产品采购和使用	287
9.5.4.2 外包软件开发	287
9.5.5 安全运维管理	288
9.5.5.1 漏洞和风险管理	288
9.5.5.2 恶意代码防范管理	288
9.5.5.3 安全事件处置	289
10 第五级测评要求	289
11 整体测评	289
11.1 概述	289
11.2 安全控制点测评	290
11.3 安全控制点间测评	290
11.4 层面间测评	290
12 测评结论	290
12.1 各层面的测评结论	290
12.2 风险分析和评价	291
12.3 等级测评结论	291
附录 A（资料性附录） 测评力度	292
A.1 概述	292
A.2 等级测评力度	292
附录 B（规范性附录） 测评单元编号说明	294
B.1 测评单元编码规则	294
B.2 专用缩略语	294
附录 C（资料性附录） 设计要求测评验证表	295
C.1 通用安全设计要求测评验证表	295
C.1.1 第一级	295
C.1.2 第二级	297
C.1.3 第三级	301
C.1.4 第四级	309
C.2 云安全设计要求测评验证表	317
C.2.1 第一级	317
C.2.2 第二级	318
C.2.3 第三级	322
C.2.4 第四级	332
C.3 移动互联安全设计要求测评验证表	342
C.3.1 第一级	342
C.3.2 第二级	343
C.3.3 第三级	344
C.3.4 第四级	347
C.4 物联网安全设计要求测评验证表	350

C.4.1	第一级	350
C.4.2	第二级	352
C.4.3	第三级	354
C.4.4	第四级	361
C.5	工业控制系统安全设计要求测评验证表	370
C.5.1	第一级	370
C.5.2	第二级	373
C.5.3	第三级	377
C.5.4	第四级	384
附录 D (资料性附录)	测评要求和基本要求对应表	394
D.1	安全测评通用要求和基本要求对应表	394
D.1.1	第一级	394
D.1.2	第二级	395
D.1.3	第三级	399
D.1.4	第四级	405
D.2	云计算安全测评扩展要求和基本要求对应表	411
D.2.1	第一级	411
D.2.2	第二级	411
D.2.3	第三级	412
D.2.4	第四级	414
D.3	移动互联安全测评扩展要求和基本要求对应表	415
D.3.1	第一级	415
D.3.2	第二级	416
D.3.3	第三级	416
D.3.4	第四级	417
D.4	物联网安全测评扩展要求和基本要求对应表	418
D.4.1	第一级	418
D.4.2	第二级	418
D.4.3	第三级	418
D.4.4	第四级	419
D.5	工业控制系统安全测评扩展要求和基本要求对应表	419
D.5.1	第一级	420
D.5.2	第二级	420
D.5.3	第三级	420
D.5.4	第四级	421
参考文献		423

前 言

本标准按照GB/T 1.1—2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

本标准代替GB/T 28448—2012《信息安全技术 信息系统安全等级保护测评要求》。与GB/T 28448—2012相比，除编辑性修改外的主要技术变化如下：

- 标准名称由“信息安全技术 信息系统安全等级保护测评要求”变更为“信息安全技术 网络安全等级保护测评要求”。
- 每个级别增加了云计算安全测评扩展要求、移动互联安全测评扩展要求、物联网安全测评扩展要求和工业控制系统安全测评扩展要求等内容。
- 增加了等级测评、测评对象、云计算和云计算基础设施等相关术语和定义（见3，2012版的3）。
- 增加了测评单元编号说明（见附录B）、设计要求测评验证表（见附录C）及测评要求和基本要求对应表（见附录D）。
- 删除了测评框架（2012版的4.1）、关于整体测评的进一步说明（2012版的附录B）、等级测评内容（2012版的4.2）和区域间测评（2012版的10.4）等内容。
- 修改了单元测评为单项测评、规范性引用文件（见2，2012版的2）和整体测评（见11，2012版的10）等内容。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出。

本标准由全国信息安全标准化技术委员会（SAC/TC260）归口。

本标准主要起草单位：公安部第三研究所、中国电子技术标准化研究院、国家信息中心、中国科学院信息工程研究所（信息安全国家重点实验室）、北京大学、新华三技术有限公司、成都科来软件有限公司、中国移动通信有限公司研究院、北京鼎普科技股份有限公司、北京洋浦伟业科技发展有限公司、北京迅达云成科技有限公司、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、公安部第一研究所、北京信息安全测评中心、国家能源局信息中心（电力行业信息安全等级保护测评中心）、全球能源互联网研究院、北京卓识网安技术股份有限公司、中国电力科学研究院、南京南瑞集团公司、国电南京自动化股份有限公司、南方电网科学研究院、中国电子信息产业集团公司第六研究所、启明星辰信息技术集团有限公司。

本标准主要起草人：陈广勇、李明、黎水林、马力、曲洁、于东升、袁静、郭启全、葛波蔚、陆磊、胡红升、陈雪鸿、章恒、张益、毛澍、王斌、艾春迪、尹湘培、王勇、高亚楠、焦安春、赵劲涛、于俊杰、徐衍龙、马晓波、江雷、黄顺京、朱建兴、苏艳芳、沙淼淼、禄凯、何申、霍珊珊、于运涛、陈震、任卫红、孙慧平、万晓兰、马红霞、杨洪起、孟召瑞、李飞、王江波、阚志刚、刘健、陶源、李秋香、许凤凯、王绍杰、李晨旸、李凌、朱世顺、张五一、陈华军、张洁昕、张彪、李升、李汪蔚、王雪、蔡学琳、胡娟、刘静。

GB/T 28448于2012年6月首次发布，本次为第一次修订。

引 言

为了配合《中华人民共和国网络安全法》的实施，同时适应移动互联、云计算、物联网和工业控制等新技术、新应用情况下网络安全等级保护工作的开展，需对GB/T 28448—2012进行修订。同时，作为测评指标进行引用的GB/T 22239—2008也启动了修订工作。修订的思路和方法依据GB/T 22239调整的内容，针对共性安全保护需求提出安全测评通用要求，针对移动互联、云计算、物联网和工业控制等新技术、新应用领域的个性安全保护需求提出安全测评扩展要求，形成新的《信息安全技术 网络安全等级保护测评要求》标准。

本标准是网络安全等级保护相关系列标准之一。

与本标准相关的标准包括：

- GB/T 25058 信息安全技术 网络安全等级保护实施指南；
- GB/T 22240 信息安全技术 网络安全等级保护定级指南；
- GB/T 22239 信息安全技术 网络安全等级保护基本要求；
- GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求；
- GB/T 28448 信息安全技术 网络安全等级保护测评过程指南。

信息安全技术 网络安全等级保护测评要求

1 范围

本标准规定了不同级别的等级保护对象的安全测评通用要求和安全测评扩展要求。对第五级等级保护对象的安全测评要求不在本标准中描述。

本标准适用于信息安全测评服务机构、等级保护对象的主管部门及运营使用单位对等级保护对象安全等级保护状况进行的安全测试评估。信息安全监管职能部门依法进行的网络安全等级保护监督检查可以参考使用。

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。凡是不注明日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 17859-1999 计算机信息系统安全保护等级划分准则

GB/T 22239-20XX 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 25070-20XX 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 28449 信息安全技术 网络安全等级保护测评过程指南

GB/T 31167-2014 信息安全技术 云计算服务安全指南

GB/T 31168-2014 信息安全技术 云计算服务安全能力要求

3 术语和定义

GB/T 25069、GB 17859、GB/T 22239-20XX、GB/T 22240、GB/T 31167—2014和GB/T 31168—2014界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 31167-2014中的某些术语和定义。

3.1

访谈 interview

测评人员通过引导等级保护对象相关人员进行有目的的（有针对性的）交流以帮助测评人员理解、澄清或取得证据的过程。

3.2

核查 examine

测评人员通过对测评对象（如制度文档、各类设备及相关安全配置等）进行观察、查验和分析，以帮助测评人员理解、澄清或取得证据的过程。

3.3

测试 test

测评人员使用预定的方法/工具使测评对象（各类设备或安全配置）产生特定的结果，将运行结果与预期的结果进行比对的过程。

3.4

评估 evaluate

对测评对象可能存在的威胁及其可能产生的后果进行综合评价和预测的过程。

3.5

测评对象 target of testing and evaluation

等级测评过程中不同测评方法作用的对象，主要涉及相关配套制度文档、设备设施及人员等。

3.6

等级测评 testing and evaluation for classified cybersecurity protection

测评机构依据国家网络安全等级保护制度规定，按照有关管理规范 and 计算标准，对未涉及国家秘密的等级保护对象进行安全等级保护状况进行检测评估的活动。

3.7

云服务商 cloud service provider

云计算服务的供应方。

注：云服务商管理、运营、支撑云计算的计算基础设施及软件，通过网络交付云计算的资源。

[GB/T 31167-2014，定义3.3]

3.8

云服务客户 cloud service customer

为使用云计算服务同云服务商建立业务关系的参与方。

[GB/T 31168-2014，定义3.4]

3.9

虚拟机监视器 hypervisor

一种运行在基础物理服务器和操作系统之间的中间软件层，可允许多个操作系统和应用共享硬件。

3.10

宿主机 host machine

运行虚拟机监视器的物理服务器。

3.11

网络策略控制器 network policy controller

把网络配置信息转化为网络设备上的转发规则集，并对这些转发规则集进行管理的核心控制系统。

3.12

移动终端 mobile device

在移动业务中使用的终端设备，包括智能手机、平板电脑、个人电脑等通用终端和专用终端设备。

3.13

无线接入设备 wireless access device

采用无线通信技术将移动终端接入有线网络的通信设备。

3.14

无线接入网关 wireless access gateway

部署在无线网络与有线网络之间，对有线网络进行安全防护的设备。

3.15

移动应用软件 mobile application

针对移动移动终端开发的应用软件。

3.16

移动终端管理系统 mobile device management system

用于进行移动终端设备管理、应用管理和内容管理的专用软件，包括客户端软件和服务端软件。

3.17

物联网 internet of things (IoT)

将感知节点设备通过互联网等网络连接起来构成的系统。

3.18

感知节点设备 sensor node

对物或环境进行信息采集和/或执行操作，并能联网进行通信的装置。

3.19

网关节点设备 sensor layer gateway

将感知节点所采集的数据进行汇总、适当处理或数据融合，并进行转发的装置。

3.20

数据新鲜性 data freshness

对所接收的历史数据或超出时限的数据进行识别的特性。

4 缩略语

下列缩略语适用于本标准。

AP	无线访问接入点 (Wireless Access Point)
APT	高级持续性威胁 (Advanced Persistent Threat)
DCS	集散控制系统 (Distributed Control System)
DDoS	分布式拒绝服务 (Distributed Denial of Service)
DMZ	隔离区 (Demilitarized Zone)
ERP	企业资源计划 (Enterprise Resource Planning)
HMI	人机界面 (Human Machine Interface)
ICS	工业控制系统 (Industrial Control System)
IoT	物联网 (internet of things)
MDMS	移动终端管理系统 (Mobile Device Management System)
MES	制造执行系统 (Manufacturing Execution System)
PLC	可编程逻辑控制器 (Programmable Logic Controller)
RFID	射频识别 (radio frequency identification)
RTU	远程终端单元 (Remote Terminal Unit)
SCADA	数据采集与监视控制系统 (Supervisory Control And Data Acquisition system)
SSID	服务集标识 (Service Set Identifier)
TCB	可信计算基 (Trusted Computing Base)
VPN	虚拟专用网 (Virtual Private Network)
WiFi	无线保真 (Wireless Fidelity)
WEP	有线等效加密 (Wired Equivalent Privacy)
WPS	WiFi保护设置 (Wi-Fi Protected Setup)

5 等级测评概述

5.1 等级测评方法

等级测评实施的基本方法是针对特定的测评对象，采用相关的测评手段，遵从一定的测评规程，获取需要的证据数据，给出是否达到特定级别安全保护能力的评判。等级测评实施的详细流程和方法参见 GB/T 28449。

本标准中针对每一个要求项的测评就构成一个单项测评，单项测评中的每一个具体测评实施要求项（以下简称“测评要求项”）是与安全控制点下面所包括的要求项（测评指标）相对应的。在对每一要求项进行测评时，可能用到访谈、核查和测试三种测试方法，也可能用到其中一种或两种。测评实施的内容完全覆盖了 GB/T 22239-20XX 及 GB/T 25070-20XX（具体参见附录 C）中所有要求项的测评要求，使用时应当从单项测评的测评实施中抽取出对于 GB/T 22239-20XX 中每一个要求项的测评要求，并按照这些测评要求开发测评指导书，以规范和指导等级测评活动。

等级测评活动中涉及测评力度，包括测评广度（覆盖面）和测评深度（强弱度）。测评广度和测评深度特性影响着访谈、核查和测试的具体手段，也影响着证据数据的可信度，关于测评力度的具体描述参见附录 A。

5.2 单项测评和整体测评

等级测评分为单项测评和整体测评。

单项测评是针对各安全要求项的测评，支持测评结果的可重复性和可再现性。本标准中单项测评由测评指标、测评对象、测评实施和单元判定结果构成。

整体测评是在单项测评基础上，对等级保护对象整体安全保护能力的判断。整体安全保护能力从纵深防护和措施互补二个角度评判。

6 第一级测评要求

6.1 安全测评通用要求

6.1.1 物理和环境安全

6.1.1.1 物理访问控制

6.1.1.1.1 测评单元（L1-PES1-01）

该测评单元包括以下要求：

- a) 测评指标：机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员；
- b) 测评对象：机房电子门禁系统和值守记录；
- c) 测评实施：应核查是否安排专人值守或配置电子门禁系统；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.1.2 防盗窃和防破坏

6.1.1.2.1 测评单元（L1-PES1-02）

该测评单元包括以下要求：

- a) 测评指标：应将机房设备或主要部件进行固定，并设置明显的不易除去的标记；
- b) 测评对象：机房设备或主要部件；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内设备或主要部件是否固定；
 - 2) 应核查机房内设备或主要部件上是否设置了明显且不易除去的标记；
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.1.3 防雷击

6.1.1.3.1 测评单元（L1-PES1-03）

该测评单元包括以下要求：

- a) 测评指标：应将各类机柜、设施和设备等通过接地系统安全接地；
- b) 测评对象：机房；
- c) 测评实施：应核查机房内机柜、设施和设备等是否进行接地处理；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.1.4 防火

6.1.1.4.1 测评单元 (L1-PES1-04)

该测评单元包括以下要求：

- a) 测评指标：机房应设置灭火设备；
- b) 测评对象：机房灭火设备；
- c) 测评实施：应核查机房内是否配备灭火设备；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.1.5 防水和防潮

6.1.1.5.1 测评单元 (L1-PES1-05)

该测评单元包括以下要求：

- a) 测评指标：应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- b) 测评对象：机房；
- c) 测评实施：应核查窗户、屋顶和墙壁是否采取了防雨水渗透的措施；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.1.6 温湿度控制

6.1.1.6.1 测评单元 (L1-PES1-06)

该测评单元包括以下要求：

- a) 测评指标：应设置必要的温湿度控制设施，使机房温湿度的变化在设备运行所允许的范围之内；
- b) 测评对象：机房温湿度控制设施；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否配备了温湿度控制设施；
 - 2) 应核查温湿度是否在设备运行所允许的范围之内。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.1.7 电力供应

6.1.1.7.1 测评单元 (L1-PES1-07)

该测评单元包括以下要求：

- a) 测评指标：应在机房供电线路上配置稳压器和过电压防护设备；
- b) 测评对象：机房供电设施；
- c) 测评实施：应核查供电线路上是否配置了稳压器和过电压防护设备；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.2 网络和通信安全

6.1.2.1 网络架构

6.1.2.1.1 测评单元 (L1-NCS1-01)

该测评单元包括以下要求：

- a) 测评指标：应保证网络设备的业务处理能力满足基本业务需要；
- b) 测评对象：路由器、交换机和防火墙等网络通信类设备；
- c) 测评实施包括以下内容：
 - 1) 应核查业务高峰时期一段时间内主要网络设备的 CPU 使用率和内存使用率是否满足需要；
 - 2) 应核查网络设备是否从未出现过宕机情况。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.2.1.2 测评单元（L1-NCS1-02）

该测评单元包括以下要求：

- a) 测评指标：应保证接入网络和核心网络的带宽满足基本业务需要；
- b) 测评对象：综合网管系统；
- c) 测评实施：应核查综合网管系统各通信链路带宽是否满足高峰时段的业务流量需要；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.2.2 通信传输

6.1.2.2.1 测评单元（L1-NCS1-03）

该测评单元包括以下要求：

- a) 测评指标：应采用校验码技术保证通信过程中数据的完整性；
- b) 测评对象：提供校验码功能的设备或组件；
- c) 测评实施：应核查是否在数据传输过程中使用校验码技术来保护其完整性；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.2.3 边界防护

6.1.2.3.1 测评单元（L1-NCS1-04）

该测评单元包括以下要求：

- a) 测评指标：应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应确认等级保护对象的网络边界位置，并核查在网络边界处是否部署访问控制设备；
 - 2) 应核查设备配置信息，是否指定端口进行跨越边界的网络通信，该端口配置并启用了安全策略；
 - 3) 应采用其他技术手段（如非法无线网络设备定位检查、核查设备配置信息等）核查是否不存在其他未受控端口进行跨越边界的网络通信。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.2.4 访问控制

6.1.2.4.1 测评单元（L1-NCS1-05）

该测评单元包括以下要求：

- a) 测评指标：应在网络边界根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查在网络边界是否部署访问控制设备，是否启用访问控制策略；
 - 2) 应核查设备的最后一条访问控制策略是否为禁止所有网络通信。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.2.4.2 测评单元（L1-NCS1-06）

该测评单元包括以下要求：

- a) 测评指标：应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查设备是否存在多余或无效的访问控制策略；
 - 2) 应核查设备的不同访问控制策略之间的逻辑关系及前后排列顺序是否合理。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.2.4.3 测评单元（L1-NCS1-07）

该测评单元包括以下要求：

- a) 测评指标：应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施：应核查设备访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3 设备和计算安全

6.1.3.1 身份鉴别

6.1.3.1.1 测评单元（L1-ECS1-01）

该测评单元包括以下要求：

- a) 测评指标：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查用户在登录时是否采用了身份鉴别措施；
 - 2) 应核查用户列表，核查用户身份标识是否具有唯一性；

- 3) 应核查用户配置信息或访谈系统管理员，核查是否不存在空口令用户；
- 4) 应核查用户鉴别信息是否具有复杂度要求并定期更换。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.3.1.2 测评单元 (L1-ECS1-02)

该测评单元包括以下要求：

- a) 测评指标：应具有登录失败处理功能，配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否配置并启用了登录失败处理功能；
 - 2) 应核查是否配置并启用了限制非法登录达到一定次数后实现账户锁定功能；
 - 3) 应核查是否配置并启用了远程登录连接超时并自动退出功能。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.3.2 访问控制

6.1.3.2.1 测评单元 (L1-ECS1-03)

该测评单元包括以下要求：

- a) 测评指标：应对登录的用户分配账户和权限；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络管理员、安全管理员、系统管理员或核查用户账户和权限设置情况；
 - 2) 应核查是否已禁用或限制匿名、默认账户的访问权限。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.3.2.2 测评单元 (L1-ECS1-04)

该测评单元包括以下要求：

- a) 测评指标：应重命名或删除默认账户，修改默认账户的默认口令；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否已经重命名默认账户或默认账户已被删除；
 - 2) 应核查是否已修改默认账户的默认口令。
- d) 单元判定：如果 1) 或 2) 为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.3.2.3 测评单元 (L1-ECS1-05)

该测评单元包括以下要求：

- a) 测评指标：应及时删除或停用多余的、过期的账户，避免共享账户的存在；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否不存在多余或过期账户；
 - 2) 应访谈网络管理员、安全管理员和系统管理员不同用户是否采用不同账户登录系统。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.3.3 入侵防范

6.1.3.3.1 测评单元（L1-ECS1-06）

该测评单元包括以下要求：

- a) 测评指标：应遵循最小安装的原则，仅安装需要的组件和应用程序；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否遵循最小安装原则；
 - 2) 应确认是否已经关闭非必要的组件和应用程序。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.3.3.2 测评单元（L1-ECS1-07）

该测评单元包括以下要求：

- a) 测评指标：应关闭不需要的系统服务、默认共享和高危端口；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否定期对系统服务进行梳理，关闭了非必要的系统服务和默认共享；
 - 2) 应核查是否不存在非必要的高危端口。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.3.4 恶意代码防范

6.1.3.4.1 测评单元（L1-ECS1-08）

该测评单元包括以下要求：

- a) 测评指标：应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应核查防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.4 应用和数据安全

6.1.4.1 身份鉴别

6.1.4.1.1 测评单元（L1-ADS1-01）

该测评单元包括以下要求：

- a) 测评指标：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查用户在登录时是否采用了身份鉴别措施；
 - 2) 应核查用户登录时是否使用唯一性身份标识；
 - 3) 应核查鉴别信息是否具有复杂度要求并定期更换；
 - 4) 应核查应用系统是否不存在空口令用户。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.4.1.2 测评单元（L1-ADS1-02）

该测评单元包括以下要求：

- a) 测评指标：应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否提供并启用登录失败处理功能；
 - 2) 应核查用户连续多次登录失败时应用系统是否采取必要的保护措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.4.2 访问控制

6.1.4.2.1 测评单元（L1-ADS1-03）

该测评单元包括以下要求：

- a) 测评指标：应提供访问控制功能，对登录的用户分配账户和权限；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否提供访问控制功能；
 - 2) 应核查是否有管理用户负责对系统用户进行账户分配和权限管理。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.4.2.2 测评单元（L1-ADS1-04）

该测评单元包括以下要求：

- a) 测评指标：应重命名或删除默认账户，修改默认账户的默认口令；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：

- 1) 应核查是否已经重命名默认账户或默认账户已被删除;
 - 2) 应核查是否已修改默认账户的默认口令。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

6.1.4.2.3 测评单元 (L1-ADS1-05)

该测评单元包括以下要求:

- a) 测评指标: 应及时删除或停用多余的、过期的账户, 避免共享账户的存在;
- b) 测评对象: 应用系统管理员和业务应用系统;
- c) 测评实施包括以下内容:
 - 1) 应访谈应用系统管理员用户与账户之间是否一一对应;
 - 2) 应核查多余的、过期的账户是否被删除或停用。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

6.1.4.3 软件容错

6.1.4.3.1 测评单元 (L1-ADS1-06)

该测评单元包括以下要求:

- a) 测评指标: 应提供数据有效性检验功能, 保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求;
- b) 测评对象: 业务应用系统和系统设计文档等;
- c) 测评实施包括以下内容:
 - 1) 应核查系统设计文档的内容是否包括数据有效性检验功能的内容或模块;
 - 2) 应测试是否对人机接口或通信接口输入的内容进行有效性检验。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

6.1.4.4 数据完整性

该测评单元包括以下要求:

6.1.4.4.1 测评单元 (L1-ADS1-07)

- a) 测评指标: 应采用校验码技术保证重要数据在传输过程中的完整性;
- b) 测评对象: 系统设计文档和业务应用系统;
- c) 测评实施包括以下内容:
 - 1) 应核查系统设计文档, 重要管理数据、重要业务数据在传输过程中是否采用了校验码技术或密码技术保证完整性;
 - 2) 应测试在传输过程中对重要管理数据、重要业务数据进行篡改, 查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

6.1.4.5 数据备份恢复

6.1.4.5.1 测评单元（L1-ADS1-08）

该测评单元包括以下要求：

- a) 测评指标：应提供重要数据的本地数据备份与恢复功能；
- b) 测评对象：配置数据和业务数据；
- c) 测评实施包括以下内容：
 - 1) 应核查是否按照备份策略进行本地备份；
 - 2) 应核查备份策略设置是否合理、配置是否正确；
 - 3) 应核查备份结果是否与备份策略一致；
 - 4) 应核查近期恢复测试记录，查看是否能够进行正常的数据恢复。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.5 安全策略和管理制度

6.1.5.1 管理制度

6.1.5.1.1 测评单元（L1-PSS1-01）

该测评单元包括以下要求：

- a) 测评指标：应建立日常管理活动中常用的安全管理制度；
- b) 测评对象：安全管理制度类文档；
- c) 测评实施：应核查各项安全管理制度是否覆盖日常管理活动中的管理内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.6 安全管理机构和人员

6.1.6.1 岗位设置

6.1.6.1.1 测评单元（L1-ORS1-01）

该测评单元包括以下要求：

- a) 测评指标：应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责；
- b) 测评对象：信息安全主管和管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否进行了信息安全管理岗位的划分；
 - 2) 应核查岗位职责文档是否明确了各岗位职责。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.6.2 人员配备

6.1.6.2.1 测评单元（L1-ORS1-02）

该测评单元包括以下要求：

- a) 测评指标：应配备一定数量的系统管理员、网络管理员、安全管理员等；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：

- 1) 应访谈信息安全主管是否配备系统管理员、网络管理员和安全安全管理员;
- 2) 应核查人员配备文档是否有各岗位人员配备情况。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

6.1.6.3 授权和审批

6.1.6.3.1 测评单元 (L1-ORS1-03)

该测评单元包括以下要求:

- a) 测评指标: 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等;
- b) 测评对象: 管理制度类文档和记录表单类文档;
- c) 测评实施包括以下内容:
 - 1) 应核查部门职责文档是否有各部门的职责和授权范围;
 - 2) 应核查岗位职责文档是否有各岗位的职责和授权范围;
 - 3) 应核查审批记录中审批事项、审批部门和批准人等内容是否与相关制度一致。
- d) 单元判定: 如果 1) -3) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

6.1.6.4 人员录用

6.1.6.4.1 测评单元 (L1-ORS1-04)

该测评单元包括以下要求:

- a) 测评指标: 应指定或授权专门的部门或人员负责人员录用;
- b) 测评对象: 信息安全主管;
- c) 测评实施: 应访谈信息安全主管是否由专门的部门或人员负责人员的录用工作;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.6.5 人员离岗

6.1.6.5.1 测评单元 (L1-ORS1-05)

该测评单元包括以下要求:

- a) 测评指标: 应及时终止离岗员工的所有访问权限, 取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备;
- b) 测评对象: 记录表单类文档;
- c) 测评实施: 应核查是否具有离岗人员交还身份证件、设备等的登记记录;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.6.6 安全意识教育和培训

6.1.6.6.1 测评单元 (L1-ORS1-06)

该测评单元包括以下要求:

- a) 测评指标: 应对各类人员进行安全意识教育和岗位技能培训, 并告知相关的安全责任和惩戒措施;

- b) 测评对象：管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查信息安全教育及技能培训文档是否明确培训周期、培训方式、培训内容和考核方式等相关内容；
 - 2) 应核查安全责任和惩戒措施管理文档是否包含具体的安全责任和惩戒措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.6.7 外部人员访问管理

6.1.6.7.1 测评单元（L1-ORS1-07）

该测评单元包括以下要求：

- a) 测评指标：应确保在外部人员访问受控区域前得到授权或审批；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查外部人员访问管理文档是否明确允许外部人员访问的范围（区域、系统、设备、信息等），外部人员进入的条件（对哪些重要区域的访问须提出书面申请批准后方可进入），外部人员进入的访问控制措施（由专人全程陪同或监督等）等；
 - 2) 应核查外部人员访问重要区域的书面申请文档是否具有批准人允许访问的批准签字等。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.7 安全建设管理

6.1.7.1 定级

6.1.7.1.1 测评单元（L1-CMS1-01）

该测评单元包括以下要求：

- a) 测评指标：应明确保护对象的安全保护等级；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查定级文档是否明确保护对象的安全保护等级，是否说明定级的方法和理由；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.7.2 安全方案设计

6.1.7.2.1 测评单元（L1-CMS1-02）

该测评单元包括以下要求：

- a) 测评指标：应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
- b) 测评对象：安全规划设计类文档；
- c) 测评实施：应核查安全设计文档是否根据安全等级选择安全措施，是否根据安全需求调整安全措施；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.7.3 产品采购和使用

6.1.7.3.1 测评单元（L1-CMS1-03）

该测评单元包括以下要求：

- a) 测评指标：应确保信息安全产品采购和使用符合国家的有关规定；
- b) 测评对象：建设负责人；
- c) 测评实施：应访谈建设负责人系统使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.7.4 工程实施

6.1.7.4.1 测评单元（L1-CMS1-04）

该测评单元包括以下要求：

- a) 测评指标：应指定或授权专门的部门或人员负责工程实施过程的管理；
- b) 测评对象：建设负责人；
- c) 测评实施：应访谈建设负责人是否指定专门部门或人员对工程实施过程进行进度和质量控制，由何部门/何人负责；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.7.5 测试验收

6.1.7.5.1 测评单元（L1-CMS1-05）

该测评单元包括以下要求：

- a) 测评指标：应进行安全性测试验收；
- b) 测评对象：建设负责人；
- c) 测评实施：应访谈建设负责人是否进行了安全性测试验收；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.7.6 系统交付

6.1.7.6.1 测评单元（L1-CMS1-06）

该测评单元包括以下要求：

- a) 测评指标：应根据交付清单对所交接的设备、软件和文档等进行清点；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查交付清单是否说明交付的各类设备、软件、文档等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.7.6.2 测评单元（L1-CMS1-07）

该测评单元包括以下要求：

- a) 测评指标：应对负责运行维护的技术人员进行相应的技能培训；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查交付技术培训记录是否包括培训内容、培训时间和参与人员等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.7.7 服务供应商管理

6.1.7.7.1 测评单元（L1-CMS1-08）

该测评单元包括以下要求：

- a) 测评指标：应确保服务供应商的选择符合国家的有关规定；
- b) 测评对象：建设负责人；
- c) 测评实施：应访谈建设负责人选择的安全服务商是否符合国家有关规定；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.7.7.2 测评单元（L1-CMS1-09）

该测评单元包括以下要求：

- a) 测评指标：应与选定的服务供应商签订与安全相关的协议，明确约定相关责任；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有与安全服务商签订的服务合同或安全责任合同书，是否明确了相关责任；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.8 安全运维管理

6.1.8.1 环境管理

6.1.8.1.1 测评单元（L1-MMS1-01）

该测评单元包括以下要求：

- a) 测评指标：应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
- b) 测评对象：物理安全负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈物理安全负责人是否指定部门和人员负责机房安全管理工作，对机房的出入进行管理、对基础设施（如空调、供配电设备、灭火设备等）进行定期维护，由何部门/何人负责；
 - 2) 应核查部门或人员岗位职责文档是否明确机房安全的责任部门及人员；
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.8.1.2 测评单元（L1-MMS1-02）

该测评单元包括以下要求：

- a) 测评指标：应对机房的安全管理做出规定，包括机房物理访问、物品带进带出和机房环境安全等方面；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查机房安全管理制度是否覆盖机房物理访问、物品带进、带出机房和机房环境安全等方面内容；
 - 2) 应核查机房环境和物理访问、物品带进、带出机房等的登记记录是否与制度相符。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.8.2 介质管理

6.1.8.2.1 测评单元（L1-MMS1-03）

该测评单元包括以下要求：

- a) 测评指标：应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储介质专人管理，并根据存档介质的目录清单定期盘点；
- b) 测评对象：资产管理类和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈资产管理类介质存放于何种环境中，是否对存放介质实施专人管理；
 - 2) 应核查介质使用管理记录是否记录介质归档和使用等情况。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.8.3 设备维护管理

6.1.8.3.1 测评单元（L1-MMS1-04）

该测评单元包括以下要求：

- a) 测评指标：应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
- b) 测评对象：设备管理类和管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈设备管理员是否对各类设施、设备指定专人或专门部门进行定期维护；
 - 2) 应核查部门或人员岗位职责文档是否明确设备维护管理的责任部门。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.8.4 漏洞和风险管理

6.1.8.4.1 测评单元（L1-MMS1-05）

该测评单元包括以下要求：

- a) 测评指标：应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；
- b) 测评对象：安全管理员和记录表单类文档；
- c) 测评实施包括以下内容：

- 1) 应访谈安全管理员是否定期进行漏洞扫描,对发现的漏洞是否及时进行修补或评估可能的影响后进行修补;
 - 2) 应核查漏洞扫描报告是否描述了存在的漏洞、严重级别、原因分析和改进意见等方面。
- d) 单元判定:如果 1)~2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

6.1.8.5 网络和系统安全管理

6.1.8.5.1 测评单元 (L1-MMS1-06)

该测评单元包括以下要求:

- a) 测评指标:应划分不同的管理员角色进行网络和系统的运维管理,明确各个角色的责任和权限;
- b) 测评对象:记录表单类文档;
- c) 测评实施:应核查网络和系统安全管理文档是否明确要求对网络和系统管理员用户进行分类,并定义各个角色的责任和权限(比如:划分不同的管理角色,系统管理权限与安全审计权限分离等);
- d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

6.1.8.5.2 测评单元 (L1-MMS1-07)

该测评单元包括以下要求:

- a) 测评指标:应指定专门的部门或人员进行账户管理,对申请账户、建立账户、删除账户等进行控制;
- b) 测评对象:运维负责人和记录表单类文档;
- c) 测评实施包括以下内容:
 - 1) 应访谈运维负责人是否指定专门的部门或人员进行账户管理;
 - 2) 应核查相关审批记录或流程是否对申请账户、建立账户、删除账户等进行控制。
- d) 单元判定:如果 1)~2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

6.1.8.6 恶意代码防范管理

6.1.8.6.1 测评单元 (L1-MMS1-08)

该测评单元包括以下要求:

- a) 测评指标:应提高所有用户的防恶意代码意识,告知对外来计算机或存储设备接入系统前进行恶意代码检查等;
- b) 测评对象:运维负责人;
- c) 测评实施:应访谈运维负责人是否采取告知方式提升员工的防病毒意识;
- d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

6.1.8.6.2 测评单元 (L1-MMS1-09)

该测评单元包括以下要求:

- a) 测评指标:应对恶意代码防范要求做出规定,包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等;

- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查恶意代码防范管理制度是否明确恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.8.7 备份与恢复管理

6.1.8.7.1 测评单元（L1-MMS1-10）

该测评单元包括以下要求：

- a) 测评指标：应识别需要定期备份的重要业务信息、系统数据及软件系统等；
- b) 测评对象：系统管理员、网络管理员、数据库管理员和管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员、数据库管理员和网络管理员是否识别需定期备份的业务信息、系统数据及软件系统；
 - 2) 应核查是否具有定期备份的重要业务信息、系统数据、软件系统的列表或清单。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.8.7.2 测评单元（L1-MMS1-11）

该测评单元包括以下要求：

- a) 测评指标：应规定备份信息的备份方式、备份频度、存储介质、保存期等；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查备份与恢复管理制度是否明确备份方式、频度、介质、保存期等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.8.8 安全事件处置

6.1.8.8.1 测评单元（L1-MMS1-12）

该测评单元包括以下要求：

- a) 测评指标：应及时向安全管理部门报告所发现的安全弱点和可疑事件；
- b) 测评对象：运维负责人和管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人是否告知用户在发现安全弱点和可疑事件时应及时向安全管理部门报告；
 - 2) 应核查是否有运维过程中发现的安全弱点和可疑事件对应的报告或相关文档，内容是否详实。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.8.8.2 测评单元（L1-MMS1-13）

该测评单元包括以下要求：

- a) 测评指标：应明确安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查安全事件报告和处置流程是否明确了与安全事件有关的工作职责，包括报告单位（人）、接报单位（人）和处置单位等职责。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2 云计算安全测评扩展要求

6.2.1 网络和通信安全

6.2.1.1 网络架构

6.2.1.1.1 测评单元（L1-NCS2-01）

该测评单元包括以下要求：

- a) 测评指标：应确保云计算平台不承载高于其安全保护等级的业务应用系统；
- b) 测评对象：云计算平台和业务应用系统定级材料；
- c) 测评实施：应核查云计算平台和云计算平台承载的业务应用系统相关定级材料，查看云计算平台安全保护等级是否不低于其承载的业务应用系统；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

6.2.1.2 访问控制

6.2.1.2.1 测评单元（L1-NCS2-02）

该测评单元包括以下要求：

- a) 测评指标：应禁止云服务客户虚拟机访问宿主机；
- b) 测评对象：云管理平台和虚拟机监视器；
- c) 测评实施：应核查云管理平台等能否检测到云服务客户虚拟机对宿主机的访问；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

6.2.1.2.2 测评单元（L1-NCS2-03）

该测评单元包括以下要求：

- a) 测评指标：应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；
- b) 测评对象：访问控制机制、网络边界设备和虚拟化网络边界设备；
- c) 测评实施包括以下内容：
 - 1) 应核查云平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略是否有效；
 - 2) 应核查云平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等是否有效；
 - 3) 应核查不同云服务客户间访问控制规则和访问控制策略是否有效；
 - 4) 应核查云服务客户业务系统不同区域间访问控制规则和访问控制策略是否有效。

- d) 单元判定：如果 1) -4) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

6.2.1.2.3 测评单元 (L1-NCS2-04)

该测评单元包括以下要求：

- a) 测评指标：应保证当虚拟机迁移时，访问控制策略随其迁移；
- b) 测评对象：虚拟机、虚拟机迁移记录和相关配置；
- c) 测评实施包括以下内容：
 - 1) 应核查虚拟机迁移时访问控制策略随之迁移的措施或手段；
 - 2) 应核查虚拟机迁移记录及相关配置，查看虚拟机迁移后访问控制策略是否部署。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

6.2.2 设备和计算安全

6.2.2.1 镜像和快照保护

6.2.2.1.1 测评单元 (L1-ECS2-01)

该测评单元包括以下要求：

- a) 测评指标：应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
- b) 测评对象：云管理平台、虚拟机监视器和虚拟机镜像文件；
- c) 测评实施包括以下内容：
 - 1) 应核查虚拟机监视器是否有对镜像文件定期进行有效性验证的记录；
 - 2) 应核查虚拟机监视器，云管理平台是否提供有效的虚拟机镜像和快照文件管理机制，虚拟机是否能够及时被备份和快照，以及是否准确地恢复到所需还原点；
 - 3) 应核查虚拟机监视器，云管理平台是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

6.2.3 应用和数据安全

6.2.3.1 数据完整性

6.2.3.1.1 测评单元 (L1-ADS2-01)

该测评单元包括以下要求：

- a) 测评指标：应确保虚拟机迁移过程中，重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；
- b) 测评对象：虚拟机；
- c) 测评实施包括以下内容：
 - 1) 应核查虚拟资源迁移过程中采用的数据完整性保障措施及恢复措施；
 - 2) 应核查在虚拟资源迁移过程中，是否采取加密、签名等措施保证虚拟资源数据及重要数据的完整性，并在检测到完整性受到破坏时是否采取必要的恢复措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

6.2.3.2 数据备份恢复

6.2.3.2.1 测评单元（L1-ADS2-02）

该测评单元包括以下要求：

- a) 测评指标：应提供查询云服务客户数据及备份存储位置的方式；
- b) 测评对象：云管理平台、云平台和相关技术文档；
- c) 测评实施包括以下内容：
 - 1) 应核查云管理平台或云平台为云服务客户提供数据及备份存储位置的查询记录；
 - 2) 应核查云服务商是否为云服务客户提供数据及备份存储位置查询的接口或其他技术、管理手段。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

6.2.4 安全建设管理

6.2.4.1 云服务商选择

6.2.4.1.1 测评单元（L1-CMS2-01）

该测评单元包括以下要求：

- a) 测评指标：应选择安全合规的云服务商，其所提供的云平台应为其所承载的业务应用系统提供相应等级的安全保护能力；
- b) 测评对象：系统建设负责人、安全责任合同书、保密协议和服务合同；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统建设负责人是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云平台及云服务商；
 - 2) 应核查云服务商提供的相关服务合同是否明确其云平台具有与所承载的业务应用系统相应或高于的安全保护能力。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

6.2.4.1.2 测评单元（L1-CMS2-02）

该测评单元包括以下要求：

- a) 测评指标：应在服务水平协议中规定云服务的各项服务内容和具体技术指标；
- b) 测评对象：服务水平协议；
- c) 测评实施：应核查服务水平协议是否规定了云服务的各项服务内容和具体指标、服务期限、双方签字或盖章等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

6.2.4.1.3 测评单元（L1-CMS2-03）

该测评单元包括以下要求：

- a) 测评指标：应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；
- b) 测评对象：服务水平协议；

- c) 测评实施：应核查服务水平协议中是否规范了安全服务商和云服务供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

6.2.4.2 供应链管理

6.2.4.2.1 测评单元（L1-CMS2-04）

该测评单元包括以下要求：

- a) 测评指标：应确保供应商的选择符合国家有关规定；
- b) 测评对象：系统建设负责人；
- c) 测评实施：应访谈系统建设负责人云服务商的选择是否符合国家的有关规定；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

6.3 移动互联安全测评扩展要求

6.3.1 物理和环境安全

6.3.1.1 无线接入点的物理位置

6.3.1.1.1 测评单元（L1-PES3-01）

该测评单元包括以下要求：

- a) 测评指标：应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰；
- b) 测评对象：无线接入设备；
- c) 测评实施包括以下内容：
 - 1) 应核查物理位置与无线信号的覆盖范围；
 - 2) 应测试无线信号的覆盖范围并测试在一定范围内是否可以进行电磁干扰。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3.2 网络和通信安全

6.3.2.1 边界防护

6.3.2.1.1 测评单元（L1-NCS3-01）

该测评单元包括以下要求：

- a) 测评指标：应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备；
- b) 测评对象：无线接入网关设备；
- c) 测评实施：应核查有线网络与无线网络边界之间是否部署无线接入网关设备；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.2.2 访问控制

6.3.2.2.1 测评单元（L1-NCS3-02）

该测评单元包括以下要求：

- a) 测评指标：无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符；
- b) 测评对象：无线接入设备；
- c) 测评实施：应核查是否开启接入认证功能，是否使用除 WEP 方式以外的其它方式进行认证，密钥长度不小于 8 位；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.3 设备和计算安全

6.3.3.1 移动应用管控

6.3.3.1.1 测评单元（L1-ECS3-01）

该测评单元包括以下要求：

- a) 测评指标：应具有选择应用软件安装、运行的功能；
- b) 测评对象：移动终端管理客户端；
- c) 测评实施：应核查是否具有选择应用软件安装、运行的功能；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.4 安全建设管理

6.3.4.1 移动应用软件采购

6.3.4.1.1 测评单元（L1-CMS3-01）

该测评单元包括以下要求：

- a) 测评指标：应保证移动终端安装、运行的应用软件来自可靠证书签名或可靠分发渠道。
- b) 测评对象：安全管理员；
- c) 测评实施：应访谈安全管理员，移动终端安装、运行的应用软件是否采用国家认可的证书签名或采用指定的可靠分发渠道；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4 物联网安全测评扩展要求

6.4.1 物理和环境安全

6.4.1.1 感知节点设备物理防护

6.4.1.1.1 测评单元（L1-PES4-01）

该测评单元包括以下要求：

- a) 测评指标：感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；
- b) 测评对象：感知节点设备所处物理环境和设计或验收文档；
- c) 测评实施包括以下内容：

- 1) 应访谈物理安全负责人现有感知节点设备的环境条件是否具有防挤压、防强振动等防物理破坏的能力；
 - 2) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备所处物理环境具有防挤压、防强振动等能力的说明，是否与实际情况一致；
 - 3) 应核查感知节点设备所处物理环境是否采取了防挤压、防强振动等的防护措施。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.1.1.2 测评单元 (L1-PES4-02)

该测评单元包括以下要求：

- a) 测评指标：感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）；
- b) 测评对象：感知节点设备所处物理环境和设计或验收文档；
- c) 测评实施包括以下内容：
 - 1) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备在工作状态所处物理环境的说明，是否与实际情况一致；
 - 2) 应核查感知节点设备在工作状态所处物理环境是否能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.2 网络和通信安全

6.4.2.1 接入控制

6.4.2.1.1 测评单元 (L1-NCS4-01)

该测评单元包括以下要求：

- a) 测评指标：应确保只有授权的感知节点可以接入；
- b) 测评对象：感知节点设备和设计文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术或其他技术手段，具体措施有哪些；
 - 2) 应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制描述。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.3 安全运维管理

6.4.3.1 感知节点管理

6.4.3.1.1 测评单元 (L1-MMS4-01)

该测评单元包括以下要求：

- a) 测评指标：应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；

- b) 测评对象：维护记录；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统运维负责人是否有专门的人员对感知节点设备、网关节点设备进行定期维护，由何部门或何人负责，维护周期多长；
 - 2) 应核查感知节点设备、网关节点设备部署环境维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.3.1.2 测评单元（L1-MMS4-02）

该测评单元包括以下要求：

- a) 测评指标：应记录感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息），对网关设备进行现场维护（除尘、充电、修理等）；
- b) 测评对象：维护记录；
- c) 测评实施：应核查感知节点设备、网关节点设备部署环境维护记录是否包括了感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息）核查、对网关设备进行现场维护（除尘、充电、修理等）等方面内容。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.3.1.3 测评单元（L1-MMS4-03）

该测评单元包括以下要求：

- a) 测评指标：应对感知节点和网关节点设备部署环境的评估方法作出明确规定；
- b) 测评对象：感知节点和网关节点设备部署环境的评估说明文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统运维负责人是否明确规定需对感知节点和网关节点设备部署环境进行评估；
 - 2) 应核查感知节点和网关节点设备部署环境的评估说明文档内容是否包含可操作的评估方法。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4.3.1.4 测评单元（L1-MMS4-04）

该测评单元包括以下要求：

- a) 测评指标：应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；
- b) 测评对象：感知节点和网关节点设备安全管理文档；
- c) 测评实施：
 - 1) 应访谈系统运维负责人是否明确规定需对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程进行全程管理；
 - 2) 应核查感知节点和网关节点设备安全管理文档是否覆盖感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等方面。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.5 工业控制系统安全测评扩展要求

6.5.1 物理和环境安全

6.5.1.1 室外控制设备物理防护

6.5.1.1.1 测评单元（L1-PES5-01）

该测评单元包括以下要求：

- a) 测评指标：室外控制设备应放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；控制设备应安装在金属或其它绝缘板上（非木质板），并紧固于箱体或装置中；
- b) 测评对象：室外控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；
 - 2) 应核查是否安装在金属或其它绝缘板上（非木质板），并紧固于箱体或装置中。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.5.1.1.2 测评单元（L1-PES5-02）

该测评单元包括以下要求：

- a) 测评指标：室外控制设备放置应远离强电磁干扰、热源和应远离极端天气环境等，如无法避免，在遇到极端天气时应及时做好应急处置及检修确保设备正常运行；
- b) 测评对象：室外控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否远离极端天气环境；
 - 2) 应核查是否有极端天气时的应急处置及检修维护记录；
 - 3) 应核查位置放置是否远离强电磁干扰和热源。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.5.2 网络和通信安全

6.5.2.1 网络架构

6.5.2.1.1 测评单元（L1-NCS5-01）

该测评单元包括以下要求：

- a) 测评指标：工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用技术隔离手段；
- b) 测评对象：网闸、路由器、交换机和防火墙等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查工业控制系统的网络是否部署单向隔离设备；
 - 2) 应核查在网络边界处是否采用了有效的隔离策略；
 - 3) 应核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离强度相同的措施。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.5.2.1.2 测评单元（L1-NCS5-02）

该测评单元包括以下要求：

- a) 测评指标：工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；
- b) 测评对象：路由器、交换机和防火墙等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查工业控制系统内部不同的子系统类型，是否按照安全等级和安全防护强度等业务特点划分了不同的安全域；
 - 2) 应核查各安全域之间交换机和防火墙是否配置了有效的访问控制策略。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.5.2.2 访问控制

6.5.2.2.1 测评单元（L1-NCS5-03）

该测评单元包括以下要求：

- a) 测评指标：工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查在工业控制系统与企业其他系统之间的网络边界是否部署访问控制设备，是否配置访问控制策略；
 - 2) 应核查设备安全策略，是否禁止 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越边界。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.5.2.3 无线使用控制

6.5.2.3.1 测评单元（L1-NCS5-04）

该测评单元包括以下要求：

- a) 测评指标：应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；
- b) 测评对象：无线通信网络及设备；
- c) 测评实施包括以下内容：
 - 1) 应核查无线通信的用户在登录时是否采用了身份鉴别措施；
 - 2) 应核查无线通信的用户列表，核查用户身份标识是否具有唯一性。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.5.2.3.2 测评单元（L1-NCS5-05）

该测评单元包括以下要求：

- a) 测评指标：应对无线连接的授权、监视以及执行使用进行限制；
- b) 测评对象：无线通信网络及设备；

- c) 测评实施：应核查无线配置文件是否对连接的授权、监视及执行进行限制。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.3 设备和计算安全

6.5.3.1 控制设备安全

6.5.3.1.1 测评单元（L1-ECS5-01）

该测评单元包括以下要求：

- a) 测评指标：控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等设备和计算方面的安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；
- b) 测评对象：控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；
 - 2) 如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。
- d) 单元判定：如果 2) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.3.1.2 测评单元（L1-ECS5-02）

该测评单元包括以下要求：

- a) 测评指标：应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；
- b) 测评对象：控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查测试环境或测试报告，核查是否有测试评估记录；
 - 2) 应核查控制设备版本、补丁及固件是否经过测试后进行了更新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.5.4 安全运维管理

6.5.4.1 漏洞和风险管理

6.5.4.1.1 测评单元（L1-MMS5-01）

该测评单元包括以下要求：

- a) 测评指标：应采取必要的措施识别安全漏洞和隐患，并根据风险分析的后果，对发现的安全漏洞和隐患在确保安全生产的情况下及时进行修补；或评估可能的影响后采取必要的补救措施，补救措施宜在系统维护期间开展；
- b) 测评对象：安全管理员、管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否采取必要的措施识别安全漏洞隐患，并根据风险分析的后果，对发现的安全漏洞和隐患在确保安全生产的情况下及时进行修补；

- 2) 应核查是否有文档描述了存在的漏洞、严重级别、原因分析和改进意见等方面;
- 3) 应核查是否有维护期间设备检修记录, 查阅相关修补说明。
- d) 单元判定: 如果 1) -3) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

7 第二级测评要求

7.1 安全测评通用要求

7.1.1 物理和环境安全

7.1.1.1 物理位置选择

7.1.1.1.1 测评单元 (L2-PES1-01)

该测评单元包括以下要求:

- a) 测评指标: 机房场地应选择在具有防震、防风和防雨等能力的建筑内;
- b) 测评对象: 记录类文档和机房;
- c) 测评实施包括以下内容:
 - 1) 应核查所在建筑物是否具有建筑物抗震设防审批文档;
 - 2) 应核查机房是否不存在雨水渗漏;
 - 3) 应核查机房门窗是否不存在因风导致的尘土严重;
 - 4) 应核查屋顶、墙体、门窗和地面等是否没有破损开裂。
- d) 单元判定: 如果 1) -4) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

7.1.1.1.2 测评单元 (L2-PES1-02)

该测评单元包括以下要求:

- a) 测评指标: 机房场地应避免设在建筑物的顶层或地下室, 否则应加强防水和防潮措施;
- b) 测评对象: 机房;
- c) 测评实施: 应核查机房是否不位于所在建筑物的顶层或地下室, 如果否, 则核查机房是否采取了防水和防潮措施;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

7.1.1.2 物理访问控制

7.1.1.2.1 测评单元 (L2-PES1-03)

该测评单元包括以下要求:

- a) 测评指标: 机房出入口应安排专人值守或配置电子门禁系统, 控制、鉴别和记录进入的人员。
- b) 测评对象: 机房电子门禁系统和值守记录;
- c) 测评实施包括以下内容:
 - 1) 应核查是否安排专人值守或配置电子门禁系统;
 - 2) 应核查相关记录是否能够控制、鉴别和记录进入的人员。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.1.3 防盗窃和防破坏

7.1.1.3.1 测评单元 (L2-PES1-04)

该测评单元包括以下要求：

- a) 测评指标：应将机房设备或主要部件进行固定，并设置明显的不易除去的标记；
- b) 测评对象：机房设备或主要部件；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内设备或主要部件是否固定；
 - 2) 应核查机房内设备或主要部件上是否设置了明显且不易除去的标记。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.1.3.2 测评单元 (L2-PES1-05)

该测评单元包括以下要求：

- a) 测评指标：应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
- b) 测评对象：机房通信线缆；
- c) 测评实施：应核查机房内通信线缆是否铺设在隐蔽处或桥架中；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.1.4 防雷击

7.1.1.4.1 测评单元 (L2-PES1-06)

该测评单元包括以下要求：

- a) 测评指标：应将各类机柜、设施和设备等通过接地系统安全接地；
- b) 测评对象：机房；
- c) 测评实施：应核查机房内机柜、设施和设备等是否进行接地处理；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.1.5 防火

7.1.1.5.1 测评单元 (L2-PES1-07)

该测评单元包括以下要求：

- a) 测评指标：机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
- b) 测评对象：机房防火设施；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否设置火灾自动消防系统；
 - 2) 应核查火灾自动消防系统是否可以自动检测火情、自动报警并自动灭火。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.1.5.2 测评单元 (L2-PES1-08)

该测评单元包括以下要求：

- a) 测评指标：机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
- b) 测评对象：机房验收类文档；
- c) 测评实施：应核查机房验收文档是否明确相关建筑材料的耐火等级；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.1.6 防水和防潮

7.1.1.6.1 测评单元 (L2-PES1-09)

该测评单元包括以下要求：

- a) 测评指标：应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- b) 测评对象：机房；
- c) 测评实施：应核查窗户、屋顶和墙壁是否采取了防雨水渗透的措施；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.1.6.2 测评单元 (L2-PES1-10)

该测评单元包括以下要求：

- a) 测评指标：应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
- b) 测评对象：机房；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否采取了防止水蒸气结露的措施；
 - 2) 应核查机房内是否采取了排泄地下积水，防止地下积水渗透的措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.1.7 防静电

7.1.1.7.1 测评单元 (L2-PES1-11)

该测评单元包括以下要求：

- a) 测评指标：应安装防静电地板并采用必要的接地防静电措施；
- b) 测评对象：机房；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否安装了防静电地板；
 - 2) 应核查机房内是否采用了接地防静电措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.1.8 温湿度控制

7.1.1.8.1 测评单元 (L2-PES1-12)

该测评单元包括以下要求：

- a) 测评指标：应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内；
- b) 测评对象：机房温湿度调节设施；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否配备了专用空调；
 - 2) 应核查机房内温湿度是否在设备运行所允许的范围之内。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.1.9 电力供应

7.1.1.9.1 测评单元（L2-PES1-13）

该测评单元包括以下要求：

- a) 测评指标：应在机房供电线路上配置稳压器和过电压防护设备；
- b) 测评对象：机房供电设施；
- c) 测评实施：应核查供电线路上是否配置了稳压器和过电压防护设备；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.1.9.2 测评单元（L2-PES1-14）

该测评单元包括以下要求：

- a) 测评指标：应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；
- b) 测评对象：机房备用供电设施；
- c) 测评实施包括以下内容：
 - 1) 应核查机房是否配备 UPS 等后备电源系统；
 - 2) 应核查 UPS 等后备电源系统是否满足设备在断电情况下的正常运行要求。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.1.10 电磁防护

7.1.1.10.1 测评单元（L2-PES1-15）

该测评单元包括以下要求：

- a) 测评指标：电源线和通信线缆应隔离铺设，避免互相干扰；
- b) 测评对象：机房线缆；
- c) 测评实施：应核查机房内电源线缆和通信线缆是否隔离铺设；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.2 网络和通信安全

7.1.2.1 网络架构

7.1.2.1.1 测评单元（L2-NCS1-01）

该测评单元包括以下要求：

- a) 测评指标：应保证网络设备的业务处理能力满足业务高峰期需要；

- b) 测评对象：路由器、交换机和防火墙等提供网络通信功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查业务高峰时期一段时间内主要网络设备的 CPU 使用率和内存使用率是否满足需要；
 - 2) 应核查网络设备是否从未出现过宕机情况。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.2.1.2 测评单元 (L2-NCS1-02)

该测评单元包括以下要求：

- a) 测评指标：应保证接入网络 and 核心网络的带宽满足业务高峰期需要；
- b) 测评对象：综合网管系统；
- c) 测评实施：应核查综合网管系统各通信链路带宽是否满足高峰时段的业务流量需要；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.2.1.3 测评单元 (L2-NCS1-03)

该测评单元包括以下要求：

- a) 测评指标：应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
- b) 测评对象：路由器、交换机和防火墙等提供网络通信功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否依据某种原则划分不同的网络区域；
 - 2) 应核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.2.1.4 测评单元 (L2-NCS1-04)

该测评单元包括以下要求：

- a) 测评指标：应避免将重要网络区域部署在网络边界处且没有边界防护措施；
- b) 测评对象：网络拓扑图；
- c) 测评实施包括以下内容：
 - 1) 应核查网络拓扑图是否与实际网络运行环境一致；
 - 2) 应核查重要网络区域未部署在网络边界处且无边界防护措施；
 - 3) 应核查重要网络区域与其他网络区域之间是否采取可靠的技术隔离手段，如网闸、防火墙和设备访问控制列表 (ACL) 等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.2.2 通信传输

7.1.2.2.1 测评单元 (L2-NCS1-05)

该测评单元包括以下要求：

- a) 测评指标：应采用校验码技术保证通信过程中数据的完整性；
- b) 测评对象：提供校验码功能的设备或组件；

- c) 测评实施：应访谈安全管理员是否在数据传输过程中使用校验码技术来保护其完整性；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.2.3 边界防护

7.1.2.3.1 测评单元（L2-NCS1-06）

该测评单元包括以下要求：

- a) 测评指标：应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查在网络边界处是否部署访问控制设备；
 - 2) 应核查设备配置信息是否指定端口进行跨越边界的网络通信，该端口配置并启用了安全策略；
 - 3) 应采用其他技术手段（如非法无线网络设备定位检查、核查设备配置信息等）核查是否不存在其他未受控端口进行跨越边界的网络通信。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.2.4 访问控制

7.1.2.4.1 测评单元（L2-NCS1-07）

该测评单元包括以下要求：

- a) 测评指标：应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查在网络边界或区域之间是否部署访问控制设备，是否启用访问控制策略；
 - 2) 应核查设备的最后一条访问控制策略是否为禁止所有网络通信。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.2.4.2 测评单元（L2-NCS1-08）

该测评单元包括以下要求：

- a) 测评指标：应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查设备是否不存在多余或无效的访问控制策略；
 - 2) 应核查设备的不同访问控制策略之间的逻辑关系及前后排列顺序是否合理。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.2.4.3 测评单元（L2-NCS1-09）

该测评单元包括以下要求：

- a) 测评指标：应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施：应核查设备访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.2.4.4 测评单元（L2-NCS1-10）

该测评单元包括以下要求：

- a) 测评指标：应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施：应核查访问控制策略中是否明确设定了源地址、目的地址、源端口、目的端口和协议，访问控制粒度是否为端口级；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.2.5 入侵防范

7.1.2.5.1 测评单元（L2-NCS1-11）

该测评单元包括以下要求：

- a) 测评指标：应在关键网络节点处监视网络攻击行为；
- b) 测评对象：抗 APT 攻击系统、网络回溯系统、抗 DDoS 攻击系统、入侵保护系统和入侵检测系统；
- c) 测评实施包括以下内容：
 - 1) 应核查相关系统或设备是否能够检测到以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；
 - 2) 应核查相关系统或设备的规则库版本是否已经更新到最新版本；
 - 3) 应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点。
 - 4) 应测试相关系统或设备验证其安全策略是否有效。
- d) 单元判定：如果 1)~4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.2.6 安全审计

7.1.2.6.1 测评单元（L2-NCS1-12）

该测评单元包括以下要求：

- a) 测评指标：应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
- b) 测评对象：路由器、交换机和防火墙等设备；
- c) 测评实施包括以下内容：
 - 1) 应核查设备是否开启了日志记录或安全审计功能；

- 2) 应核查安全审计范围是否覆盖到每个用户;
- 3) 应核查是否对重要的用户行为和重要安全事件进行了审计。
- d) 单元判定: 如果 1) -3) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

7.1.2.6.2 测评单元 (L2-NCS1-13)

该测评单元包括以下要求:

- a) 测评指标: 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;
- b) 测评对象: 路由器、交换机和防火墙等设备;
- c) 测评实施: 应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;
- d) 单元判定: 如果以上测评实施内容, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

7.1.2.6.3 测评单元 (L2-NCS1-14)

该测评单元包括以下要求:

- a) 测评指标: 应对审计记录进行保护, 定期备份, 避免受到未预期的删除、修改或覆盖等;
- b) 测评对象: 路由器、交换机和防火墙等设备;
- c) 测评实施包括以下内容:
 - 1) 应核查是否采取了技术措施对审计记录进行保护;
 - 2) 应核查审计记录的备份机制和备份策略是否合理。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

7.1.2.6.4 测评单元 (L2-NCS1-15)

该测评单元包括以下要求:

- a) 测评指标: 应确保审计记录的留存时间符合法律法规要求;
- b) 测评对象: 综合安全审计系统、路由器、交换机和防火墙等设备;
- c) 测评实施: 应核查审计记录的留存时间是否至少为 6 个月;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

7.1.3 设备和计算安全

7.1.3.1 身份鉴别

7.1.3.1.1 测评单元 (L2-ECS1-01)

该测评单元包括以下要求:

- a) 测评指标: 应对登录的用户进行身份标识和鉴别, 身份标识具有唯一性, 身份鉴别信息具有复杂度要求并定期更换;
- b) 测评对象: 终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备;
- c) 测评实施包括以下内容:

- 1) 应核查用户在登录时是否采用了身份鉴别措施;
 - 2) 应核查用户列表, 核查用户身份标识是否具有唯一性;
 - 3) 应核查用户配置信息或访谈系统管理员, 核查是否不存在空口令用户;
 - 4) 应核查用户鉴别信息是否具有复杂度要求并定期更换。
- d) 单元判定: 如果 1) -4) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

7.1.3.1.2 测评单元 (L2-ECS1-02)

该测评单元包括以下要求:

- a) 测评指标: 应具有登录失败处理功能, 配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施;
- b) 测评对象: 终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备;
- c) 测评实施包括以下内容:
 - 1) 应核查是否配置并启用了登录失败处理功能;
 - 2) 应核查是否配置并启用了限制非法登录达到一定次数后实现账户锁定功能;
 - 3) 应核查是否配置并启用了远程登录连接超时并自动退出功能。
- d) 单元判定: 如果 1) -3) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

7.1.3.1.3 测评单元 (L2-ECS1-03)

该测评单元包括以下要求:

- a) 测评指标: 当进行远程管理时, 应采取必要措施, 防止鉴别信息在网络传输过程中被窃听。
- b) 测评对象: 终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备;
- c) 测评实施: 应核查是否采用加密等安全方式对系统进行远程管理, 防止鉴别信息在网络传输过程中被窃听;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

7.1.3.2 访问控制

7.1.3.2.1 测评单元 (L2-ECS1-04)

该测评单元包括以下要求:

- a) 测评指标: 应对登录的用户分配账户和权限;
- b) 测评对象: 终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备;
- c) 测评实施包括以下内容:
 - 1) 应访谈网络管理员、安全管理员、系统管理员或核查用户账户和权限设置情况;
 - 2) 应核查是否已禁用或限制匿名、默认账户的访问权限。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

7.1.3.2.2 测评单元 (L2-ECS1-05)

该测评单元包括以下要求：

- a) 测评指标：应重命名或删除默认账户，修改默认账户的默认口令；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否已经重命名默认账户或默认账户已被删除；
 - 2) 应核查是否已修改默认账户的默认口令。
- d) 单元判定：如果 1) 或 2) 为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.3.2.3 测评单元（L2-ECS1-06）

该测评单元包括以下要求：

- a) 测评指标：应及时删除或停用多余的、过期的账户，避免共享账户的存在；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否不存在多余或过期账户；
 - 2) 应访谈网络管理员、安全管理员和系统管理员不同用户是否采用不同账户登录系统。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.3.2.4 测评单元（L2-ECS1-07）

该测评单元包括以下要求：

- a) 测评指标：应授予管理用户所需的最小权限，实现管理用户的权限分离；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查访问控制策略，核查管理用户的权限是否已进行分离；
 - 2) 应核查管理用户权限是否为其工作任务所需的最小权限。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.3.3 安全审计

7.1.3.3.1 测评单元（L2-ECS1-08）

该测评单元包括以下要求：

- a) 测评指标：应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否开启了安全审计功能；
 - 2) 应核查安全审计范围是否覆盖到每个用户；
 - 3) 应核查是否对重要的用户行为和重要安全事件进行审计。

- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.3.3.2 测评单元 (L2-ECS1-09)

该测评单元包括以下要求：

- a) 测评指标：审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.3.3.3 测评单元 (L2-ECS1-10)

该测评单元包括以下要求：

- a) 测评指标：应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否采取了保护措施对审计记录进行保护；
 - 2) 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.3.3.4 测评单元 (L2-ECS1-11)

该测评单元包括以下要求：

- a) 测评指标：应确保审计记录的留存时间符合法律法规要求；
- b) 测评对象：综合安全审计系统、终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应核查审计记录的留存时间是否至少为 6 个月；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.3.4 入侵防范

7.1.3.4.1 测评单元 (L2-ECS1-12)

该测评单元包括以下要求：

- a) 测评指标：应遵循最小安装的原则，仅安装需要的组件和应用程序；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否遵循最小安装原则；
 - 2) 应确认是否已经关闭非必要的组件和应用程序。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.3.4.2 测评单元 (L2-ECS1-13)

该测评单元包括以下要求：

- a) 测评指标：应关闭不需要的系统服务、默认共享和高危端口；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否定期对系统服务进行梳理，关闭了非必要的系统服务和默认共享；
 - 2) 应核查是否不存在非必要的高危端口。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.3.4.3 测评单元 (L2-ECS1-14)

该测评单元包括以下要求：

- a) 测评指标：应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应核查配置文件是否对终端接入范围进行限制；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.3.4.4 测评单元 (L2-ECS1-15)

该测评单元包括以下要求：

- a) 测评指标：应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应进行漏洞扫描，核查是否不存在高风险漏洞；
 - 2) 应访谈系统管理员是否在经过充分测试评估后及时修补漏洞。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.3.5 恶意代码防范

7.1.3.5.1 测评单元 (L2-ECS1-16)

该测评单元包括以下要求：

- a) 测评指标：应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应核查防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.3.6 资源控制

7.1.3.6.1 测评单元 (L2-ECS1-17)

该测评单元包括以下要求：

- a) 测评指标：应限制单个用户或进程对系统资源的最大使用限度；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否存在系统资源控制的措施，如核查配置参数是否设置最大进程数；
 - 2) 应引用产品（应用）测试结果或核查数据库表空间，确认目前系统资源利用率是否在允许范围之内或目前总体数据库表空间占用率是否不超过阈值；
 - 3) 应核查是否存在对数据库资源过大或最小的用户的限制措施。
- d) 单元判定：如果 1)～3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4 应用和数据安全

7.1.4.1 身份鉴别

7.1.4.1.1 测评单元（L2-ADS1-01）

该测评单元包括以下要求：

- a) 测评指标：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查用户在登录时是否采用了身份鉴别措施；
 - 2) 应核查用户登录时是否使用唯一性身份标识；
 - 3) 应核查鉴别信息是否具有复杂度要求并定期更换；
 - 4) 应核查应用系统是否不存在空口令用户。
- d) 单元判定：如果 1)～4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.1.2 测评单元（L2-ADS1-02）

该测评单元包括以下要求：

- a) 测评指标：应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否提供并启用登录失败处理功能；
 - 2) 应核查用户连续多次登录失败时应用系统是否采取必要的保护措施。
- d) 单元判定：如果 1)～2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.1.3 测评单元（L2-ADS1-03）

该测评单元包括以下要求：

- a) 测评指标：应强制用户首次登录时修改初始口令；
- b) 测评对象：业务应用系统；
- c) 测评实施：应核查用户首次登录时是否被强制修改初始口令；

- d) 单元判定：如果以上测评实施内容，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.1.4 测评单元（L2-ADS1-04）

该测评单元包括以下要求：

- a) 测评指标：用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查用户身份鉴别信息丢失时，是否采用鉴别信息重置或其他技术措施保证安全；
 - 2) 应核查用户身份鉴别信息失效时，是否采用鉴别信息重置或其他技术措施保证安全。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.2 访问控制

7.1.4.2.1 测评单元（L2-ADS1-05）

该测评单元包括以下要求：

- a) 测评指标：应提供访问控制功能，对登录的用户分配账户和权限；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否提供访问控制功能；
 - 2) 应核查是否有管理用户负责对系统用户进行账户分配和权限管理。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.2.2 测评单元（L2-ADS1-06）

该测评单元包括以下要求：

- a) 测评指标：应重命名或删除默认账户，修改默认账户的默认口令；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否已经重命名默认账户或默认账户已被删除；
 - 2) 应核查是否已修改默认账户的默认口令。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.2.3 测评单元（L2-ADS1-07）

该测评单元包括以下要求：

- a) 测评指标：应及时删除或停用多余的、过期的账户，避免共享账户的存在；
- b) 测评对象：应用系统管理员和业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应访谈应用系统管理员用户与账户之间是否一一对应；
 - 2) 应核查多余的、过期的账户是否被删除或停用。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.3 安全审计

7.1.4.3.1 测评单元 (L2-ADS1-08)

该测评单元包括以下要求：

- a) 测评指标：应提供并启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否提供并启用了安全审计功能；
 - 2) 应核查审计范围是否覆盖到每个用户；
 - 3) 应核查是否对重要的用户行为和重要安全事件进行审计。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.3.2 测评单元 (L2-ADS1-09)

该测评单元包括以下要求：

- a) 测评指标：审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- b) 测评对象：业务应用系统；
- c) 测评实施：应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- d) 单元判定：如果以上测评实施内容，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.3.3 测评单元 (L2-ADS1-10)

该测评单元包括以下要求：

- a) 测评指标：应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否采取了保护措施对审计记录进行保护；
 - 2) 应核查审计记录的备份机制及备份策略。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.3.4 测评单元 (L2-ADS1-11)

该测评单元包括以下要求：

- a) 测评指标：应确保审计记录的留存时间符合法律法规要求；
- b) 测评对象：综合安全审计系统和业务应用系统；
- c) 测评实施：应核查审计记录的留存时间是否至少为 6 个月；

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.4.4 软件容错

7.1.4.4.1 测评单元（L2-ADS1-12）

该测评单元包括以下要求：

- a) 测评指标：应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
- b) 测评对象：业务应用系统和系统设计文档等；
- c) 测评实施包括以下内容：
 - 1) 应核查系统设计文档的内容是否包括数据有效性检验功能的内容或模块；
 - 2) 应测试是否对人机接口或通信接口输入的内容进行有效性检验。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.4.2 测评单元（L2-ADS1-13）

该测评单元包括以下要求：

- a) 测评指标：在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施；
- b) 测评对象：系统设计文档和维护文档等；
- c) 测评实施包括以下内容：
 - 1) 应核查应用系统设计文档和维护文档，应用系统有故障发生时是否能继续提供一部分功能；
 - 2) 应核查应用系统设计文档和维护文档，应用系统有故障发生后，是否能够实施必要的措施使系统恢复功能。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.5 资源控制

7.1.4.5.1 测评单元（L2-ADS1-14）

该测评单元包括以下要求：

- a) 测评指标：当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；
- b) 测评对象：业务应用系统；
- c) 测评实施：应测试应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.5.2 测评单元（L2-ADS1-15）

该测评单元包括以下要求：

- a) 测评指标：应能够对系统的最大并发会话连接数进行限制；
- b) 测评对象：业务应用系统或中间件等；
- c) 测评实施包括以下内容：
 - 1) 应核查应用系统配置信息是否对最大并发会话连接数进行限制；

- 2) 应核查中间件配置信息是否对最大并发会话连接数进行限制。
- d) 单元判定：如果 1) 或 2) 为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.5.3 测评单元 (L2-ADS1-16)

该测评单元包括以下要求：

- a) 测评指标：应能够对单个账户的多重并发会话进行限制；
- b) 测评对象：业务应用系统；
- c) 测评实施：应测试是否能够正确地限制单个账户的多重并发会话数；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.4.6 数据完整性

7.1.4.6.1 测评单元 (L2-ADS1-17)

该测评单元包括以下要求：

- a) 测评指标：应采用校验码技术保证重要数据在传输过程中的完整性；
- b) 测评对象：系统设计文档和业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查系统设计文档，重要管理数据、重要业务数据在传输过程中是否采用了校验码技术或密码技术保证完整性；
 - 2) 应测试在传输过程中对重要管理数据、重要业务数据进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.7 数据备份恢复

7.1.4.7.1 测评单元 (L2-ADS1-18)

该测评单元包括以下要求：

- a) 测评指标：应提供重要数据的本地数据备份与恢复功能；
- b) 测评对象：配置数据和业务数据；
- c) 测评实施包括以下内容：
 - 1) 应核查是否按照备份策略进行本地备份；
 - 2) 应核查备份策略设置是否合理、配置是否正确；
 - 3) 应核查备份结果是否与备份策略一致；
 - 4) 应核查近期恢复测试记录，查看是否能够进行正常的数据恢复。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.7.2 测评单元 (L2-ADS1-19)

该测评单元包括以下要求：

- a) 测评指标：应提供数据的异地备份功能，利用通信网络将重要数据定时批量传送至备用场地；
- b) 测评对象：配置数据和业务数据；

- c) 测评实施：应核查是否提供异地数据备份功能，并通过通信网络将重要配置数据、重要业务数据定时批量传送至备份场地；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.4.8 剩余信息保护

7.1.4.8.1 测评单元（L2-ADS1-20）

该测评单元包括以下要求：

- a) 测评指标：应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及业务应用系统；
- c) 测评实施：应核查相关配置信息或访谈应用系统管理员，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。
- d) 单元判定：如果 以上测评实施内容，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.9 个人信息保护

7.1.4.9.1 测评单元（L2-ADS1-21）

该测评单元包括以下要求：

- a) 测评指标：应仅采集和保存业务必需的用户个人信息；
- b) 测评对象：用户数据和业务应用系统；
- c) 测评实施：应核查采集的用户信息是否是业务应用必需的；
- d) 单元判定：如果以上测评实施内容，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4.9.2 测评单元（L2-ADS1-22）

该测评单元包括以下要求：

- a) 测评指标：应禁止未授权访问和非法使用用户个人信息；
- b) 测评对象：用户数据和业务应用系统；
- c) 测评实施：应核查是否采用技术措施限制对用户信息的访问和使用；
- d) 单元判定：如果以上测评实施内容，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.5 安全策略和管理制度

7.1.5.1 安全策略（L2-PSS1-01）

该测评单元包括以下要求：

- a) 测评指标：应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
- b) 测评对象：总体方针策略类文档；
- c) 测评实施：应核查信息安全工作的总体方针和安全策略文件是否明确机构安全工作的总体目标、范围、原则和各类安全策略；

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.5.2 管理制度

7.1.5.2.1 测评单元（L2-PSS1-02）

该测评单元包括以下要求：

- a) 测评指标：应对安全管理活动中的主要管理内容建立安全管理制度；
- b) 测评对象：安全管理制度类文档；
- c) 测评实施：应核查各项安全管理制度是否覆盖物理、网络、主机系统、数据、应用、建设和运维等层面的管理内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.5.2.2 测评单元（L2-PSS1-03）

该测评单元包括以下要求：

- a) 测评指标：应对要求管理人员或操作人员执行的日常管理操作建立操作规程；
- b) 测评对象：操作规程类文档；
- c) 测评实施：应核查是否具有日常管理操作的操作规程，如系统维护手册和用户操作规程等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.5.3 制定和发布

7.1.5.3.1 测评单元（L2-PSS1-04）

该测评单元包括以下要求：

- a) 测评指标：应指定或授权专门的部门或人员负责安全管理制度的制定；
- b) 测评对象：信息安全主管；
- c) 测评实施：应访谈信息安全主管是否由专门的部门或人员负责制定安全管理制度；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.5.3.2 测评单元（L2-PSS1-05）

该测评单元包括以下要求：

- a) 测评指标：安全管理制度应通过正式、有效的方式发布，并进行版本控制；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查制度制定和发布要求管理文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容；
 - 2) 应核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导签署和单位盖章等，是否注明发布范围。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.5.4 评审和修订

7.1.5.4.1 测评单元 (L2-PSS1-06)

该测评单元包括以下要求：

- a) 测评指标：应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否定期对安全管理制度体系的合理性和适用性进行审定；
 - 2) 应核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制度。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.6 安全管理机构和人员

7.1.6.1 岗位设置

7.1.6.1.1 测评单元 (L2-ORS1-01)

该测评单元包括以下要求：

- a) 测评指标：应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
- b) 测评对象：信息安全主管和管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否进行了信息安全管理职能部门的划分；
 - 2) 应核查部门职责文档是否明确信息安全管理工作的职能部门和各负责人职责；
 - 3) 应核查岗位职责文档是否有岗位划分情况和岗位职责。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.6.1.2 测评单元 (L2-ORS1-02)

该测评单元包括以下要求：

- a) 测评指标：应设立系统管理员、网络管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责；
- b) 测评对象：信息安全主管和管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否进行了信息安全管理岗位的划分；
 - 2) 应核查岗位职责文档是否明确了各岗位职责。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.6.2 人员配备

7.1.6.2.1 测评单元 (L2-ORS1-03)

该测评单元包括以下要求：

- a) 测评指标：应配备一定数量的系统管理员、网络管理员、安全管理员等。
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否配备了系统管理员、网络管理员和安全管理员；
 - 2) 应核查人员配备文档是否有各岗位人员配备情况。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.6.3 授权和审批

7.1.6.3.1 测评单元（L2-ORS1-04）

该测评单元包括以下要求：

- a) 测评指标：应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查部门职责文档，查看各部门的职责和授权范围；
 - 2) 应核查岗位职责文档，查看各岗位的职责和授权范围；
 - 3) 应核查审批记录，查看审批事项、审批部门和批准人等内容是否与相关制度一致。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.6.3.2 测评单元（L2-ORS1-05）

该测评单元包括以下要求：

- a) 测评指标：应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查各类审批记录是否针对系统变更、重要操作、物理访问和系统接入等事项进行审批；
- d) 单元判定：如果以上测评实施内容，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.6.4 沟通和合作

7.1.6.4.1 测评单元（L2-ORS1-06）

该测评单元包括以下要求：

- a) 测评指标：应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理信息安全问题；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否建立了各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通机制；
 - 2) 应核查会议记录是否明确各类管理人员之间、组织内部机构之间以及信息安全职能部门内部开展了合作与沟通。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.6.4.2 测评单元 (L2-ORS1-07)

该测评单元包括以下要求：

- a) 测评指标：应加强与公安机关、各类供应商、业界专家及安全组织的合作与沟通；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否建立了与公安机关、各类供应商、业界专家及安全组织的合作与沟通机制；
 - 2) 应核查会议记录是否明确了与公安机关、各类供应商、业界专家及安全组织是否开展了合作与沟通。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.6.4.3 测评单元 (L2-ORS1-08)

该测评单元包括以下要求：

- a) 测评指标：应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查外联单位联系列表是否记录了外联单位名称、合作内容、联系人和联系方式等信息；
- d) 单元判定：如果以上测评实施内容，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.6.5 审核和检查

7.1.6.5.1 测评单元 (L2-ORS1-09)

该测评单元包括以下要求：

- a) 测评指标：应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否定期进行常规安全核查；
 - 2) 应核查常规安全核查记录是否包括了系统日常运行、系统漏洞和数据备份等情况。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.6.6 人员录用

7.1.6.6.1 测评单元 (L2-ORS1-10)

该测评单元包括以下要求：

- a) 测评指标：应指定或授权专门的部门或人员负责人员录用；
- b) 测评对象：信息安全主管；

- c) 测评实施：应访谈信息安全主管是否由专门的部门或人员负责人员的录用工作；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.6.6.2 测评单元（L2-ORS1-11）

该测评单元包括以下要求：

- a) 测评指标：应对被录用人员的身份、背景、专业资格和资质等进行审查；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查人员安全管理文档是否说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）；
 - 2) 应核查是否具有人员录用时对录用人身份、背景、专业资格和资质等进行审查的相关文档或记录，是否记录审查内容和审查结果等；
 - 3) 应核查人员录用时的技能考核文档或记录是否记录考核内容和考核结果等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.6.7 人员离岗

7.1.6.7.1 测评单元（L2-ORS1-12）

该测评单元包括以下要求：

- a) 测评指标：应及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有离岗人员交还身份证件、设备等的登记记录；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.6.8 安全意识教育和培训

7.1.6.8.1 测评单元（L2-ORS1-13）

该测评单元包括以下要求：

- a) 测评指标：应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
- b) 测评对象：管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查信息安全教育及技能培训文档是否明确培训周期、培训方式、培训内容和考核方式等相关内容；
 - 2) 应核查安全责任和惩戒措施管理文档是否包含具体的安全责任和惩戒措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.6.9 外部人员访问管理

7.1.6.9.1 测评单元（L2-ORS1-14）

该测评单元包括以下要求：

- a) 测评指标：应确保在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查外部人员访问管理文档是否明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等；
 - 2) 应核查外部人员访问重要区域的书面申请文档是否具有批准人允许访问的批准签字等；
 - 3) 应核查外部人员访问重要区域的登记记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.6.9.2 测评单元（L2-ORS1-15）

该测评单元包括以下要求：

- a) 测评指标：应确保在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查外部人员访问管理文档是否明确外部人员接入受控网络前的申请审批流程；
 - 2) 应核查外部人员访问系统的书面申请文档是否明确外部人员的访问权限，是否具有允许访问的批准签字等；
 - 3) 应核查外部人员访问系统的登记记录是否记录了外部人员访问的权限、时限、账户等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.6.9.3 测评单元（L2-ORS1-16）

该测评单元包括以下要求：

- a) 测评指标：外部人员离场后应及时清除其所有的访问权限；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查外部人员访问管理文档是否明确外部人员离开后及时清除其所有访问权限；
 - 2) 应核查外部人员访问系统的登记记录是否记录了访问权限清除时间。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.7 安全建设管理

7.1.7.1 定级和备案

7.1.7.1.1 测评单元（L2-CMS1-01）

该测评单元包括以下要求：

- a) 测评指标：应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
- b) 测评对象：记录表单类文档；

- c) 测评实施：应核查定级文档是否明确保护对象的安全保护等级，是否说明定级的方法和理由；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.1.2 测评单元（L2-CMS1-02）

该测评单元包括以下要求：

- a) 测评指标：应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查定级结果的论证评审会议记录是否有相关部门和有关安全技术专家对定级结果的论证意见；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.1.3 测评单元（L2-CMS1-03）

该测评单元包括以下要求：

- a) 测评指标：应确保定级结果经过相关部门的批准；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查定级结果部门审批文档是否有上级主管部门或本单位相关部门的审批意见；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.1.4 测评单元（L2-CMS1-04）

该测评单元包括以下要求：

- a) 测评指标：应将备案材料报主管部门和相应公安机关备案；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有公安机关出具的备案证明文档；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.2 安全方案设计

7.1.7.2.1 测评单元（L2-CMS1-05）

该测评单元包括以下要求：

- a) 测评指标：应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
- b) 测评对象：安全规划设计类文档；
- c) 测评实施：应核查安全设计文档是否根据安全等级选择安全措施，是否根据安全需求调整安全措施；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.2.2 测评单元（L2-CMS1-06）

- a) 测评指标：应根据保护对象的安全保护等级进行安全方案设计；
- b) 测评对象：安全规划设计类文档；

- c) 测评实施：应核查是否有总体规划和安全设计方案等配套文件；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求；

7.1.7.2.3 测评单元（L2-CMS1-07）

该测评单元包括以下要求：

- a) 测评指标：应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查配套文件的论证评审记录或文档是否有相关部门和有关安全技术专家对总体规划、安全设计方案等相关配套文件的论证意见；
 - 2) 应核查是否有总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件，各个文件是否有机构管理层的批准。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.7.3 产品采购和使用

7.1.7.3.1 测评单元（L2-CMS1-08）

该测评单元包括以下要求：

- a) 测评指标：应确保信息安全产品采购和使用符合国家的有关规定；
- b) 测评对象：建设负责人；
- c) 测评实施：应访谈建设负责人使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.3.2 测评单元（L2-CMS1-09）

该测评单元包括以下要求：

- a) 测评指标：应确保密码产品与服务的采购和使用符合国家密码主管部门的要求；
- b) 测评对象：建设负责人；
- c) 测评实施：应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.4 自行软件开发

7.1.7.4.1 测评单元（L2-CMS1-10）

该测评单元包括以下要求：

- a) 测评指标：应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
- b) 测评对象：建设负责人；
- c) 测评实施包括以下内容：

- 1) 应访谈建设负责人自主开发软件是否在独立的物理环境中完成编码和调试,与实际运行环境分开;
 - 2) 应核查测试数据和结果是否受控使用。
- d) 单元判定:如果 1)~2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

7.1.7.4.2 测评单元 (L2-CMS1-11)

该测评单元包括以下要求:

- a) 测评指标:应确保在软件开发过程中对安全性进行测试,在软件安装前对可能存在的恶意代码进行检测;
- b) 测评对象:记录表单类文档;
- c) 测评实施:应核查是否具有软件安全测试报告,明确软件存在的安全问题及可能存在的恶意代码。
- d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

7.1.7.5 外包软件开发

7.1.7.5.1 测评单元 (L2-CMS1-12)

该测评单元包括以下要求:

- a) 测评指标:应在软件交付前检测其中可能存在的恶意代码;
- b) 测评对象:记录表单类文档;
- c) 测评实施:应核查是否具有交付前的恶意代码检测报告;
- d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

7.1.7.5.2 测评单元 (L2-CMS1-13)

该测评单元包括以下要求:

- a) 测评指标:应要求开发单位提供软件设计文档和使用指南;
- b) 测评对象:记录表单类文档;
- c) 测评实施:应核查是否具有软件开发的相关文档,如需求分析说明书、软件设计说明书等,是否具有软件操作手册或使用指南;
- d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

7.1.7.6 工程实施

7.1.7.6.1 测评单元 (L2-CMS1-14)

该测评单元包括以下要求:

- a) 测评指标:应指定或授权专门的部门或人员负责工程实施过程的管理;
- b) 测评对象:建设负责人;
- c) 测评实施:应访谈建设负责人是否指定专门部门或人员对工程实施过程进行进度和质量控制,由何部门/何人负责;

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.6.2 测评单元（L2-CMS1-15）

该测评单元包括以下要求：

- a) 测评指标：应制定工程实施方案控制安全工程实施过程；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查工程实施方案是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.7 测试验收

7.1.7.7.1 测评单元（L2-CMS1-16）

该测评单元包括以下要求：

- a) 测评指标：应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查工程测试验收方案是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容；
 - 2) 应核查测试验收报告是否有相关部门和人员对测试验收报告进行审定的意见。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.7.7.2 测评单元（L2-CMS1-17）

该测评单元包括以下要求：

- a) 测评指标：应进行上线前的安全性测试，并出具安全测试报告；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有上线前的安全测试报告；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.8 系统交付

7.1.7.8.1 测评单元（L2-CMS1-18）

该测评单元包括以下要求：

- a) 测评指标：应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查交付清单是否说明交付的各类设备、软件、文档等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.8.2 测评单元（L2-CMS1-19）

该测评单元包括以下要求：

- a) 测评指标：应对负责运行维护的技术人员进行相应的技能培训；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查交付技术培训记录是否包括培训内容、培训时间和参与人员等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.8.3 测评单元（L2-CMS1-20）

该测评单元包括以下要求：

- a) 测评指标：应确保提供建设过程中的文档和指导用户进行运行维护的文档；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查交付文档否有指导用户进行运维的文档等，提交的文档是否符合管理规定的要求；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.9 等级测评

7.1.7.9.1 测评单元（L2-CMS1-21）

该测评单元包括以下要求：

- a) 测评指标：应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人本次测评是否为首次，若非首次，以往进行过几次测评，是否根据测评结果进行相应的安全整改；
 - 2) 应核查是否具有以往等级测评报告和安全整改方案。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.7.9.2 测评单元（L2-CMS1-22）

该测评单元包括以下要求：

- a) 测评指标：应在发生重大变更或级别发生变化时进行等级测评；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人是否有过重大变更或级别发生过变化，若有，是否进行相应的等级测评；
 - 2) 应核查是否具有相应情况下的等级测评报告。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.7.9.3 测评单元（L2-CMS1-23）

该测评单元包括以下要求：

- a) 测评指标：应确保测评机构的选择符合国家有关规定；
- b) 测评对象：运维负责人；

- c) 测评实施：应访谈运维负责人以往等级测评的测评单位是否具有国家相关等级测评资质的单位；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.10 服务供应商管理

7.1.7.10.1 测评单元（L2-CMS1-24）

该测评单元包括以下要求：

- a) 测评指标：应确保服务供应商的选择符合国家的有关规定；
- b) 测评对象：运维负责人；
- c) 测评实施：应访谈建设负责人选择的安全服务商是否符合国家有关规定；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.7.10.2 测评单元（L2-CMS1-25）

该测评单元包括以下要求：

- a) 测评指标：应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的信息安全相关义务；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查与安全服务商签订的服务合同或安全责任合同书是否明确了后期的技术支持和服务承诺等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8 安全运维管理

7.1.8.1 环境管理

7.1.8.1.1 测评单元（L2-MMS1-01）

该测评单元包括以下要求：

- a) 测评指标：应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
- b) 测评对象：物理安全负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈物理安全负责人是否指定部门和人员负责机房安全管理工作，对机房的出入进行管理、对基础设施（如空调、供配电设备、灭火设备等）进行定期维护，由何部门/何人负责；
 - 2) 应核查部门或人员岗位职责文档是否明确机房安全的责任部门及人员；
 - 3) 应核查机房的出入登记记录是否记录来访人员、来访时间、离开时间、携带物品等信息；
 - 4) 应核查机房的基础设施的维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.1.2 测评单元（L2-MMS1-02）

该测评单元包括以下要求：

- a) 测评指标：应对机房的安全管理做出规定，包括机房物理访问、物品带进带出和机房环境安全等；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查机房安全管理制度是否覆盖机房物理访问、物品带进、带出机房和机房环境安全等方面内容；
 - 2) 应核查机房环境和物理访问、物品带进、带出机房等的登记记录是否与制度相符。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.1.3 测评单元（L2-MMS1-03）

该测评单元包括以下要求：

- a) 测评指标：应不在重要区域接待来访人员和桌面上没有包含敏感信息的纸档文件、移动介质等；
- b) 测评对象：安全管理员和办公环境；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否有相关规定明确接待来访人员区域；
 - 2) 应核查办公桌面上是否不包含敏感信息的纸档文件和移动介质等。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.2 资产管理

7.1.8.2.1 测评单元（L2-MMS1-04）

该测评单元包括以下要求：

- a) 测评指标：应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查资产清单是否覆盖资产范围（含设备设施、软件、文档等）、资产责任部门、重要程度和所处位置等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8.3 介质管理

7.1.8.3.1 测评单元（L2-MMS1-05）

该测评单元包括以下要求：

- a) 测评指标：应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储介质专人管理，并根据存档介质的目录清单定期盘点；
- b) 测评对象：资产管理员和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈资产管理员介质存放于何种环境中，是否对存放介质实施专人管理；
 - 2) 应核查介质使用管理记录是否记录介质归档和使用等情况。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.3.2 测评单元 (L2-MMS1-06)

该测评单元包括以下要求：

- a) 测评指标：应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录；
- b) 测评对象：资产管理类和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈资产管理类介质在物理传输过程中的人员、打包交付等情况是否进行控制；
 - 2) 应核查是否有对介质的归档和查询等的登记记录。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.4 设备维护管理

7.1.8.4.1 测评单元 (L2-MMS1-07)

该测评单元包括以下要求：

- a) 测评指标：应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
- b) 测评对象：设备管理类和管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈设备管理员是否对各类设施、设备指定专人或专门部门进行定期维护；
 - 2) 应核查部门或人员岗位职责文档是否明确设备维护管理的责任部门。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.4.2 测评单元 (L2-MMS1-08)

该测评单元包括以下要求：

- a) 测评指标：应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查设备维护管理制度是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容；
 - 2) 应核查是否留有维修和服务的审批、维修过程等记录，审批、记录内容是否与制度相符。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.5 漏洞和风险管理

7.1.8.5.1 测评单元 (L2-MMS1-09)

该测评单元包括以下要求：

- a) 测评指标：应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；
- b) 测评对象：安全管理员和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否定期进行漏洞扫描，对发现的漏洞是否及时进行修补或评估可能的影响后进行修补；
 - 2) 应核查漏洞扫描报告是否描述了存在的漏洞、严重级别、原因分析和改进意见等方面。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.6 网络和系统安全管理

7.1.8.6.1 测评单元（L2-MMS1-10）

该测评单元包括以下要求：

- a) 测评指标：应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查网络和系统安全管理文档是否明确要求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8.6.2 测评单元（L2-MMS1-11）

该测评单元包括以下要求：

- a) 测评指标：应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人是否指定专门的部门或人员进行账户管理；
 - 2) 应核查相关审批记录或流程是否对申请账户、建立账户、删除账户等进行控制。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.6.3 测评单元（L2-MMS1-12）

该测评单元包括以下要求：

- a) 测评指标：应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略，账户管理（用户责任、义务、风险、权限审批、权限分配、账户注销等），配置文件的生成、备份，变更审批、符合性核查等，授权访问，最小服务，升级与打补丁，审计日志，登录设备和系统的口令更新周期等方面；

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8.6.4 测评单元（L2-MMS1-13）

该测评单元包括以下要求：

- a) 测评指标：应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
- b) 测评对象：操作规程类文档；
- c) 测评实施：应核查重要设备（如操作系统、数据库、网络设备、安全设备、应用和组件）的配置和操作手册是否明确操作步骤、维护记录、参数配置等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.6.5 测评单元（L2-MMS1-14）

该测评单元包括以下要求：

- a) 测评指标：应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修改等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8.7 恶意代码防范管理

7.1.8.7.1 测评单元（L2-MMS1-15）

该测评单元包括以下要求：

- a) 测评指标：应提高所有用户的防恶意代码意识，告知对外来计算机或存储设备接入系统前进行恶意代码检查等；
- b) 测评对象：运维负责人；
- c) 测评实施：应访谈运维负责人是否采取告知方式提升员工的防病毒意识；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8.7.2 测评单元（L2-MMS1-16）

该测评单元包括以下要求：

- a) 测评指标：应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查恶意代码防范管理制度是否明确防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8.7.3 测评单元（L2-MMS1-17）

该测评单元包括以下要求：

- a) 测评指标：应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理；
- b) 测评对象：安全管理员和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否定期对恶意代码库进行升级，且对升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报，是否出现过大规模的病毒事件，如何处理；
 - 2) 应核查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.8 配置管理

7.1.8.8.1 测评单元（L2-MMS1-18）

该测评单元包括以下要求：

- a) 测评指标：应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；
- b) 测评对象：系统管理员；
- c) 测评实施：应访谈系统管理员是否对系统的基本配置信息进行记录和保存；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8.9 密码管理

7.1.8.9.1 测评单元（L2-MMS1-19）

该测评单元包括以下要求：

- a) 测评指标：应使用符合国家密码管理规定的密码技术和产品；
- b) 测评对象：安全管理员；
- c) 测评实施：应核查相关产品是否获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8.10 变更管理

7.1.8.10.1 测评单元（L2-MMS1-20）

该测评单元包括以下要求：

- a) 测评指标：应明确系统变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查变更方案是否包含变更类型、变更原因、变更过程、变更前评估等内容；
 - 2) 应核查是否具有变更方案评审记录和变更过程记录文档。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.11 备份与恢复管理

7.1.8.11.1 测评单元（L2-MMS1-21）

该测评单元包括以下要求：

- a) 测评指标：应识别需要定期备份的重要业务信息、系统数据及软件系统等；
- b) 测评对象：系统管理员、网络管理员、数据库管理员和管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员、数据库管理员和网络管理员是否识别需定期备份的业务信息、系统数据及软件系统；
 - 2) 应核查是否具有定期备份的重要业务信息、系统数据、软件系统的列表或清单。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.11.2 测评单元（L2-MMS1-22）

该测评单元包括以下要求：

- a) 测评指标：应规定备份信息的备份方式、备份频度、存储介质、保存期等；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查备份与恢复管理制度是否明确备份方式、频度、介质、保存期等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8.11.3 测评单元（L2-MMS1-23）

该测评单元包括以下要求：

- a) 测评指标：应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查备份和恢复的策略是否明确备份策略和恢复策略文档规范了数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8.12 安全事件处置

7.1.8.12.1 测评单元（L2-MMS1-24）

该测评单元包括以下要求：

- a) 测评指标：应及时向安全管理部门报告所发现的安全弱点和可疑事件；
- b) 测评对象：运维负责人和管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人是否告知用户在发现安全弱点和可疑事件时应及时向安全管理部门报告；

- 2) 应核查是否有运维过程中发现的安全弱点和可疑事件对应的报告或相关文档,内容是否详实。
- d) 单元判定:如果1)-2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

7.1.8.12.2 测评单元 (L2-MMS1-25)

该测评单元包括以下要求:

- a) 测评指标:应制定安全事件报告和处置管理制度,明确不同安全事件的报告、处置和响应流程,规定安全事件的现场处理、事件报告和后期恢复的管理职责等;
- b) 测评对象:管理制度类文档;
- c) 测评实施:应核查安全事件报告和处置管理制度是否明确了与安全事件有关的工作职责,包括报告单位(人)、接报单位(人)和处置单位等职责;
- d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

7.1.8.12.3 测评单元 (L2-MMS1-26)

该测评单元包括以下要求:

- a) 测评指标:应在安全事件报告和响应处理过程中,分析和鉴定事件产生的原因,收集证据,记录处理过程,总结经验教训;
- b) 测评对象:记录表单类文档;
- c) 测评实施:应核查安全事件报告和响应处置记录是否记录引发安全事件的系统弱点、不同安全事件发生的原因、处置过程、经验教训总结、补救措施等内容;
- d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

7.1.8.13 应急预案管理

7.1.8.13.1 测评单元 (L2-MMS1-27)

该测评单元包括以下要求:

- a) 测评指标:应制定重要事件的应急预案,包括应急处理流程、系统恢复流程等内容;
- b) 测评对象:管理制度类文档;
- c) 测评实施:应核查制定重要事件的应急预案(如针对机房、系统、网络等各个层面);
- d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

7.1.8.13.2 测评单元 (L2-MMS1-28)

该测评单元包括以下要求:

- a) 测评指标:应定期对系统相关的人员进行应急预案培训,并进行应急预案的演练;
- b) 测评对象:运维负责人和记录表单类文档;
- c) 测评实施包括以下内容:
 - 1) 应访谈运维负责人是否定期对相关人员进行应急预案培训和演练;
 - 2) 应核查应急预案培训记录是否明确培训对象、培训内容、培训结果等;
 - 3) 应核查应急预案演练记录是否记录演练时间、主要操作内容、演练结果等。

- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.8.14 外包运维管理

7.1.8.14.1 测评单元 (L2-MMS1-29)

该测评单元包括以下要求：

- a) 测评指标：应确保外包运维服务商的选择符合国家的有关规定；
- b) 测评对象：运维负责人；
- c) 测评实施：应访谈运维负责人是否有外包运维服务情况，若有，外包运维服务的单位是否符合国家有关规定；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.1.8.14.2 测评单元 (L2-MMS1-30)

该测评单元包括以下要求：

- a) 测评指标：应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查外包运维服务协议是否明确约定外包运维的范围和工作内容。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.2 云计算安全测评扩展要求

7.2.1 物理和环境安全

7.2.1.1 物理位置选择

7.2.1.1.1 测评单元 (L2-PES2-01)

该测评单元包括以下要求：

- a) 测评指标：应确保云计算基础设施位于中国境内；
- b) 测评对象：机房管理员、办公场地、机房和平台建设方案；
- c) 测评实施包括以下内容：
 - 1) 应访谈机房管理员云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和数据的软硬件是否均位于中国境内；
 - 2) 应核查云平台建设方案是否明确云计算服务器、云管理平台、信息系统上重要信息的处理、存储、业务的运行需位于中国境内。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.2 网络和通信安全

7.2.2.1 网络架构

7.2.2.1.1 测评单元 (L2-NCS2-01)

该测评单元包括以下要求：

- a) 测评指标：应确保云计算平台不承载高于其安全保护等级的业务应用系统；
- b) 测评对象：云计算平台和业务应用系统定级材料；
- c) 测评实施：应核查云计算平台和云计算平台承载的业务应用系统相关定级材料，查看云计算平台安全保护等级是否不低于其承载的业务应用系统；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.2.1.2 测评单元（L2-NCS2-02）

该测评单元包括以下要求：

- a) 测评指标：应绘制与当前运行情况相符的虚拟化网络拓扑结构图；
- b) 测评对象：综合网管系统、云管理平台、网络拓扑图、网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务商综合网管系统、云管理平台或云服务客户管理平台，核查是否对虚拟化网络资源（如虚拟交换机、虚拟防火墙等）、虚拟网络拓扑进行了绘制；
 - 2) 应核查网络拓扑结构图是否与当前运行情况相符。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.2.1.3 测评单元（L2-NCS2-03）

该测评单元包括以下要求：

- a) 测评指标：应实现不同云服务客户虚拟网络之间的隔离；
- b) 测评对象：网络资源隔离措施、综合网管系统和云管理平台；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户之间虚拟网络隔离措施；
 - 2) 应核查云服务客户之间虚拟网络资源隔离策略是否有效。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.2.1.4 测评单元（L2-NCS2-04）

该测评单元包括以下要求：

- a) 测评指标：应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；
- b) 测评对象：防火墙、入侵检测系统等安全设备；
- c) 测评实施包括以下内容：
 - 1) 核查防火墙、入侵检测系统等设备，是否能为客户提供虚拟化的安全机制；
 - 2) 核查虚拟防火墙、虚拟入侵保护系统等安全机制是否满足客户业务安全需求。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.2.2 访问控制

7.2.2.2.1 测评单元（L2-NCS2-05）

该测评单元包括以下要求：

- a) 测评指标：应禁止云服务客户虚拟机访问宿主机；
- b) 测评对象：云管理平台和虚拟机监视器；
- c) 测评实施：应核查云管理平台等能否检测到云服务客户虚拟机对宿主机的访问；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.2.2.2 测评单元（L2-NCS2-06）

该测评单元包括以下要求：

- a) 测评指标：应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；
- b) 测评对象：访问控制机制、网络边界设备和虚拟化网络边界设备；
- c) 测评实施包括以下内容：
 - 1) 应核查云平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略是否有效；
 - 2) 应核查云平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等是否有效；
 - 3) 应核查不同云服务客户间访问控制规则和访问控制策略是否有效；
 - 4) 应核查云服务客户业务系统不同区域间访问控制规则和访问控制策略是否有效。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.2.2.3 测评单元（L2-NCS2-07）

该测评单元包括以下要求：

- a) 测评指标：应保证当虚拟机迁移时，访问控制策略随其迁移；
- b) 测评对象：虚拟机、虚拟机迁移记录和相关配置；
- c) 测评实施包括以下内容：
 - 1) 应核查虚拟机迁移时访问控制策略随之迁移的措施或手段；
 - 2) 应核查虚拟机迁移记录及相关配置，查看虚拟机迁移后访问控制策略是否部署。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.2.2.4 测评单元（L2-NCS2-08）

该测评单元包括以下要求：

- a) 测评指标：应允许云服务客户设置不同虚拟机之间的访问控制策略；
- b) 测评对象：云服务商管理平台、云服务客户管理系统和虚拟化网络边界访问控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务商的云管理平台等是否允许云服务客户设置不同虚拟机间访问控制策略；
 - 2) 应核查云服务商的云管理平台是否存在不同虚拟机间的访问控制管理模块，是否开启该访问控制功能；
 - 3) 应核查云服务客户管理系统，不同虚拟机间访问控制策略是否安全。
- d) 单元判定：如果 1)、2) 或 3) 为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.2.3 入侵防范

7.2.2.3.1 测评单元（L2-NCS2-09）

该测评单元包括以下要求：

- a) 测评指标：应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；
- b) 测评对象：网络入侵检测系统、入侵保护系统、国家认可的相关机制和入侵防范措施；
- c) 测评实施包括以下内容：
 - 1) 应核查是否有专门设备对网络入侵进行防范，核查网络入侵防范规则库的升级方式；
 - 2) 应核查网络入侵检测系统、入侵保护系统或机制，当采用网络入侵防范机制时所采取的机制是否已被测试是安全的（如第三方测试报告），核查入侵检测系统、入侵保护系统或机制的规则库是否为最新；
 - 3) 应核查系统是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能、报警功能和清洗处置功能；
 - 4) 应核查是否具有对 SQL 注入、跨站脚本等攻击进行检测发现并阻断的能力；
 - 5) 应具有对恶意虚拟机，如具有恶意行为、过分占用计算资源和带宽资源等的虚拟机，进行检测的能力；
 - 6) 应核查云管理平台等对云服务客户攻击的防范措施，核查对云服务客户的网络攻击行为的记录情况，记录应包括攻击类型、攻击时间、攻击流量等；
 - 7) 应对云平台内部发起的恶意攻击或恶意对外连接的行为进行限制，核查是否对内部行为进行监控且保存相关日志记录；
 - 8) 应通过对外攻击发生器伪造对外攻击行为，核查云租的网络攻击的日志记录，确认是否正确记录到相应攻击行为，攻击行为日志记录是否包含攻击类型、攻击时间、攻击者 IP、攻击流量规模等；
 - 9) 应核查运行虚拟机监控器（VMM）和云管理平台软件的物理主机，核查其安全加固手段是否能够应对虚拟化共享带来的安全漏洞。
- d) 单元判定：如果 1) -9) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.2.3.2 测评单元（L2-NCS2-10）

该测评单元包括以下要求：

- a) 测评指标：应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；
- b) 测评对象：网络入侵检测系统、入侵保护系统、国家认可的相关机制和入侵防范措施；
- c) 测评实施包括以下内容：
 - 1) 应核查是否有专门设备对虚拟网络节点的网络攻击行为进行防范，核查网络入侵防范规则库的升级方式；
 - 2) 应核查网络入侵检测系统、入侵保护系统或机制，当对虚拟网络节点采用网络入侵防范机制时，应查看所采取的机制是否有效，查看入侵检测系统、入侵保护系统或机制的规则库是否为最新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.2.3.3 测评单元（L2-NCS2-11）

该测评单元包括以下要求：

- a) 测评指标：应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；
- b) 测评对象：虚拟机、宿主机、入侵检测系统和入侵保护系统；
- c) 测评实施：应核查系统是否具备虚拟机与宿主机之间、虚拟机与虚拟机之间的异常流量、大规模攻击流量、高级持续性攻击的检测功能；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.2.4 安全审计

7.2.2.4.1 测评单元（L2-NCS2-12）

该测评单元包括以下要求：

- a) 测评指标：应对云服务商和云服务客户远程管理时执行特权命令进行审计，至少包括虚拟机删除、虚拟机重启；
- b) 测评对象：边界网络设备、网络虚拟化设备和相关审计数据；
- c) 测评实施包括以下内容：
 - 1) 应核查对云服务商和云服务客户远程管理时执行的远程特权命令后是否有相关审计记录；
 - 2) 当云服务商采用第三方运维时，应核查第三方运维方是否向云服务商提供审计数据，或云服务商是否可采取措施收集相关审计数据；
 - 3) 应核查边界网络设备、网络虚拟化设备远程执行特权命令的限制措施，核查是否对远程执行特权命令的行为进行安全审计，至少包括虚拟机删除、虚拟机重启；
 - 4) 应测试云服务商或云服务客户远程删除或重启虚拟机后，是否有产生相应审计记录。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.3 设备和计算安全

7.2.3.1 身份鉴别

7.2.3.1.1 测评单元（L2-ECS2-01）

该测评单元包括以下要求：

- a) 测评指标：应在网络策略控制器和网络设备（或设备代理）之间建立通信时验证身份；
- b) 测评对象：网络管理员、网络策略控制器和网络设备（代理设备）；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络管理员是否在网络策略控制器和网络设备（或设备代理）之间建立通信时建立身份验证机制；
 - 2) 应核查网络策略控制器和网络设备（或设备代理）之间的身份验证机制；
 - 3) 应对网络策略控制器和网络设备（代理设备）进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）对网络设备进行渗透测试，验证网络设备防护能力是否符合要求，是否在网络策略控制器和网络设备（或设备代理）之间建立通信时建立身份验证机制。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.3.2 访问控制

7.2.3.2.1 测评单元（L2-ECS2-02）

该测评单元包括以下要求：

- a) 测评指标：应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；
- b) 测评对象：云平台、数据库、相关授权文档和管理文档；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户数据管理权限授权流程、授权方式、授权内容；
 - 2) 应核查云计算平台是否具有云服务客户数据的管理权限，如果具有，核查相关授权证明及数据管理权限保护措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.3.3 安全审计

7.2.3.3.1 测评单元（L2-ECS2-03）

该测评单元包括以下要求：

- a) 测评指标：应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计；
- b) 测评对象：安全审计策略、审计设备和审计数据；
- c) 测评实施包括以下内容：
 - 1) 应核查安全审计配置是否能够保证云服务商对云服务客户系统和数据的操作（如增、删、改、查等操作）可被云服务客户审计；
 - 2) 应核查是否支持云服务客户部署第三方安全审计设备，保证云服务商对云服务客户系统和数据的操作可被租户审计；
 - 3) 应核查云服务商与云服务客户收集的审计数据，查看云服务商对云服务客户系统和数据的操作是否可被云服务客户审计。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.3.4 资源控制

7.2.3.4.1 测评单元（L2-ECS2-04）

该测评单元包括以下要求：

- a) 测评指标：应屏蔽虚拟资源故障，某个虚拟机宕机后不影响虚拟机监视器及其他虚拟机；
- b) 测评对象：资源控制相关平台和云平台；
- c) 测评实施包括以下内容：
 - 1) 应核查资源控制相关平台所采取的屏蔽虚拟资源故障措施、相关虚拟机故障记录，核查是否不存在虚拟机崩溃后影响虚拟机监视器及其他虚拟机的历史记录；
 - 2) 应核查云平台所采取的屏蔽虚拟资源故障的技术手段是否能在某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.3.4.2 测评单元（L2-ECS2-05）

该测评单元包括以下要求：

- a) 测评指标：应对物理资源和虚拟资源按照策略做统一管理调度与分配；
- b) 测评对象：运营管理平台、资源调度平台和云管理平台；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户的运营管理平台或资源调度平台的资源调度策略、资源调度分配情况；
 - 2) 应核查云服务商云管理平台所提供策略能否对物理资源和虚拟资源做统一管理调度与分配。
- d) 单元判定：如果 1)-2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.3.4.3 测评单元（L2-ECS2-06）

该测评单元包括以下要求：

- a) 测评指标：应确保云计算平台具有虚拟机内存隔离措施；
- b) 测评对象：云管理平台和虚拟机监视器；
- c) 测评实施包括以下内容：
 - 1) 应核查云管理平台和虚拟机监视器的计算资源分配情况、资源分配的审计记录或告警记录是否不存在内存资源过量占用警告；
 - 2) 应核查云计算平台和虚拟机监视器的虚拟机内存隔离措施或机制。
- d) 单元判定：如果 1)-2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.3.5 镜像和快照保护

7.2.3.5.1 测评单元（L2-ECS2-07）

该测评单元包括以下要求：

- a) 测评指标：应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
- b) 测评对象：云管理平台、虚拟机监视器和虚拟机镜像文件；
- c) 测评实施包括以下内容：
 - 1) 应核查虚拟机监视器是否有对镜像文件定期进行有效性验证的记录；
 - 2) 应核查虚拟机监视器，云管理平台是否提供有效的虚拟机镜像和快照文件管理机制，虚拟机是否能够及时被备份和快照，以及是否准确地恢复到所需还原点；
 - 3) 应核查虚拟机监视器，云管理平台是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。
- d) 单元判定：如果 1)-3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.3.5.2 测评单元（L2-ECS2-08）

该测评单元包括以下要求：

- a) 测评指标：应针对重要业务系统提供加固的操作系统镜像；
- b) 测评对象：云管理平台、虚拟机监视器和虚拟机镜像文件；
- c) 测评实施：应核查虚拟机监视器，云管理平台是否对生成的虚拟机镜像进行必要的加固措施，如关闭不必要的端口、服务及进行安全加固配置；

- d) 单元判定：如果以上测评实施内容均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.4 应用和数据安全

7.2.4.1 数据完整性

7.2.4.1.1 测评单元（L2-ADS2-01）

该测评单元包括以下要求：

- a) 测评指标：应确保虚拟机迁移过程中，重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；
- b) 测评对象：虚拟机；
- c) 测评实施包括以下内容：
 - 1) 应核查虚拟资源迁移过程中采用的数据完整性保障措施及恢复措施；
 - 2) 应核查在虚拟资源迁移过程中，是否采取加密、签名等措施保证虚拟资源数据及重要数据的完整性，并在检测到完整性受到破坏时是否采取必要的恢复措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.4.2 数据备份恢复

7.2.4.2.1 测评单元（L2-ADS2-02）

该测评单元包括以下要求：

- a) 测评指标：应提供查询云服务客户数据及备份存储位置的方式；
- b) 测评对象：云管理平台、云平台和相关技术文档；
- c) 测评实施包括以下内容：
 - 1) 应核查云管理平台或云平台为云服务客户提供数据及备份存储位置的查询记录；
 - 2) 应核查云服务商是否为云服务客户提供数据及备份存储位置查询的接口或其他技术、管理手段。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.4.2.2 测评单元（L2-ADS2-03）

该测评单元包括以下要求：

- a) 测评指标：云服务客户应在本地保存其业务数据的备份；
- b) 测评对象：虚拟机、虚拟机监视器和云平台；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否采取措施使云服务客户可以在本地保存其业务数据的备份；
 - 2) 应核查是否提供备份措施保证云服务客户可以在本地保存其业务数据。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.4.3 剩余信息保护

7.2.4.3.1 测评单元（L2-ADS2-04）

该测评单元包括以下要求：

- a) 测评指标：应保证虚拟机所使用的内存和存储空间回收时得到完全清除；
- b) 测评对象：系统管理员、虚拟机、虚拟机监视器系统、云管理平台系统、操作系统技术开发手册或产品检测报告、数据库系统技术开发手册和产品检测报告；
- c) 测评实施包括以下内容：
 - 1) 应核查资源抽象层用户的鉴别信息存储空间在回收时的数据清除策略；
 - 2) 应核查系统和数据库系统技术开发手册或产品检测报告，查看用户的鉴别信息存储空间回收时是否得到完全清除；
 - 3) 应核查操作系统和数据库系统技术开发手册或产品检测报告，查看文件、目录和数据库记录等资源所在的存储空间回收时是否得到完全清除。
 - 4) 应核查虚拟机监视器和云管理平台内的文件、目录、数据库记录和虚拟资源等所在的存储空间回收时是否得到完全清除；
 - 5) 应核查虚拟机的内存和存储空间回收时，是否得到完全清除；
 - 6) 应核查在迁移或删除虚拟机后，数据以及备份数据（如镜像文件、快照文件等）是否已清理。
- d) 单元判定：如果 1) -6) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.4.3.2 测评单元（L2-ADS2-05）

该测评单元包括以下要求：

- a) 测评指标：云服务客户删除业务应用数据时，云计算平台应确保云存储中所有副本被删除；
- b) 测评对象：云存储和云计算平台；
- c) 测评实施包括以下内容：
 - 1) 应核查云平台中云服务客户业务应用数据备份方式和备份管理方式，当云服务客户删除业务应用数据时，核查是否支持所有副本删除；
 - 2) 应核查云计算平台，当云服务客户删除业务应用数据时，云存储中所有副本是否被删除。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.4.4 个人信息保护

7.2.4.4.1 测评单元（L2-ADS2-06）

该测评单元包括以下要求：

- a) 测评指标：应确保云服务客户账户信息、鉴别信息、系统信息存储于中国境内，如需出境应遵循国家相关规定；
- b) 测评对象：数据库服务器、数据存储设备和管理文档记录；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户账户信息、鉴别信息、系统信息所在的服务器及数据存储设备是否存储于中国境内；
 - 2) 应核查相关管理文档或记录，核查云服务客户账户信息、鉴别信息、系统信息及其备份是否存储于中国境内。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.5 安全建设管理

7.2.5.1 云服务商选择

7.2.5.1.1 测评单元（L2-CMS2-01）

该测评单元包括以下要求：

- a) 测评指标：应选择安全合规的云服务商，其所提供的云平台应为其所承载的业务应用系统提供相应等级的安全保护能力；
- b) 测评对象：系统建设负责人、安全责任合同书、保密协议和服务合同；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统建设负责人是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云平台及云服务商；
 - 2) 应核查云服务商提供的相关服务合同是否明确其云平台具有与所承载的业务应用系统相应或高于的安全保护能力。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.5.1.2 测评单元（L2-CMS2-02）

该测评单元包括以下要求：

- a) 测评指标：应在服务水平协议中规定云服务的各项服务内容和具体技术指标；
- b) 测评对象：服务水平协议；
- c) 测评实施：应核查服务水平协议是否规定了云服务的各项服务内容和具体指标、服务期限、双方签字或盖章等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.5.1.3 测评单元（L2-CMS2-03）

该测评单元包括以下要求：

- a) 测评指标：应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；
- b) 测评对象：服务水平协议；
- c) 测评实施：应核查服务水平协议中是否规范了安全服务商和云服务供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.5.1.4 测评单元（L2-CMS2-04）

该测评单元包括以下要求：

- a) 测评指标：应在服务水平协议中规定服务合约到期时，完整地返还云服务客户信息，并承诺相关信息在云计算平台上清除；
- b) 测评对象：服务水平协议；
- c) 测评实施：应核查服务水平协议是否明确服务合约到期时，云服务商完整地返还云服务客户信息，并承诺相关信息在云平台上清除；

- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.5.2 供应链管理

7.2.5.2.1 测评单元（L2-CMS2-05）

该测评单元包括以下要求：

- a) 测评指标：应确保供应商的选择符合国家有关规定；
- b) 测评对象：系统建设负责人；
- c) 测评实施：应访谈系统建设负责人云服务商的选择是否符合国家的有关规定；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

7.2.5.2.2 测评单元（L2-CMS2-06）

该测评单元包括以下要求：

- a) 测评指标：应确保供应链安全事件信息或威胁信息能够及时传达到云服务客户；
- b) 测评对象：系统建设负责人、供应链安全事件或威胁报告；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统建设负责人云服务商供应商是否及时传达安全事件或威胁信息；
 - 2) 应核查供应链安全事件或威胁报告是否明确相关事件信息或威胁信息。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.6 安全运维管理

7.2.6.1 云计算环境管理

7.2.6.1.1 测评单元（L2-MMS2-01）

该测评单元包括以下要求：

- a) 测评指标：云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定；
- b) 测评对象：运维设备、运维地点、运维记录和相关管理文档；
- c) 测评实施包括以下内容：
 - 1) 应核查运维地点是否位于中国境内，是否不存在从境外对境内云计算平台实施远程运维的设备、地点和相关内容；
 - 2) 应核查云计算平台远程运维记录中境外对境内云计算平台实施运维操作是否遵循国家相关规定。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.2.6.1.2 测评单元（L2-MMS2-02）

该测评单元包括以下要求：

- a) 测评指标：云计算平台运维过程产生的配置数据、日志信息等存储于中国境内，如需出境应遵循国家相关规定；

- b) 测评对象：云计算平台运行管理设计文档和管理文档；
- c) 测评实施包括以下内容：
 - 1) 应核查云计算平台运维过程产生的配置数据、日志信息等是否存储于中国境内；
 - 2) 对于有出境需求的配置数据和日志信息，应核查数据出境是否遵循国家相关规定。
- d) 单元判定：如果 1) 或 2) 为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

7.3 移动互联安全测评扩展要求

7.3.1 物理和环境安全

7.3.1.1 无线接入点的物理位置

7.3.1.1.1 测评单元（L2-PES3-01）

该测评单元包括以下要求：

- a) 测评指标：应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰；
- b) 测评对象：无线接入设备；
- c) 测评实施包括以下内容：
 - 1) 应核查物理位置与无线信号的覆盖范围；
 - 2) 应测试无线信号的覆盖范围并测试在一定范围内是否可以进行电磁干扰。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.2 网络和通信安全

7.3.2.1 边界防护

7.3.2.1.1 测评单元（L2-NCS3-01）

该测评单元包括以下要求：

- a) 测评指标：应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备；
- b) 测评对象：无线接入网关设备；
- c) 测评实施：应核查有线网络与无线网络边界之间是否部署无线接入网关设备；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.2.2 访问控制

7.3.2.2.1 测评单元（L2-NCS3-02）

该测评单元包括以下要求：

- a) 测评指标：无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符；
- b) 测评对象：无线接入设备；
- c) 测评实施：应核查是否开启接入认证功能，是否使用除 WEP 方式以外的其它方式进行认证，密钥长度不小于 8 位；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.2.3 入侵防范

7.3.2.3.1 测评单元 (L2-NCS3-03)

该测评单元包括以下要求：

- a) 测评指标：应能够检测、记录非授权无线接入设备；
- b) 测评对象：入侵防范设备；
- c) 测评实施：应核查是否能够检测、记录非授权无线接入设备；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.2.3.2 测评单元 (L2-NCS3-04)

该测评单元包括以下要求：

- a) 测评指标：应能够对非授权移动终端接入的行为进行检测、记录；
- b) 测评对象：入侵防范设备；
- c) 测评实施：应核查是否能够检测、记录非授权移动终端的接入行为；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.2.3.3 测评单元 (L2-NCS3-05)

该测评单元包括以下要求：

- a) 测评指标：应具备对针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录；
- b) 测评对象：入侵防范设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否能够对网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录；
 - 2) 应核查规则库版本，查看其规则库是否及时更新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.2.3.4 测评单元 (L2-NCS3-06)

该测评单元包括以下要求：

- a) 测评指标：应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；
- b) 测评对象：入侵防范设备；
- c) 测评实施：应核查入侵防范设备，是否能够检测无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.2.3.5 测评单元 (L2-NCS3-07)

该测评单元包括以下要求：

- a) 测评指标：应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等；
- b) 测评对象：无线接入设备和无线接入网关设备；

- c) 测评实施：应核查是否关闭了 SSID 广播、WEP 认证等存在风险的功能；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.2.3.6 测评单元（L2-NCS3-08）

该测评单元包括以下要求：

- a) 测评指标：应禁止多个 AP 使用同一个鉴别密钥；
- b) 测评对象：无线接入设备；
- c) 测评实施：应核查是否分别使用了不同的鉴别密钥；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.3 设备和计算安全

7.3.3.1 移动应用管控

7.3.3.1.1 测评单元（L2-ECS3-01）

该测评单元包括以下要求：

- a) 测评指标：应具有选择应用软件安装、运行的功能；
- b) 测评对象：移动终端管理客户端；
- c) 测评实施：应核查是否具有选择应用软件安装、运行的功能；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.3.1.2 测评单元（L2-ECS3-02）

该测评单元包括以下要求：

- a) 测评指标：应具有软件白名单功能，应能根据白名单控制应用软件安装、运行；
- b) 测评对象：移动终端管理客户端；
- c) 测评实施包括以下内容：
 - 1) 应核查是否具有软件白名单功能；
 - 2) 应测试使用白名单控制应用软件安装、运行。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.3.1.3 测评单元（L2-ECS3-03）

该测评单元包括以下要求：

- a) 测评指标：应具有应用软件权限控制功能，应能控制应用软件对移动终端中资源访问；
- b) 测评对象：移动终端管理客户端；
- c) 测评实施包括以下内容：
 - 1) 应核查是否具有应用软件权限控制功能；
 - 2) 应测试是否可以对移动终端中资源的访问进行限制。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.3.1.4 测评单元（L2-ECS3-04）

该测评单元包括以下要求：

- a) 测评指标：应只允许可靠证书签名的应用软件安装和运行；
- b) 测评对象：移动终端管理客户端；
- c) 测评实施：应核查允许使用的签名证书；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.3.2 资源控制

7.3.3.2.1 测评单元（L2-ECS3-05）

该测评单元包括以下要求：

- a) 测评指标：应保证移动终端处理不同等级系统业务的运行环境进行应用级隔离；
- b) 测评对象：移动终端；
- c) 测评实施：应核查是否采用安全隔离手段或措施进行应用级隔离；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.3.2.2 测评单元（L2-ECS3-06）

该测评单元包括以下要求：

- a) 测评指标：应限制用户或进程对移动终端系统资源的最大使用限度，防止移动终端被提权；
- b) 测评对象：移动终端；
- c) 测评实施：应核查是否可以对用户或进程等可访问资源进行限定，是否可以防止移动终端被提权；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.4 安全建设管理

7.3.4.1 移动应用软件采购

7.3.4.1.1 测评单元（L2-CMS3-01）

该测评单元包括以下要求：

- a) 测评指标：应保证移动终端安装、运行的应用软件来自可靠证书签名或可靠分发渠道；
- b) 测评对象：安全管理员；
- c) 测评实施：应访谈安全管理员，移动终端安装、运行的应用软件是否采用可靠的证书签名或使用可靠的分发渠道；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.4.1.2 测评单元（L2-CMS3-02）

该测评单元包括以下要求：

- a) 测评指标：应保证移动终端安装、运行的移动应用软件由可靠的开发者开发；
- b) 测评对象：安全管理员；

- c) 测评实施：应访谈安全管理员，移动应用软件是否由可靠的开发者开发；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.4.2 移动应用软件开发

7.3.4.2.1 测评单元（L2-CMS3-03）

该测评单元包括以下要求：

- a) 测评指标：应要求对移动业务应用软件开发进行资格审查；
- b) 测评对象：系统建设负责人；
- c) 测评实施：应访谈系统建设负责人，是否对开发者进行资格审查；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.3.4.2.2 测评单元（L2-CMS3-04）

该测评单元包括以下要求：

- a) 测评指标：应要求开发移动业务应用软件的签名证书合法性；
- b) 测评对象：移动应用软件；
- c) 测评实施：应核查开发移动业务应用软件的签名证书是否具有合法性；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.4 物联网安全测评扩展要求

7.4.1 物理和环境安全

7.4.1.1 感知节点设备物理防护

7.4.1.1.1 测评单元（L2-PES4-01）

该测评单元包括以下要求：

- a) 测评指标：感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；
- b) 测评对象：感知节点设备所处物理环境和设计或验收文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈物理安全负责人现有感知节点设备的环境条件是否具有防挤压、防强振动等防物理破坏的能力；
 - 2) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备所处物理环境具有防挤压、防强振动等能力的说明，是否与实际情况一致；
 - 3) 应核查感知节点设备所处物理环境是否采取了防挤压、防强振动等的防护措施。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.1.1.2 测评单元（L2-PES4-02）

该测评单元包括以下要求：

- a) 测评指标：感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）；

- b) 测评对象：感知节点设备所处物理环境和设计或验收文档；
- c) 测评实施包括以下内容：
 - 1) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备在工作状态所处物理环境的说明，是否与实际情况一致；
 - 2) 应核查感知节点设备在工作状态所处物理环境是否能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.2 网络和通信安全

7.4.2.1 入侵防范

7.4.2.1.1 测评单元（L2-NCS4-01）

该测评单元包括以下要求：

- a) 测评指标：应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为；
- b) 测评对象：感知节点设备和设计文档；
- c) 测评实施包括以下内容：
 - 1) 应核查感知层安全设计文档，是否有对感知节点通信目标地址的控制措施说明；
 - 2) 应核查感知节点设备，是否配置了对感知节点通信目标地址的控制措施，相关参数配置是否符合设计要求。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.2.1.2 测评单元（L2-NCS4-02）

该测评单元包括以下要求：

- a) 测评指标：应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为；
- b) 测评对象：网关节点设备和设计文档；
- c) 测评实施包括以下内容：
 - 1) 应核查感知层安全设计文档，是否有对网关节点通信目标地址的控制措施说明；
 - 2) 应核查网关节点设备，是否配置了对网关节点通信目标地址的控制措施，相关参数配置是否符合设计要求。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.2.2 接入控制

7.4.2.2.1 测评单元（L2-NCS4-03）

该测评单元包括以下要求：

- a) 测评指标：应确保只有授权的感知节点可以接入；
- b) 测评对象：感知节点设备和设计文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术或其他技术手段，具体措施有哪些；

- 2) 应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制描述。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.3 安全运维管理

7.4.3.1 感知节点管理

7.4.3.1.1 测评单元 (L2-MMS4-01)

该测评单元包括以下要求：

- a) 测评指标：应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；
- b) 测评对象：维护记录；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统运维负责人是否有专门的人员对感知节点设备、网关节点设备进行定期维护，由何部门或何人负责，维护周期多长；
 - 2) 应核查感知节点设备、网关节点设备部署环境维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.3.1.2 测评单元 (L2-MMS4-02)

该测评单元包括以下要求：

- a) 测评指标：应记录感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息），对网关设备进行现场维护（除尘、充电、修理等）；
- b) 测评对象：维护记录；
- c) 测评实施：应核查感知节点设备、网关节点设备部署环境维护记录是否包括了感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息）核查、对网关设备进行现场维护（除尘、充电、修理等）等方面内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.3.1.3 测评单元 (L2-MMS4-03)

该测评单元包括以下要求：

- a) 测评指标：应对感知节点和网关节点设备部署环境的评估方法作出明确规定；
- b) 测评对象：感知节点和网关节点设备部署环境的评估说明文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统运维负责人是否明确规定需对感知节点和网关节点设备部署环境进行评估；
 - 2) 应核查感知节点和网关节点设备部署环境的评估说明文档内容是否包含可操作的评估方法。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.3.1.4 测评单元（L2-MMS4-04）

该测评单元包括以下要求：

- a) 测评指标：应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；
- b) 测评对象：感知节点和网关节点设备安全管理文档；
- c) 测评实施：
 - 1) 应访谈系统运维负责人是否明确规定需对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程进行全程管理；
 - 2) 应核查感知节点和网关节点设备安全管理文档是否覆盖感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等方面。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5 工业控制系统安全测评扩展要求

7.5.1 物理和环境安全

7.5.1.1 室外控制设备物理防护

7.5.1.1.1 测评单元（L2-PES5-01）

该测评单元包括以下要求：

- a) 测评指标：室外控制设备应放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；控制设备应安装在金属或其它绝缘板上（非木质板），并紧固于箱体或装置中；
- b) 测评对象：室外控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；
 - 2) 应核查是否安装在金属或其它绝缘板上（非木质板），并紧固于箱体或装置中。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.1.1.2 测评单元（L2-PES5-02）

该测评单元包括以下要求：

- a) 测评指标：室外控制设备放置应远离强电磁干扰、热源和应远离极端天气环境等，如无法避免，在遇到极端天气时应及时做好应急处置及检修确保设备正常运行；
- b) 测评对象：室外控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否远离极端天气环境；
 - 2) 应核查是否有极端天气时的应急处置及检修维护记录；
 - 3) 应核查位置放置是否远离强电磁干扰和热源。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.2 网络和通信安全

7.5.2.1 网络架构

7.5.2.1.1 测评单元（L2-NCS5-01）

该测评单元包括以下要求：

- a) 测评指标：工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用技术隔离手段；
- b) 测评对象：网闸、路由器、交换机和防火墙等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查工业控制系统的网络是否部署单向隔离设备；
 - 2) 应核查在网络边界处是否采用了有效的隔离策略；
 - 3) 应核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离强度相同的措施。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.2.1.2 测评单元（L2-NCS5-02）

该测评单元包括以下要求：

- a) 测评指标：工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；
- b) 测评对象：路由器、交换机和防火墙等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查工业控制系统内部不同的子系统类型，是否按照安全等级和安全防护强度等业务特点划分了不同的安全域；
 - 2) 应核查各安全域之间交换机和防火墙是否配置了有效的访问控制策略。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.2.1.3 测评单元（L2-NCS5-03）

该测评单元包括以下要求：

- a) 测评指标：涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其它数据网及外部公共信息网的安全隔离；
- b) 测评对象：路由器和交换机等提供网络通信功能的设备；
- c) 测评实施：应核查工业控制系统关键区域的传输数据要求，涉及实时传输数据与控制要求的，核查是否采用独立的网络和设备组网实现关键部位安全防护；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.5.2.2 通信传输

7.5.2.2.1 测评单元（L2-NCS5-04）

该测评单元包括以下要求：

- a) 测评指标：在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输；
- b) 测评对象：加密认证设备、路由器、交换机和防火墙等提供访问控制功能的设备；

- c) 测评实施：应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.5.2.3 访问控制

7.5.2.3.1 测评单元（L2-NCS5-05）

该测评单元包括以下要求：

- a) 测评指标：工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查在工业控制系统与企业其他系统之间的网络边界是否部署访问控制设备，是否配置访问控制策略；
 - 2) 应核查设备安全策略，是否禁止 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越边界。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.2.3.2 测评单元（L2-NCS5-06）

该测评单元包括以下要求：

- a) 测评指标：应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备，监控预警设备；
- c) 测评实施包括以下内容：
 - 1) 应核查设备是否可以在策略失效的时候进行告警；
 - 2) 应核查是否部署监控预警系统或相关模块，在边界防护机制失效时可及时告警。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.2.4 拨号使用控制

7.5.2.4.1 测评单元（L2-NCS5-07）

该测评单元包括以下要求：

- a) 测评指标：工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量；并采取用户身份鉴别和访问控制等措施；
- b) 测评对象：拨号服务类设备；
- c) 测评实施包括以下内容：
 - 1) 应核查工业控制系统是否确需使用拨号服务；
 - 2) 应核查拨号设备是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用账户/口令等身份鉴别方式，是否采用控制账户权限等访问控制措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.2.5 无线使用控制

7.5.2.5.1 测评单元（L2-NCS5-08）

该测评单元包括以下要求：

- a) 测评指标：应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；
- b) 测评对象：无线通信网络及设备；
- c) 测评实施包括以下内容：
 - 1) 应核查无线通信的用户在登录时是否采用了身份鉴别措施；
 - 2) 应核查无线通信的用户列表，核查用户身份标识是否具有唯一性。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.2.5.2 测评单元（L2-NCS5-09）

该测评单元包括以下要求：

- a) 测评指标：应对所有参与无线通信的用户（人员、软件进程或者设备）进行授权以及执行使用进行限制；
- b) 测评对象：无线通信网络及设备；
- c) 测评实施：应核查无线通信过程中是否对用户进行授权，核查具体权限是否合理；核查未授权的使用是否可以被发现及告警；
- d) 单元判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.5.3 设备和计算安全

7.5.3.1 控制设备安全

7.5.3.1.1 测评单元（L2-ECS5-01）

该测评单元包括以下要求：

- a) 测评指标：控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等设备和计算方面的安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；
- b) 测评对象：控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；
 - 2) 如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。
- d) 单元判定：如果 2) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.5.3.1.2 测评单元（L2-ECS5-02）

该测评单元包括以下要求：

- a) 测评指标：应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；
- b) 测评对象：控制设备；

- c) 测评实施包括以下内容：
 - 1) 应核查测试环境或测试报告，核查是否有测试评估记录；
 - 2) 应核查控制设备版本、补丁及固件是否经过充分测试后进行了更新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.4 安全建设管理

7.5.4.1 产品采购和使用

7.5.4.1.1 测评单元（L2-CMS5-01）

该测评单元包括以下要求：

- a) 测评指标：工业控制系统重要设备及专用信息安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用；
- b) 测评对象：安全管理员和检测报告类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员系统使用的工业控制系统重要设备及专用信息安全产品是否通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测；
 - 2) 应核查工业控制系统是否有通过国家及行业监管部门认可的专业机构出具的安全性及电磁兼容性检测的检测报告。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.4.2 外包软件开发

7.5.4.2.1 测评单元（L2-CMS5-02）

该测评单元包括以下要求：

- a) 测评指标：应在外包开发合同中包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款；
- b) 测评对象：外包合同；
- c) 测评实施：应核查外包开发合同中是否包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

7.5.5 安全运维管理

7.5.5.1 漏洞和风险管理

7.5.5.1.1 测评单元（L2-MMS5-01）

该测评单元包括以下要求：

- a) 测评指标：应采取必要的措施识别安全漏洞和隐患，并根据风险分析的后果，对发现的安全漏洞和隐患在确保安全生产的情况下及时进行修补；或评估可能的影响后采取必要的补救措施，补救措施宜在系统维护期间开展；
- b) 测评对象：安全管理员、管理制度类文档和记录表单类文档；

- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否采取必要的措施识别安全漏洞隐患，并根据风险分析的后果，对发现的安全漏洞和隐患在确保安全生产的情况下及时进行修补；
 - 2) 应核查是否有文档描述了存在的漏洞、严重级别、原因分析和改进意见等方面；
 - 3) 应核查是否有维护期间设备检修记录，查阅相关修补说明。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.5.2 恶意代码防范管理

7.5.5.2.1 测评单元 (L2-MMS5-02)

该测评单元包括以下要求：

- a) 测评指标：在更新恶意代码库、木马库以及规则库前，应首先在测试环境中测试通过，对隔离区域恶意代码更新应有专人负责，更新操作应离线进行，并保存更新记录；
- b) 测评对象：安全管理员、管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否在更新恶意代码库、木马库以及规则库前在实验环境进行测试，对隔离区域恶意代码更新是否有专人负责，更新操作是否离线进行，是否保存更新记录；
 - 2) 应核查恶意代码防范管理制度中是否对恶意代码库升级测试及更新等流程提出相关要求；
 - 3) 应核查恶意代码库升级测试及更新记录是否与制度要求相符。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.5.5.3 安全事件处置

7.5.5.3.1 测评单元 (L2-MMS5-03)

该测评单元包括以下要求：

- a) 测评指标：应建立工业控制系统联合防护和应急机制，负责处置跨单位工业控制系统安全事件；
- b) 测评对象：安全管理员、管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否建立跨单位处置工业控制系统安全事件流程；
 - 2) 应核查跨单位安全事件报告和处置管理制度，核查是否含有工业控制系统联合防护和应急的相关内容。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8 第三级测评要求

8.1 安全测评通用要求

8.1.1 物理和环境安全

8.1.1.1 物理位置选择

8.1.1.1.1 测评单元 (L3-PES1-01)

该测评单元包括以下要求：

- a) 测评指标：机房场地应选择在具有防震、防风和防雨等能力的建筑内；
- b) 测评对象：记录类文档和机房。
- c) 测评实施包括以下内容：
 - 1) 应核查所在建筑物是否具有建筑物抗震设防审批文档；
 - 2) 应核查机房是否不存在雨水渗漏；
 - 3) 应核查门窗是否不存在因风导致的尘土严重；
 - 4) 应核查屋顶、墙体、门窗和地面等是否不存在破损开裂。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.1.2 测评单元（L3-PES1-02）

该测评单元包括以下要求：

- a) 测评指标：机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施；
- b) 测评对象：机房；
- c) 测评实施：应核查机房是否不位于所在建筑物的顶层或地下室，如果否，则核查机房是否采取了防水和防潮措施；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.1.2 物理访问控制

8.1.1.2.1 测评单元（L3-PES1-03）

该测评单元包括以下要求：

- a) 测评指标：机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员；
- b) 测评对象：机房电子门禁系统；
- c) 测评实施包括以下内容：
 - 1) 应核查出入口是否配置电子门禁系统；
 - 2) 应核查电子门禁系统是否可以鉴别、记录进入的人员信息。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.3 防盗窃和防破坏

8.1.1.3.1 测评单元（L3-PES1-04）

该测评单元包括以下要求：

- a) 测评指标：应将机房设备或主要部件进行固定，并设置明显的不易除去的标记；
- b) 测评对象：机房设备或主要部件；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内设备或主要部件是否固定；
 - 2) 应核查机房内设备或主要部件上是否设置了明显且不易除去的标记。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.3.2 测评单元（L3-PES1-05）

该测评单元包括以下要求：

- a) 测评指标：应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
- b) 测评对象：机房通信线缆；
- c) 测评实施：应核查机房内通信线缆是否铺设在隐蔽处或桥架中；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.1.3.3 测评单元（L3-PES1-06）

该测评单元包括以下要求：

- a) 测评指标：应设置机房防盗报警系统或设置有专人值守的视频监控系统；
- b) 测评对象：机房防盗报警系统或视频监控系统；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否配置防盗报警系统或专人值守的视频监控系统；
 - 2) 应核查防盗报警系统或视频监控系统是否启用。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.4 防雷击

8.1.1.4.1 测评单元（L3-PES1-07）

该测评单元包括以下要求：

- a) 测评指标：应将各类机柜、设施和设备等通过接地系统安全接地；
- b) 测评对象：机房；
- c) 测评实施：应核查机房内机柜、设施和设备等是否进行接地处理；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.1.4.2 测评单元（L3-PES1-08）

该测评单元包括以下要求：

- a) 测评指标：应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等；
- b) 测评对象：机房防雷设施；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否设置防感应雷措施；
 - 2) 应核查防雷装置是否通过验收或国家有关部门的技术检测。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.5 防火

8.1.1.5.1 测评单元（L3-PES1-09）

该测评单元包括以下要求：

- a) 测评指标：应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；

- b) 测评对象：机房防火设施；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否设置火灾自动消防系统；
 - 2) 应核查火灾自动消防系统是否可以自动检测火情、自动报警并自动灭火。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.5.2 测评单元 (L3-PES1-10)

该测评单元包括以下要求：

- a) 测评指标：机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
- b) 测评对象：机房验收类文档；
- c) 测评实施：应核查机房验收文档是否明确相关建筑材料的耐火等级；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.1.5.3 测评单元 (L3-PES1-11)

该测评单元包括以下要求：

- a) 测评指标：应对机房划分区域进行管理，区域和区域之间设置隔离防火措施；
- b) 测评对象：机房管理员和机房；
- c) 测评实施包括以下内容：
 - 1) 应访谈机房管理员是否进行了区域划分；
 - 2) 应核查各区域间是否采取了防火措施进行隔离。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.6 防水和防潮

8.1.1.6.1 测评单元 (L3-PES1-12)

该测评单元包括以下要求：

- a) 测评指标：应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- b) 测评对象：机房；
- c) 测评实施：应核查窗户、屋顶和墙壁是否采取了防雨水渗透的措施；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.1.6.2 测评单元 (L3-PES1-13)

该测评单元包括以下要求：

- a) 测评指标：应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
- b) 测评对象：机房；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否采取了防止水蒸气结露的措施；
 - 2) 应核查机房内是否采取了排泄地下积水，防止地下积水渗透的措施。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.6.3 测评单元 (L3-PES1-14)

该测评单元包括以下要求：

- a) 测评指标：应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警；
- b) 测评对象：机房防水检测设施；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否安装了对水敏感的检测装置；
 - 2) 应核查防水检测和报警装置是否启用。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.7 防静电

8.1.1.7.1 测评单元 (L3-PES1-15)

该测评单元包括以下要求：

- a) 测评指标：应安装防静电地板并采用必要的接地防静电措施；
- b) 测评对象：机房；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否安装了防静电地板；
 - 2) 应核查机房内是否采用了接地防静电措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.7.2 测评单元 (L3-PES1-16)

该测评单元包括以下要求：

- a) 测评指标：应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等；
- b) 测评对象：机房；
- c) 测评实施：应核查机房内是否配备了防静电设备。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.1.8 温湿度控制

8.1.1.8.1 测评单元 (L3-PES1-17)

该测评单元包括以下要求：

- a) 测评指标：机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内；
- b) 测评对象：机房温湿度调节设施；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否配备了专用空调；
 - 2) 应核查机房内温湿度是否在设备运行所允许的范围之内。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.9 电力供应

8.1.1.9.1 测评单元 (L3-PES1-18)

该测评单元包括以下要求：

- a) 测评指标：应在机房供电线路上配置稳压器和过电压防护设备；
- b) 测评对象：机房供电设施；
- c) 测评实施：应核查供电线路上是否配置了稳压器和过电压防护设备；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.1.9.2 测评单元 (L3-PES1-19)

该测评单元包括以下要求：

- a) 测评指标：应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；
- b) 测评对象：机房备用供电设施；
- c) 测评实施包括以下内容：
 - 1) 应核查是否配备 UPS 等后备电源系统。
 - 2) 应核查 UPS 等后备电源系统是否满足设备在断电情况下的正常运行要求。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.9.3 测评单元 (L3-PES1-20)

该测评单元包括以下要求：

- a) 测评指标：应设置冗余或并行的电力电缆线路为计算机系统供电；
- b) 测评对象：机房；
- c) 测评实施：应核查机房内是否设置了冗余或并行的电力电缆线路为计算机系统供电；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.1.10 电磁防护

8.1.1.10.1 测评单元 (L3-PES1-21)

该测评单元包括以下要求：

- a) 测评指标：电源线和通信线缆应隔离铺设，避免互相干扰；
- b) 测评对象：机房线缆；
- c) 测评实施：应核查机房内电源线缆和通信线缆是否隔离铺设；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.1.10.2 测评单元 (L3-PES1-22)

该测评单元包括以下要求：

- a) 测评指标：应对关键设备实施电磁屏蔽；

- b) 测评对象：机房关键设备；
- c) 测评实施：应核查机房内是否为关键设备配备了电磁屏蔽装置；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.2 网络和通信安全

8.1.2.1 网络架构

8.1.2.1.1 测评单元（L3-NCS1-01）

该测评单元包括以下要求：

- a) 测评指标：应保证网络设备的业务处理能力满足业务高峰期需要；
- b) 测评对象：路由器、交换机和防火墙提供网络通信功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查业务高峰时期一段时间内主要网络设备的 CPU 使用率和内存使用率是否满足需要；
 - 2) 应核查网络设备是否从未出现过宕机情况。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.1.2 测评单元（L3-NCS1-02）

该测评单元包括以下要求：

- a) 测评指标：应保证网络各个部分的带宽满足业务高峰期需要；
- b) 测评对象：综合网管系统；
- c) 测评实施：应核查综合网管系统各通信链路带宽是否满足高峰时段的业务流量需要；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.2.1.3 测评单元（L3-NCS1-03）

该测评单元包括以下要求：

- a) 测评指标：应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
- b) 测评对象：路由器、交换机和防火墙等提供网络通信功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否依据某种原则划分不同的网络区域；
 - 2) 应核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.1.4 测评单元（L3-NCS1-04）

该测评单元包括以下要求：

- a) 测评指标：应避免将重要网络区域部署在网络边界处且没有边界防护措施；
- b) 测评对象：网络拓扑图；
- c) 测评实施包括以下内容：
 - 1) 应核查网络拓扑图是否与实际网络运行环境一致；
 - 2) 应核查重要网络区域未部署在网络边界处且无边界防护措施；

- 3) 应核查重要网络区域与其他网络区域之间是否采取可靠的技术隔离手段，如网闸、防火墙和设备访问控制列表（ACL）等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.1.5 测评单元（L3-NCS1-05）

该测评单元包括以下要求：

- a) 测评指标：应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性；
- b) 测评对象：网络拓扑图；
- c) 测评实施：应核查系统是否有主要网络设备、安全设备的硬件冗余和通信线路冗余；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.2.2 通信传输

8.1.2.2.1 测评单元（L3-NCS1-06）

该测评单元包括以下要求：

- a) 测评指标：应采用校验码技术或密码技术保证通信过程中数据的完整性；
- b) 测评对象：提供密码技术功能的设备或组件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否在数据传输过程中使用校验码技术或密码技术来保证其完整性；
 - 2) 应测试验证密码技术设备或组件是否保证通信过程中数据的完整性。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.2.2 测评单元（L3-NCS1-07）

该测评单元包括以下要求：

- a) 测评指标：应采用密码技术保证通信过程中敏感信息字段或整个报文的保密性；
- b) 测评对象：提供密码技术功能的设备或组件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否在通信过程中采取保密措施，具体采用哪些技术措施；
 - 2) 应测试验证在通信过程中是否对敏感信息字段或整个报文进行加密。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.3 边界防护

8.1.2.3.1 测评单元（L3-NCS1-08）

该测评单元包括以下要求：

- a) 测评指标：应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查在网络边界处是否部署访问控制设备；

- 2) 应核查设备配置信息是否指定端口进行跨越边界的网络通信,该端口配置并启用了安全策略;
- 3) 应采用其他技术手段(如非法无线网络设备定位检查、核查设备配置信息等)核查是否不存在其他未受控端口进行跨越边界的网络通信。
- d) 单元判定:如果1)~3)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.2.3.2 测评单元(L3-NCS1-09)

该测评单元包括以下要求:

- a) 测评指标:应能够对非授权设备私自联到内部网络的行为进行限制或检查;
- b) 测评对象:终端管理系统和网络设备;
- c) 测评实施包括以下内容:
 - 1) 应核查是否采用技术措施防止非授权设备接入内部网络并进行有效阻断;
 - 2) 应核查所有路由器和交换机等相关设备闲置端口是否均已关闭。
- d) 单元判定:如果1)~2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.2.3.3 测评单元(L3-NCS1-10)

该测评单元包括以下要求:

- a) 测评指标:应能够对内部用户非授权联到外部网络的行为进行限制或检查;
- b) 测评对象:终端管理系统或设备;
- c) 测评实施:应核查是否采用技术措施防止内部用户非法外联行为;
- d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

8.1.2.3.4 测评单元(L3-NCS1-11)

该测评单元包括以下要求:

- a) 测评指标:应限制无线网络的使用,确保无线网络通过受控的边界防护设备接入内部网络;
- b) 测评对象:网络拓扑图和无线网络设备;
- c) 测评实施包括以下内容:
 - 1) 应核查无线网络的部署方式,是否单独组网后再连接到有线网络;
 - 2) 应核查无线网络是否通过受控的边界防护设备接入到内部有线网络。
- d) 单元判定:如果1)~2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.2.4 访问控制

8.1.2.4.1 测评单元(L3-NCS1-12)

该测评单元包括以下要求:

- a) 测评指标:应在网络边界或区域之间根据访问控制策略设置访问控制规则,默认情况下除允许通信外受控接口拒绝所有通信;
- b) 测评对象:网闸、防火墙、路由器和交换机等提供访问控制功能的设备;
- c) 测评实施包括以下内容:

- 1) 应核查在网络边界或区域之间是否部署访问控制设备，是否启用访问控制策略；
 - 2) 应核查设备的最后一条访问控制策略是否为禁止所有网络通信。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.4.2 测评单元（L3-NCS1-13）

该测评单元包括以下要求：

- a) 测评指标：应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查设备是否不存在多余或无效的访问控制策略；
 - 2) 应核查设备的不同访问控制策略之间的逻辑关系及前后排列顺序是否合理。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.4.3 测评单元（L3-NCS1-14）

该测评单元包括以下要求：

- a) 测评指标：应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施：应核查设备访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.2.4.4 测评单元（L3-NCS1-15）

该测评单元包括以下要求：

- a) 测评指标：应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施：应核查访问控制策略中是否明确设定了源地址、目的地址、源端口、目的端口和协议，访问控制粒度是否为端口级；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.2.4.5 测评单元（L3-NCS1-16）

该测评单元包括以下要求：

- a) 测评指标：应在关键网络节点处对进出网络的信息内容进行过滤，实现对内容的访问控制；
- b) 测评对象：应用层防火墙等提供访问控制功能和内容过滤功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查在关键网络节点处是否部署相关设备，是否启用访问控制策略；

- 2) 应测试设备访问控制策略是否能够对进出网络的信息内容进行过滤,实现对内容的访问控制。
- d) 单元判定:如果 1)~2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.2.5 入侵防范

8.1.2.5.1 测评单元 (L3-NCS1-17)

该测评单元包括以下要求:

- a) 测评指标:应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为;
- b) 测评对象:抗 APT 攻击系统、网络回溯系统、抗 DDoS 攻击系统和入侵保护系统;
- c) 测评实施包括以下内容:
 - 1) 应核查相关系统或设备是否能够检测从外部发起的网络攻击行为;
 - 2) 应核查相关系统或设备的规则库版本是否已经更新到最新版本;
 - 3) 应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点。
 - 4) 应测试相关系统或设备验证其安全策略有效性。
- d) 单元判定:如果 1)~4) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.2.5.2 测评单元 (L3-NCS1-18)

该测评单元包括以下要求:

- a) 测评指标:应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为;
- b) 测评对象:抗 APT 攻击系统、网络回溯系统、抗 DDoS 攻击系统和入侵保护系统;
- c) 测评实施包括以下内容:
 - 1) 应核查相关系统或设备是否能够检测到从内部发起的网络攻击行为;
 - 2) 应核查相关系统或设备的规则库版本是否已经更新到最新版本;
 - 3) 应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点。
 - 4) 应测试相关系统或设备验证其安全策略有效性。
- d) 单元判定:如果 1)~4) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.2.5.3 测评单元 (L3-NCS1-19)

该测评单元包括以下要求:

- a) 测评指标:应采取技术措施对网络行为进行分析,实现对网络攻击特别是新型网络攻击行为的分析;
- b) 测评对象:抗 APT 攻击系统和网络回溯系统;
- c) 测评实施包括以下内容:
 - 1) 应核查是否部署网络回溯系统或抗 APT 攻击系统对新型网络攻击进行检测和分析;
 - 2) 应测试验证是否对网络行为进行分析,实现对网络攻击特别是未知的新型网络攻击的检测和分析。
- d) 单元判定:如果 1)~2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.2.5.4 测评单元 (L3-NCS1-20)

该测评单元包括以下要求：

- a) 测评指标：当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警；
- b) 测评对象：抗 APT 攻击系统、网络回溯系统、抗 DDoS 攻击系统和入侵保护系统；
- c) 测评实施包括以下内容：
 - 1) 应核查相关系统或设备的记录是否包括入侵源 IP、攻击类型、攻击目的、攻击时间等相关内容；
 - 2) 应测试验证相关系统或设备报警策略是否有效。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.6 恶意代码防范

8.1.2.6.1 测评单元（L3-NCS1-21）

该测评单元包括以下要求：

- a) 测评指标：应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；
- b) 测评对象：防病毒网关和 UTM 等提供防恶意代码功能的设备或系统；
- c) 测评实施包括以下内容：
 - 1) 应核查在关键网络节点处是否有防恶意代码技术措施；
 - 2) 应核查防恶意代码产品运行是否正常，恶意代码库是否已经更新到最新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.6.2 测评单元（L3-NCS1-22）

- a) 测评指标：应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新；
- b) 测评对象：反垃圾邮件网关提供防垃圾邮件功能的设备或系统；
- c) 测评实施包括以下内容：
 - 1) 应核查在关键网络节点处是否部署了防垃圾邮件设备或系统；
 - 2) 应核查防垃圾邮件产品运行是否正常，防垃圾邮件规则库是否已经更新到最新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.7 安全审计

8.1.2.7.1 测评单元（L3-NCS1-23）

该测评单元包括以下要求：

- a) 测评指标：应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
- b) 测评对象：综合安全审计系统、路由器、交换机和防火墙等设备；
- c) 测评实施包括以下内容：
 - 1) 应核查设备是否开启了日志记录或安全审计功能；
 - 2) 应核查是否部署了综合安全审计系统或类似功能的系统平台；

- 3) 应核查安全审计范围是否覆盖到每个用户;
- 4) 应核查是否对重要的用户行为和重要安全事件进行了审计。
- d) 单元判定: 如果 1)~4) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.2.7.2 测评单元 (L3-NCS1-24)

该测评单元包括以下要求:

- a) 测评指标: 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;
- b) 测评对象: 综合安全审计系统、路由器、交换机和防火墙等设备;
- c) 测评实施: 应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.2.7.3 测评单元 (L3-NCS1-25)

该测评单元包括以下要求:

- a) 测评指标: 应对审计记录进行保护, 定期备份, 避免受到未预期的删除、修改或覆盖等;
- b) 测评对象: 综合安全审计系统、路由器、交换机和防火墙等设备;
- c) 测评实施包括以下内容:
 - 1) 应核查是否采取了技术措施对审计记录进行保护;
 - 2) 应核查审计记录的备份机制和备份策略是否合理。
- d) 单元判定: 如果 1)~2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.2.7.4 测评单元 (L3-NCS1-26)

该测评单元包括以下要求:

- a) 测评指标: 应确保审计记录的留存时间符合法律法规要求;
- b) 测评对象: 综合安全审计系统、路由器、交换机和防火墙等设备;
- c) 测评实施: 应核查审计记录的留存时间是否至少为 6 个月;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

8.1.2.7.5 测评单元 (L3-NCS1-27)

- a) 测评指标: 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析;
- b) 测评对象: 上网行为管理系统或综合安全审计系统;
- c) 测评实施: 应核查是否对远程访问用户及互联网访问用户行为单独进行审计分析;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.2.8 集中管控

8.1.2.8.1 测评单元 (L3-NCS1-28)

该测评单元包括以下要求：

- a) 测评指标：应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
- b) 测评对象：网络拓扑图；
- c) 测评实施包括以下内容：
 - 1) 应核查是否划分出单独的网络区域用于部署安全管理系统；
 - 2) 应核查各个安全管理系统是否集中部署在单独的网络区域内。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.8.2 测评单元（L3-NCS1-29）

该测评单元包括以下要求：

- a) 测评指标：应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
- b) 测评对象：路由器、交换机和防火墙等设备；
- c) 测评实施包括以下内容：
 - 1) 应核查网络中是否划分单独的管理 VLAN 用于对安全设备或安全组件进行管理；
 - 2) 应核查网络是否使用独立的带外管理网络对安全设备或安全组件进行管理。
- d) 单元判定：如果 1) -2) 其中之一为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.2.8.3 测评单元（L3-NCS1-30）

该测评单元包括以下要求：

- a) 测评指标：应对网络链路、安全设备、网络设备和服务器等运行状况进行集中监测；
- b) 测评对象：综合网管系统等提供运行状态监测功能的系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否部署了具备运行状态监测功能的系统或设备，能够对网络链路、安全设备、网络设备等运行状况进行集中监测；
 - 2) 应测试验证运行状态监测系统是否根据网络链路、安全设备、网络设备和服务器等的工作状态、依据设定的阈值（或默认阈值）实时报警。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.8.4 测评单元（L3-NCS1-31）

该测评单元包括以下要求：

- a) 测评指标：应对分散在各个设备上的审计数据进行收集汇总和集中分析；
- b) 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统；
- c) 测评实施包括以下内容：
 - 1) 应核查各个设备是否配置并启用了相关策略，将审计数据发送到独立于设备自身的外部相关系统平台中；
 - 2) 应核查是否部署统一的集中安全审计平台，统一收集和存储各设备日志，并根据需要进行集中审计分析。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.8.5 测评单元（L3-NCS1-32）

该测评单元包括以下要求：

- a) 测评指标：应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
- b) 测评对象：提供集中安全管控功能的系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否能够对安全策略（如防火墙访问控制策略、入侵保护系统防护策略、WAF 安全防护策略等）进行集中管理；
 - 2) 应核查是否实现对操作系统防恶意代码系统及网络恶意代码防护设备的集中管理，实现防恶意代码病毒规则库的升级进行集中管理；
 - 3) 应核查是否能够实现对各设备的补丁升级进行集中管理。
- d) 单元判定：如果 1)～3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2.8.6 测评单元（L3-NCS1-33）

该测评单元包括以下要求：

- a) 测评指标：应能对网络中发生的各类安全事件进行识别、报警和分析；
- b) 测评对象：提供集中安全管控功能的系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否部署了相关系统平台能够对各类安全事件进行分析并通过声光等方式实时报警；
 - 2) 应核查安全事件的监测范围是否能够覆盖网络所有关键路径。
- d) 单元判定：如果 1)～2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3 设备和计算安全

8.1.3.1 身份鉴别

8.1.3.1.1 测评单元（L3-ECS1-01）

该测评单元包括以下要求：

- a) 测评指标：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查用户在登录时是否采用了身份鉴别措施；
 - 2) 应核查用户列表，核查用户身份标识是否具有唯一性；
 - 3) 应核查用户配置信息或访谈系统管理员，核查是否存在空口令用户；
 - 4) 应核查用户鉴别信息是否具有复杂度要求并定期更换。
- d) 单元判定：如果 1)～4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3.1.2 测评单元（L3-ECS1-02）

该测评单元包括以下要求：

- a) 测评指标：应具有登录失败处理功能，配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否配置并启用了登录失败处理功能；
 - 2) 应核查是否配置并启用了限制非法登录达到一定次数后实现账户锁定功能；
 - 3) 应核查是否配置并启用了远程登录连接超时并自动退出功能。
- d) 单元判定：如果 1)～3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3.1.3 测评单元（L3-ECS1-03）

该测评单元包括以下要求：

- a) 测评指标：当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施：应核查是否采用加密等安全方式对系统进行远程管理，防止鉴别信息在网络传输过程中被窃听；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.3.1.4 测评单元（L3-ECS1-04）

该测评单元包括以下要求：

- a) 测评指标：应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施：应核查系统是否采用两种或两种以上组合的鉴别技术对用户身份进行鉴别，其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.3.2 访问控制

8.1.3.2.1 测评单元（L3-ECS1-05）

该测评单元包括以下要求：

- a) 测评指标：应对登录的用户分配账户和权限；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络管理员、安全管理员、系统管理员或核查用户账户和权限设置情况；
 - 2) 应核查是否已禁用或限制匿名、默认账户的访问权限。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3.2.2 测评单元 (L3-ECS1-06)

该测评单元包括以下要求：

- a) 测评指标：应重命名或删除默认账户，修改默认账户的默认口令；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否已经重命名默认账户或默认账户已被删除；
 - 2) 应核查是否已修改默认账户的默认口令。
- d) 单元判定：如果 1) 或 2) 为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3.2.3 测评单元 (L3-ECS1-07)

该测评单元包括以下要求：

- a) 测评指标：应及时删除或停用多余的、过期的账户，避免共享账户的存在；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否存在多余或过期账户；
 - 2) 应访谈网络管理员、安全管理员和系统管理员不同用户是否采用不同账户登录系统。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3.2.4 测评单元 (L3-ECS1-08)

该测评单元包括以下要求：

- a) 测评指标：应进行角色划分，并授予管理用户所需的最小权限，实现管理用户的权限分离；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否进行角色划分；
 - 2) 应核查访问控制策略，查看管理用户的权限是否已进行分离；
 - 3) 应核查管理用户权限是否为其工作任务所需的最小权限。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3.2.5 测评单元 (L3-ECS1-09)

该测评单元包括以下要求：

- a) 测评指标：应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：

- 1) 应核查是否有管理用户负责配置访问控制策略;
 - 2) 应核查授权主体是否依据安全策略配置了主体对客体的访问规则;
 - 3) 应测试用户是否有可越权访问情形。
- d) 单元判定: 如果 1) -3) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.3.2.6 测评单元 (L3-ECS1-10)

该测评单元包括以下要求:

- a) 测评指标: 访问控制的粒度应达到主体为用户级或进程级, 客体为文件、数据库表级;
- b) 测评对象: 终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备;
- c) 测评实施: 应核查访问控制策略的控制粒度是否达到主体为用户级或进程级, 客体为文件、数据库表、记录或字段级;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

8.1.3.2.7 测评单元 (L3-ECS1-11)

该测评单元包括以下要求:

- a) 测评指标: 应对敏感信息资源设置安全标记, 并控制主体对有安全标记信息资源的访问;
- b) 测评对象: 终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备;
- c) 测评实施包括以下内容:
 - 1) 应核查是否依据安全策略对敏感信息资源设置了安全标记;
 - 2) 应测试是否依据主体、客体安全标记控制主体对客体访问的强制访问控制策略。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.3.3 安全审计

8.1.3.3.1 测评单元 (L3-ECS1-12)

该测评单元包括以下要求:

- a) 测评指标: 应启用安全审计功能, 审计覆盖到每个用户, 对重要的用户行为和重要安全事件进行审计;
- b) 测评对象: 终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件;
- c) 测评实施包括以下内容:
 - 1) 应核查是否开启了安全审计功能;
 - 2) 应核查安全审计范围是否覆盖到每个用户;
 - 3) 应核查是否对重要的用户行为和重要安全事件进行审计。
- d) 单元判定: 如果 1) -3) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.3.3.2 测评单元 (L3-ECS1-13)

该测评单元包括以下要求:

- a) 测评指标：审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.3.3.3 测评单元（L3-ECS1-14）

该测评单元包括以下要求：

- a) 测评指标：应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否采取了保护措施对审计记录进行保护；
 - 2) 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.3.3.4 测评单元（L3-ECS1-15）

该测评单元包括以下要求：

- a) 测评指标：应确保审计记录的留存时间符合法律法规要求；
- b) 测评对象：综合安全审计系统、终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应核查审计记录的留存时间是否至少为 6 个月；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.3.3.5 测评单元（L3-ECS1-16）

该测评单元包括以下要求：

- a) 测评指标：应对审计进程进行保护，防止未经授权的中断；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应测试通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.3.4 入侵防范

8.1.3.4.1 测评单元（L3-ECS1-17）

该测评单元包括以下要求：

- a) 测评指标：应遵循最小安装的原则，仅安装需要的组件和应用程序；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否遵循最小安装原则；

- 2) 应确认是否已经关闭非必要的组件和应用程序。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3.4.2 测评单元 (L3-ECS1-18)

该测评单元包括以下要求：

- a) 测评指标：应关闭不需要的系统服务、默认共享和高危端口；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否定期对系统服务进行梳理，关闭了非必要的系统服务和默认共享；
 - 2) 应核查是否不存在非必要的高危端口。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3.4.3 测评单元 (L3-ECS1-19)

该测评单元包括以下要求：

- a) 测评指标：应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应核查配置文件是否对终端接入范围进行限制；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.3.4.4 测评单元 (L3-ECS1-20)

该测评单元包括以下要求：

- a) 测评指标：应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应进行漏洞扫描，核查是否不存在高风险漏洞；
 - 2) 应访谈系统管理员，核查是否在经过充分测试评估后及时修补漏洞。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3.4.5 测评单元 (L3-ECS1-21)

该测评单元包括以下要求：

- a) 测评指标：应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应访谈并核查是否有入侵检测的措施；
 - 2) 应核查在发生严重入侵事件时是否提供报警。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3.5 恶意代码防范

8.1.3.5.1 测评单元 (L3-ECS1-22)

该测评单元包括以下要求：

- a) 测评指标：应采用免受恶意代码攻击的技术措施或可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证，并在检测到其完整性受到破坏时采取恢复措施；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应核查防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库，或核查是否采用可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证；
 - 2) 应核查是否有保护重要系统程序或文件完整性的措施；
 - 3) 当检测到程序或文件受到破坏后，核查是否具备恢复的措施。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3.6 资源控制

8.1.3.6.1 测评单元 (L3-ECS1-23)

该测评单元包括以下要求：

- a) 测评指标：应限制单个用户或进程对系统资源的最大使用限度；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否存在系统资源控制的措施，如核查配置参数是否设置最大进程数；
 - 2) 应引用产品（应用）测试结果或核查数据库表空间，确认目前系统资源利用率是否在允许范围之内或目前总体数据库表空间占用率是否不超过阈值；
 - 3) 应核查是否存在对数据库资源过大或最小的用户的限制措施。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3.6.2 测评单元 (L3-ECS1-24)

该测评单元包括以下要求：

- a) 测评指标：应提供重要节点设备的硬件冗余，保证系统的可用性；
- b) 测评对象：终端和服务器等设备；
- c) 测评实施：核查重要节点设备是否有硬件冗余；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.3.6.3 测评单元 (L3-ECS1-25)

该测评单元包括以下要求：

- a) 测评指标：应对重要节点进行监视，包括监视 CPU、硬盘、内存等资源的使用情况；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否有保证上述安全功能的措施（包括通过第三方工具或增强功能实现）；

- 2) 应核查是否对重要节点的系统 CPU、硬盘、内存、磁盘容量、网络服务等进行监视。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3.6.4 测评单元 (L3-ECS1-26)

该测评单元包括以下要求：

- a) 测评指标：应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否有保证上述安全功能的措施（包括通过第三方工具或增强功能实现）；
 - 2) 应核查重要节点的服务水平降低到预设的最小值时是否进行报警。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4 应用和数据安全

8.1.4.1 身份鉴别

8.1.4.1.1 测评单元 (L3-ADS1-01)

该测评单元包括以下要求：

- a) 测评指标：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查用户在登录时是否采用了身份鉴别措施；
 - 2) 应测试身份鉴别措施是否能够不被绕过；
 - 3) 应核查用户登录时是否使用唯一性身份标识；
 - 4) 应核查鉴别信息是否具有复杂度要求并定期更换；
 - 5) 应测试应用系统是否不存在空口令用户。
- d) 单元判定：如果 1) -5) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.1.2 测评单元 (L3-ADS1-02)

该测评单元包括以下要求：

- a) 测评指标：应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否提供并启用登录失败处理功能；
 - 2) 应核查登录失败反馈信息是否进行模糊处理；
 - 3) 应测试用户连续多次登录失败时应用系统是否采取必要的保护措施。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.1.3 测评单元（L3-ADS1-03）

该测评单元包括以下要求：

- a) 测评指标：应强制用户首次登录时修改初始口令；
- b) 测评对象：业务应用系统；
- c) 测评实施：应测试用户首次登录时是否被强制修改初始口令；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.4.1.4 测评单元（L3-ADS1-04）

该测评单元包括以下要求：

- a) 测评指标：用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查用户身份鉴别信息丢失时，是否采用鉴别信息重置或其他技术措施保证安全；
 - 2) 应核查用户身份鉴别信息失效时，是否采用鉴别信息重置或其他技术措施保证安全。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.1.5 测评单元（L3-ADS1-05）

该测评单元包括以下要求：

- a) 测评指标：应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现；
- b) 测评对象：业务应用系统；
- c) 测评实施：应核查系统是否采用两种或两种以上组合的鉴别技术实现用户身份进行鉴别，其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.4.2 访问控制

8.1.4.2.1 测评单元（L3-ADS1-06）

该测评单元包括以下要求：

- a) 测评指标：应提供访问控制功能，对登录的用户分配账户和权限；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否提供访问控制功能；
 - 2) 应核查是否有管理用户负责对系统用户进行账户分配和权限管理；
 - 3) 应测试不同角色用户是否具有系统规定的权限。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.2.2 测评单元（L3-ADS1-07）

该测评单元包括以下要求：

- a) 测评指标：应重命名或删除默认账户，修改默认账户的默认口令；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否已经重命名默认账户或默认账户已被删除；
 - 2) 应核查并测试是否已修改默认账户的默认口令。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.2.3 测评单元（L3-ADS1-08）

该测评单元包括以下要求：

- a) 测评指标：应及时删除或停用多余的、过期的账户，避免共享账户的存在；
- b) 测评对象：应用系统管理员和业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应访谈应用系统管理员用户与账户之间是否一一对应；
 - 2) 应核查并测试多余的、过期的账户是否被删除或停用。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.2.4 测评单元（L3-ADS1-09）

该测评单元包括以下要求：

- a) 测评指标：应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查并测试不同岗位用户是否仅拥有其工作任务所需的最小权限；
 - 2) 应核查并测试业务岗位与管理岗位用户操作权限相互之间是否相互制约；
 - 3) 应核查并测试关键业务岗位用户操作权限相互之间是否相互制约；
 - 4) 应核查并测试关键管理岗位用户操作权限相互之间是否相互制约。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.2.5 测评单元（L3-ADS1-10）

该测评单元包括以下要求：

- a) 测评指标：应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否由授权主体负责配置访问控制策略；
 - 2) 应核查授权主体是否依据安全策略配置了主体对客体的访问规则；
 - 3) 应测试是否不存在可越权访问情形。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.2.6 测评单元（L3-ADS1-11）

该测评单元包括以下要求：

- a) 测评指标：访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级；
- b) 测评对象：业务应用系统；
- c) 测评实施：应核查并测试访问控制策略的控制粒度是否达到主体为用户级，客体为文件、数据库表、记录或字段级；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.4.2.7 测评单元（L3-ADS1-12）

该测评单元包括以下要求：

- a) 测评指标：应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否依据安全策略对敏感信息资源设置了安全标记；
 - 2) 应测试依据安全标记是否实现主体对客体的强制访问控制功能。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.3 安全审计

8.1.4.3.1 测评单元（L3-ADS1-13）

该测评单元包括以下要求：

- a) 测评指标：应提供并启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否提供并启用了安全审计功能；
 - 2) 应核查审计范围是否覆盖到每个用户；
 - 3) 应核查并测试是否对重要的用户行为和重要安全事件进行审计。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.3.2 测评单元（L3-ADS1-14）

该测评单元包括以下要求：

- a) 测评指标：审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- b) 测评对象：业务应用系统；
- c) 测评实施：应核查并测试审计记录信息是否包括事件的日期、时间、类型、主体标识、客体标识和结果等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.3.3 测评单元（L3-ADS1-15）

该测评单元包括以下要求：

- a) 测评指标：应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否采取了保护措施对审计记录进行保护；
 - 2) 应核查审计记录的备份机制及备份策略是否有效。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.3.4 测评单元（L3-ADS1-16）

该测评单元包括以下要求：

- a) 测评指标：应确保审计记录的留存时间符合法律法规要求；
- b) 测评对象：综合安全审计系统和业务应用系统；
- c) 测评实施：应核查审计记录的留存时间是否至少为 6 个月；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.4.3.5 测评单元（L3-ADS1-17）

该测评单元包括以下要求：

- a) 测评指标：应对审计进程进行保护，防止未经授权的中断；
- b) 测评对象：业务应用系统；
- c) 测评实施：应测试应用系统可试图通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.4 软件容错

8.1.4.4.1 测评单元（L3-ADS1-18）

该测评单元包括以下要求：

- a) 测评指标：应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
- b) 测评对象：业务应用系统和系统设计文档等；
- c) 测评实施包括以下内容：
 - 1) 应核查系统设计文档的内容是否包括数据有效性检验功能的内容或模块；
 - 2) 应测试是否对人机接口或通信接口输入的内容进行有效性检验。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.4.2 测评单元（L3-ADS1-19）

该测评单元包括以下要求：

- a) 测评指标：在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施；
- b) 测评对象：开发文档和维护文档等；

- c) 测评实施包括以下内容：
 - 1) 应核查应用系统设计文档和维护文档,应用系统有故障发生时是否能继续提供一部分功能;
 - 2) 应核查应用系统设计文档和维护文档,应用系统有故障发生后,是否能够实施必要的措施使系统恢复功能。
- d) 单元判定:如果 1)-2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.4.4.3 测评单元 (L3-ADS1-20)

该测评单元包括以下要求:

- a) 测评指标:在故障发生时,应自动保存易失性数据和所有状态,保证系统能够进行恢复;
- b) 测评对象:系统设计文档和维护文档等;
- c) 测评实施包括以下内容：
 - 1) 应核查应用系统设计文档和维护文档,当故障发生时应用系统是否能自动保存易失性数据和当前所有状态;
 - 2) 应核查应用系统设计文档和维护文档,应用系统发生故障后能够恢复故障时的状态。
- d) 单元判定:如果 1)-2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.4.5 资源控制

8.1.4.5.1 测评单元 (L3-ADS1-21)

该测评单元包括以下要求:

- a) 测评指标:当通信双方中的一方在一段时间内未作任何响应,另一方应能够自动结束会话;
- b) 测评对象:业务应用系统;
- c) 测评实施:应测试应用系统,当应用系统的通信双方中的一方在一段时间内未作任何响应,查看另一方是否能够自动结束会话;
- d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.4.5.2 测评单元 (L3-ADS1-22)

该测评单元包括以下要求:

- a) 测评指标:应能够对系统的最大并发会话连接数进行限制;
- b) 测评对象:业务应用系统或中间件等;
- c) 测评实施包括以下内容：
 - 1) 应核查应用系统配置信息是否对最大并发会话连接数进行限制;
 - 2) 应核查中间件配置信息是否对最大并发会话连接数进行限制。
- d) 单元判定:如果 1) 或 2) 为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.4.5.3 测评单元 (L3-ADS1-23)

该测评单元包括以下要求:

- a) 测评指标:应能够对单个账户的多重并发会话进行限制;
- b) 测评对象:业务应用系统;

- c) 测评实施：应测试是否能够正确地限制单个账户的多重并发会话数；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.4.6 数据完整性

8.1.4.6.1 测评单元（L3-ADS1-24）

该测评单元包括以下要求：

- a) 测评指标：应采用校验码技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
- b) 测评对象：系统设计文档和业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查系统设计文档，鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了校验码技术或密码技术保证完整性；
 - 2) 应测试在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.6.2 测评单元（L3-ADS1-25）

该测评单元包括以下要求：

- a) 测评指标：应采用校验码技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
- b) 测评对象：系统设计文档、业务应用系统和数据安全保护系统，终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备中的重要配置数据；
- c) 测评实施包括以下内容：
 - 1) 应核查设计文档，是否采用校验码技术或密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；
 - 2) 应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；
 - 3) 应测试在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.7 数据保密性

8.1.4.7.1 测评单元（L3-ADS1-26）

该测评单元包括以下要求：

- a) 测评指标：应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
- b) 测评对象：系统设计文档和业务应用系统；

- c) 测评实施包括以下内容：
 - 1) 应核查系统设计文档，鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性；
 - 2) 应通过嗅探等方式抓取传输过程中的数据包，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.7.2 测评单元 (L3-ADS1-27)

该测评单元包括以下要求：

- a) 测评指标：应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
- b) 测评对象：系统设计文档、业务应用系统和数据安全保护系统，终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备中的重要配置数据；
- c) 测评实施包括以下内容：
 - 1) 应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性；
 - 2) 应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.8 数据备份恢复

8.1.4.8.1 测评单元 (L3-ADS1-28)

该测评单元包括以下要求：

- a) 测评指标：应提供重要数据的本地数据备份与恢复功能；
- b) 测评对象：配置数据和业务数据；
- c) 测评实施包括以下内容：
 - 1) 应核查是否按照备份策略进行本地备份；
 - 2) 应核查备份策略设置是否合理、配置是否正确；
 - 3) 应核查备份结果是否与备份策略一致；
 - 4) 应核查近期恢复测试记录，查看是否能够进行正常的数据恢复。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.8.2 测评单元 (L3-ADS1-29)

该测评单元包括以下要求：

- a) 测评指标：应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
- b) 测评对象：配置数据和业务数据；
- c) 测评实施：应核查是否提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地；

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.4.8.3 测评单元（L3-ADS1-30）

该测评单元包括以下要求：

- a) 测评指标：应提供重要数据处理系统的热冗余，保证系统的高可用性；
- b) 测评对象：重要数据处理系统；
- c) 测评实施：应核查重要数据处理系统（包括边界交换机、边界防火墙、核心路由器、应用服务器和数据库服务器等）是否采用热冗余方式部署；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.4.9 剩余信息保护

8.1.4.9.1 测评单元（L3-ADS1-31）

该测评单元包括以下要求：

- a) 测评指标：应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及业务应用系统；
- c) 测评实施：应核查相关配置信息或访谈应用系统管理员，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.9.2 测评单元（L3-ADS1-32）

该测评单元包括以下要求：

- a) 测评指标：应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及业务应用系统；
- c) 测评实施：应核查相关配置信息或访谈应用系统管理员，敏感数据所在的存储空间被释放或重新分配给其他用户前是否得到完全清除；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.10 个人信息保护

8.1.4.10.1 测评单元（L3-ADS1-33）

该测评单元包括以下要求：

- a) 测评指标：应仅采集和保存业务必需的用户个人信息；
- b) 测评对象：用户数据和业务应用系统；
- c) 测评实施：应核查采集的用户信息是否是业务应用必需的；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4.10.2 测评单元（L3-ADS1-34）

该测评单元包括以下要求：

- a) 测评指标：应禁止未授权访问和非法使用用户个人信息；
- b) 测评对象：用户数据和业务应用系统；
- c) 测评实施：应核查是否采用技术措施限制对用户信息的访问和使用；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.5 安全策略和管理制度

8.1.5.1 安全策略

8.1.5.1.1 测评单元（L3-PSS1-01）

该测评单元包括以下要求：

- a) 测评指标：应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
- b) 测评对象：总体方针策略类文档；
- c) 测评实施：应核查信息安全工作的总体方针和安全策略文件是否明确机构安全工作的总体目标、范围、原则和各类安全策略；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.5.2 管理制度

8.1.5.2.1 测评单元（L3-PSS1-02）

该测评单元包括以下要求：

- a) 测评指标：应对安全管理活动中的各类管理内容建立安全管理制度；
- b) 测评对象：安全管理制度类文档；
- c) 测评实施：应核查各项安全管理制度是否覆盖物理、网络、主机系统、数据、应用、建设和运维等层面的管理内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.5.2.2 测评单元（L3-PSS1-03）

该测评单元包括以下要求：

- a) 测评指标：应对要求管理人员或操作人员执行的日常管理操作建立操作规程；
- b) 测评对象：操作规程类文档；
- c) 测评实施：应核查是否具有日常管理操作的操作规程，如系统维护手册和用户操作规程等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.5.2.3 测评单元（L3-PSS1-04）

该测评单元包括以下要求：

- a) 测评指标：应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的信息安全管理制度体系；
- b) 测评对象：总体方针策略类文档、管理制度类文档、操作规程类文档和记录表单类文档；
- c) 测评实施：应核查总体方针策略文件、管理制度和操作规程是否形成体系化；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.5.3 制定和发布

8.1.5.3.1 测评单元（L3-PSS1-05）

该测评单元包括以下要求：

- a) 测评指标：应指定或授权专门的部门或人员负责安全管理制度的制定；
- b) 测评对象：信息安全主管；
- c) 测评实施：应访谈信息安全主管是否由专门的部门或人员负责制定安全管理制度；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.5.3.2 测评单元（L3-PSS1-06）

该测评单元包括以下要求：

- a) 测评指标：安全管理制度应通过正式、有效的方式发布，并进行版本控制；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查制度制定和发布要求管理文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容；
 - 2) 应核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导签署和单位盖章等，是否注明发布范围。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.5.4 评审和修订

8.1.5.4.1 测评单元（L3-PSS1-07）

该测评单元包括以下要求：

- a) 测评指标：应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订；
- b) 测评对象：信息安全主管和管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否定期对安全管理制度体系的合理性和适用性进行审定；
 - 2) 应核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制度。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6 安全管理机构和人员

8.1.6.1 岗位设置

8.1.6.1.1 测评单元（L3-ORS1-01）

该测评单元包括以下要求：

- a) 测评指标：应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
- b) 测评对象：信息安全主管和管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否进行了信息安全管理职能部门的划分；
 - 2) 应核查部门职责文档是否明确信息安全管理工作的职能部门和各负责人职责；
 - 3) 应核查岗位职责文档是否明确岗位划分情况和岗位职责。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.1.2 测评单元（L3-ORS1-02）

该测评单元包括以下要求：

- a) 测评指标：应设立系统管理员、网络管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责；
- b) 测评对象：信息安全主管和管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否进行了信息安全管理岗位的划分；
 - 2) 应核查岗位职责文档是否明确了各岗位职责。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.1.3 测评单元（L3-ORS1-03）

该测评单元包括以下要求：

- a) 测评指标：应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；
- b) 测评对象：信息安全主管、管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否成立了指导和管理信息安全工作的委员会或领导小组；
 - 2) 应核查部门职责文档是否明确了信息安全工作委员会或领导小组构成情况和相关职责；
 - 3) 应核查是否具有信息安全工作的委员会或领导小组开展工作的会议纪要或相关记录。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.2 人员配备

8.1.6.2.1 测评单元（L3-ORS1-04）

该测评单元包括以下要求：

- a) 测评指标：应配备一定数量的系统管理员、网络管理员、安全管理员等；
- b) 测评对象：信息安全主管和记录表单类文档；

- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否配备系统管理员、网络管理员和系统管理员；
 - 2) 应核查人员配备文档是否明确各岗位人员配备情况。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.2.2 测评单元（L3-ORS1-05）

该测评单元包括以下要求：

- a) 测评指标：应配备专职安全管理员，不可兼任；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查人员配备文档是否配备了专职安全管理员；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.6.3 授权和审批

8.1.6.3.1 测评单元（L4-ORS1-06）

该测评单元包括以下要求：

- a) 测评指标：应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查部门职责文档是否明确各部门的职责和授权范围；
 - 2) 应核查岗位职责文档是否明确各岗位的职责和授权范围；
 - 3) 应核查审批记录，审批事项、审批部门和批准人等内容是否与相关制度一致。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.3.2 测评单元（L4-ORS1-07）

该测评单元包括以下要求：

- a) 测评指标：应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
- b) 测评对象：操作规程类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查系统变更、重要操作、物理访问和系统接入等事项的操作规范是否明确相关操作过程中建立了逐级审批程序；
 - 2) 应核查审批记录、操作记录，审批结果是否与相关制度一致。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.3.3 测评单元（L4-ORS1-08）

该测评单元包括以下要求：

- a) 测评指标：应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
- b) 测评对象：信息安全主管；

- c) 测评实施：应访谈信息安全主管是否对各类审批事项进行更新；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.6.4 沟通和合作

8.1.6.4.1 测评单元（L3-ORS1-09）

该测评单元包括以下要求：

- a) 测评指标：应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理信息安全问题；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否建立了各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通机制；
 - 2) 应核查会议记录是否明确各类管理人员之间、组织内部机构之间以及信息安全职能部门内部开展了合作与沟通。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.4.2 测评单元（L3-ORS1-10）

该测评单元包括以下要求：

- a) 测评指标：应加强与公安机关、各类供应商、业界专家及安全组织的合作与沟通；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否建立了与公安机关、各类供应商、业界专家及安全组织的合作与沟通机制；
 - 2) 应核查会议记录是否明确与公安机关、各类供应商、业界专家及安全组织开展了合作与沟通。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.4.3 测评单元（L3-ORS1-11）

该测评单元包括以下要求：

- a) 测评指标：应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查外联单位联系列表，查看是否记录了外联单位名称、合作内容、联系人和联系方式等信息；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.6.5 审核和检查

8.1.6.5.1 测评单元（L3-ORS1-12）

该测评单元包括以下要求：

- a) 测评指标：应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否定期进行常规安全核查；
 - 2) 应核查常规安全检查记录是否包括了系统日常运行、系统漏洞和数据备份等情况。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.5.2 测评单元（L3-ORS1-13）

该测评单元包括以下要求：

- a) 测评指标：应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否定期进行全面安全核查；
 - 2) 应核查全面安全检查记录是否包括了现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.5.3 测评单元（L3-ORS1-14）

该测评单元包括以下要求：

- a) 测评指标：应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有安全检查表格、安全检查记录、安全检查报告、安全检查结果通报记录；
- d) 单元判定：如果以上测评实施内容肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.6.6 人员录用

8.1.6.6.1 测评单元（L3-ORS1-15）

该测评单元包括以下要求：

- a) 测评指标：应指定或授权专门的部门或人员负责人员录用；
- b) 测评对象：信息安全主管；
- c) 测评实施：应访谈信息安全主管是否由专门的部门或人员负责人员的录用工作；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.6.6.2 测评单元（L3-ORS1-16）

该测评单元包括以下要求：

- a) 测评指标：应对被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查人员安全管理文档是否说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）；
 - 2) 应核查是否具有人员录用时对录用人员身份、背景、专业资格和资质等进行审查的相关文档或记录，是否记录审查内容和审查结果等；
 - 3) 应核查人员录用时的技能考核文档或记录是否记录考核内容和考核结果等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.6.3 测评单元（L3-ORS1-17）

该测评单元包括以下要求：

- a) 测评指标：应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查保密协议是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容；
 - 2) 应核查岗位安全协议是否有岗位安全责任定义、协议的有效期限和责任人签字等内容。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.7 人员离岗

8.1.6.7.1 测评单元（L3-ORS1-18）

该测评单元包括以下要求：

- a) 测评指标：应及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有离岗人员交还身份证件、设备等的登记记录。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.6.7.2 测评单元（L3-ORS1-19）

该测评单元包括以下要求：

- a) 测评指标：应办理严格的调离手续，并承诺调离后的保密义务后方可离开；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查人员离岗的管理文档是否规定了人员调离手续和离岗要求等；
 - 2) 应核查是否具有按照离岗程序办理调离手续的记录；
 - 3) 应核查保密承诺文档是否有调离人员的签字。

- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.8 安全意识教育和培训

8.1.6.8.1 测评单元 (L3-ORS1-20)

该测评单元包括以下要求：

- a) 测评指标：应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
- b) 测评对象：管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查信息安全教育及技能培训文档是否明确培训周期、培训方式、培训内容和考核方式等相关内容；
 - 2) 应核查安全责任和惩戒措施管理文档是否包含具体的安全责任和惩戒措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.8.2 测评单元 (L3-ORS1-21)

该测评单元包括以下要求：

- a) 测评指标：应针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查安全教育和培训计划文档是否具有不同岗位的培训计划；查看培训内容是否包含信息安全基础知识、岗位操作规程等；
 - 2) 应核查安全教育和培训记录是否有培训人员、培训内容、培训结果等的描述。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.8.3 测评单元 (L3-ORS1-22)

该测评单元包括以下要求：

- a) 测评指标：应定期对不同岗位的人员进行技能考核；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有针对各岗位人员的技能考核记录。
- d) 单元判定：如果以上测评实施为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.9 外部人员访问管理

8.1.6.9.1 测评单元 (L3-ORS1-23)

该测评单元包括以下要求：

- a) 测评指标：应确保在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
- b) 测评对象：管理制度类文档和记录表单类文档；

- c) 测评实施包括以下内容：
 - 1) 应核查外部人员访问管理文档是否明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等；
 - 2) 应核查外部人员访问重要区域的书面申请文档是否具有批准人允许访问的批准签字等；
 - 3) 应核查外部人员访问重要区域的登记记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.9.2 测评单元 (L3-ORS1-24)

该测评单元包括以下要求：

- a) 测评指标：应确保在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查外部人员访问管理文档是否明确外部人员接入受控网络前的申请审批流程；
 - 2) 应核查外部人员访问系统的书面申请文档是否明确外部人员的访问权限，是否具有允许访问的批准签字等；
 - 3) 应核查外部人员访问系统的登记记录是否记录了外部人员访问的权限、时限、账户等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.9.3 测评单元 (L3-ORS1-25)

该测评单元包括以下要求：

- a) 测评指标：外部人员离场后应及时清除其所有的访问权限；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查外部人员访问管理文档是否明确外部人员离开后及时清除其所有访问权限；
 - 2) 应核查外部人员访问系统的登记记录是否记录了访问权限清除时间。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.6.9.4 测评单元 (L3-ORS1-26)

该测评单元包括以下要求：

- a) 测评指标：获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查外部人员访问保密协议是否明确人员的保密义务(如不得进行非授权操作，不得复制信息等)；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7 安全建设管理

8.1.7.1 定级和备案

8.1.7.1.1 测评单元（L3-CMS1-01）

该测评单元包括以下要求：

- a) 测评指标：应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查定级文档是否明确等级保护对象的安全保护等级，是否说明定级的方法和理由。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.1.2 测评单元（L3-CMS1-02）

该测评单元包括以下要求：

- a) 测评指标：应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查定级结果的论证评审会议记录是否有相关部门和有关安全技术专家对定级结果的论证意见；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.1.3 测评单元（L3-CMS1-03）

该测评单元包括以下要求：

- a) 测评指标：应确保定级结果经过相关部门的批准；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查定级结果部门审批文档是否有上级主管部门或本单位相关部门的审批意见；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.1.4 测评单元（L3-CMS1-04）

该测评单元包括以下要求：

- a) 测评指标：应将备案材料报主管部门和相应公安机关备案；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有公安机关出具的备案证明文档；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.2 安全方案设计

8.1.7.2.1 测评单元（L3-CMS1-05）

该测评单元包括以下要求：

- a) 测评指标：应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
- b) 测评对象：安全规划设计类文档；

- c) 测评实施：应核查安全设计文档是否根据安全等级选择安全措施，是否根据安全需求调整安全措施；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.2.2 测评单元（L3-CMS1-06）

该测评单元包括以下要求：

- a) 测评指标：应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码相关内容，并形成配套文件；
- b) 测评对象：安全规划设计类文档；
- c) 测评实施：应核查是否有总体规划和安全设计方案等配套文件，设计方案中应保护密码相关内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.2.3 测评单元（L3-CMS1-07）

该测评单元包括以下要求：

- a) 测评指标：应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查配套文件的论证评审记录或文档是否有相关部门和有关安全技术专家对总体安全规划、安全设计方案等相关配套文件的论证意见；
 - 2) 应核查是否有总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件，各个文件是否有机构管理层的批准。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.7.3 产品采购和使用

8.1.7.3.1 测评单元（L3-CMS1-08）

该测评单元包括以下要求：

- a) 测评指标：应确保信息安全产品采购和使用符合国家的有关规定；
- b) 测评对象：建设负责人；
- c) 测评实施：应访谈建设负责人系统使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.3.2 测评单元（L3-CMS1-09）

该测评单元包括以下要求：

- a) 测评指标：应确保密码产品与服务的采购和使用符合国家密码主管部门的要求；
- b) 测评对象：建设负责人；

- c) 测评实施：应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.3.3 测评单元（L3-CMS1-10）

该测评单元包括以下要求：

- a) 测评指标：应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有产品选型测试结果文档、候选产品采购清单及审定或更新的记录；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.4 自行软件开发

8.1.7.4.1 测评单元（L3-CMS1-11）

该测评单元包括以下要求：

- a) 测评指标：应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
- b) 测评对象：建设负责人；
- c) 测评实施包括以下内容：
 - 1) 应访谈建设负责人自主开发软件是否在独立的物理环境中完成编码和调试，与实际运行环境分开；
 - 2) 应核查测试数据和结果是否受控使用。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.7.4.2 测评单元（L3-CMS1-12）

该测评单元包括以下要求：

- a) 测评指标：应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查软件开发管理制度是否明确软件设计、开发、测试和验收过程的控制方法和人员行为准则，是否明确哪些开发活动应经过授权和审批；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.4.3 测评单元（L3-CMS1-13）

该测评单元包括以下要求：

- a) 测评指标：应制定代码编写安全规范，要求开发人员参照规范编写代码；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查代码编写安全规范是否明确代码安全编写规则；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.4.4 测评单元（L3-CMS1-14）

该测评单元包括以下要求：

- a) 测评指标：应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制；
- b) 测评对象：软件开发类文档；
- c) 测评实施：应核查是否具有软件开发文档和使用指南；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.4.5 测评单元（L3-CMS1-15）

该测评单元包括以下要求：

- a) 测评指标：应确保在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有软件安全测试报告，明确软件存在的安全问题及可能存在的恶意代码；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.4.6 测评单元（L3-CMS1-16）

该测评单元包括以下要求：

- a) 测评指标：应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查对程序资源库的修改、更新、发布进行授权和审批的文档或记录是否有批准人的签字；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.4.7 测评单元（L3-CMS1-17）

该测评单元包括以下要求：

- a) 测评指标：应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查；
- b) 测评对象：建设负责人；
- c) 测评实施：应访谈建设负责人开发人员是否为专职，是否对开发人员活动进行控制等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.5 外包软件开发

8.1.7.5.1 测评单元（L3-CMS1-18）

该测评单元包括以下要求：

- a) 测评指标：应在软件交付前检测软件其中可能存在的恶意代码；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有交付前的恶意代码检测报告；

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.5.2 测评单元（L3-CMS1-19）

该测评单元包括以下要求：

- a) 测评指标：应要求开发单位提供软件设计文档和使用指南；
- b) 测评对象：操作规程类文档和记录表单类文档；
- c) 测评实施：应核查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.5.3 测评单元（L3-CMS1-20）

该测评单元包括以下要求：

- a) 测评指标：应要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道；
- b) 测评对象：建设负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈建设负责人委托开发单位是否提供软件源代码；
 - 2) 应核查软件测试报告是否明确审查了软件可能存在的后门和隐蔽信道并记录。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.7.6 工程实施

8.1.7.6.1 测评单元（L3-CMS1-21）

该测评单元包括以下要求：

- a) 测评指标：应指定或授权专门的部门或人员负责工程实施过程的管理；
- b) 测评对象：建设负责人；
- c) 测评实施：应访谈建设负责人是否指定专门部门或人员对工程实施过程进行进度和质量控制，由何部门/何人负责；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.6.2 测评单元（L3-CMS1-22）

该测评单元包括以下要求：

- a) 测评指标：应制定工程实施方案控制安全工程实施过程；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查工程实施方案是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.6.3 测评单元（L3-CMS1-23）

该测评单元包括以下要求：

- a) 测评指标：应通过第三方工程监理控制项目的实施过程；
- b) 测评对象：记录表单类文档；
- c) 测评实施：如果安全建设为第三方实施时，应核查工程监理报告是否明确了工程进展、时间计划、控制措施等方面内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.7 测试验收

8.1.7.7.1 测评单元（L3-CMS1-24）

该测评单元包括以下要求：

- a) 测评指标：应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查工程测试验收方案是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容；
 - 2) 应核查测试验收报告是否有相关部门和人员对测试验收报告进行审定的意见。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.7.7.2 测评单元（L3-CMS1-25）

该测评单元包括以下要求：

- a) 测评指标：应进行上线前的安全性测试，验证安全措施的有效性，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有上线前的安全测试报告，报告应包含密码应用安全性测试相关内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.8 系统交付

8.1.7.8.1 测评单元（L3-CMS1-26）

该测评单元包括以下要求：

- a) 测评指标：应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查交付清单是否说明交付的各类设备、软件、文档等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.8.2 测评单元（L3-CMS1-27）

该测评单元包括以下要求：

- a) 测评指标：应对负责运行维护的技术人员进行相应的技能培训；
- b) 测评对象：记录表单类文档；

- c) 测评实施：应核查系统交付技术培训记录是否包括培训内容、培训时间和参与人员等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.8.3 测评单元（L3-CMS1-28）

该测评单元包括以下要求：

- a) 测评指标：应确保提供建设过程中的文档和指导用户进行运行维护的文档；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查交付文档是否有指导用户进行运维的文档等，提交的文档是否符合管理规定的要求；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.9 等级测评

8.1.7.9.1 测评单元（L3-CMS1-29）

该测评单元包括以下要求：

- a) 测评指标：应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人本次测评是否为首次，若非首次，以往进行过几次测评，是否根据测评结果进行相应的安全整改；
 - 2) 应核查是否具有以往等级测评报告和安全整改方案。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.7.9.2 测评单元（L3-CMS1-30）

该测评单元包括以下要求：

- a) 测评指标：应在发生重大变更或级别发生变化时进行等级测评；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人系统是否有过重大变更或级别发生过变化，若有，是否进行相应的等级测评；
 - 2) 应核查是否具有相应情况下的等级测评报告。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.7.9.3 测评单元（L3-CMS1-31）

该测评单元包括以下要求：

- a) 测评指标：应确保测评机构的选择符合国家有关规定；
- b) 测评对象：运维负责人；
- c) 测评实施：应访谈运维负责人以往等级测评的测评单位是否具有国家相关等级测评资质的单位；

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.10 服务供应商管理

8.1.7.10.1 测评单元（L3-CMS1-32）

该测评单元包括以下要求：

- a) 测评指标：应确保服务供应商的选择符合国家的有关规定；
- b) 测评对象：运维负责人；
- c) 测评实施：应访谈建设负责人选择的安全服务商是否符合国家有关规定；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.10.2 测评单元（L3-CMS1-33）

该测评单元包括以下要求：

- a) 测评指标：应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的信息安全相关义务；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查与安全服务商签订的服务合同或安全责任合同书是否明确了后期的技术支持和服务承诺等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.7.10.3 测评单元（L3-CMS1-34）

该测评单元包括以下要求：

- a) 测评指标：应定期监视、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查是否具有安全服务商定期提交的安全服务报告；
 - 2) 应核查是否定期审核评价安全服务供应商所提供的服务，是否具有服务审核报告；
 - 3) 应核查是否具有安全服务商评价审核管理制度，明确针对服务商的评价指标和考核内容等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8 安全运维管理

8.1.8.1 环境管理

8.1.8.1.1 测评单元（L3-MMS1-01）

该测评单元包括以下要求：

- a) 测评指标：应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
- b) 测评对象：物理安全负责人和记录表单类文档；
- c) 测评实施包括以下内容：

- 1) 应访谈物理安全负责人是否指定部门和人员负责机房安全管理工作,对机房的出入进行管理、对基础设施(如空调、供配电设备、灭火设备等)进行定期维护,由何部门/何人负责;
 - 2) 应核查部门或人员岗位职责文档是否明确机房安全的责任部门及人员;
 - 3) 应核查机房的出入登记记录是否记录来访人员、来访时间、离开时间、携带物品等信息;
 - 4) 应核查机房的基础设施的维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
- d) 单元判定:如果1)~4)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.8.1.2 测评单元(L3-MMS1-02)

该测评单元包括以下要求:

- a) 测评指标:应对机房的安全管理做出规定,包括机房物理访问、物品带进带出和机房环境安全等;
- b) 测评对象:管理制度类文档和记录表单类文档;
- c) 测评实施包括以下内容:
 - 1) 应核查机房安全管理制度是否覆盖机房物理访问、物品带进、带出机房和机房环境安全等方面内容;
 - 2) 应核查机房环境和物理访问、物品带进、带出机房等的登记记录是否与制度相符。
- d) 单元判定:如果1)~2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.8.1.3 测评单元(L3-MMS1-03)

该测评单元包括以下要求:

- a) 测评指标:应不在重要区域接待来访人员和桌面上没有包含敏感信息的纸档文件、移动介质等;
- b) 测评对象:管理制度类文档和办公环境;
- c) 测评实施包括以下内容:
 - 1) 应核查机房安全管理制度是否明确来访人员的接待区域;
 - 2) 应核查办公桌面上是否不包含敏感信息的纸档文件和移动介质等。
- d) 单元判定:如果1)~2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.8.2 资产管理

8.1.8.2.1 测评单元(L3-MMS1-04)

该测评单元包括以下要求:

- a) 测评指标:应编制并保存与保护对象相关的资产清单,包括资产责任部门、重要程度和所处位置等内容;
- b) 测评对象:记录表单类文档;
- c) 测评实施:应核查资产清单是否覆盖资产范围(含设备设施、软件、文档等)、资产责任部门、重要程度和所处位置等内容。
- d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

8.1.8.2.2 测评单元（L3-MMS1-05）

该测评单元包括以下要求：

- a) 测评指标：应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
- b) 测评对象：资产管理、管理制度类文档和设备；
- c) 测评实施包括以下内容：
 - 1) 应访谈资产管理是否依据资产的重要程度对资产进行标识，不同类别的资产在管理措施的选取上是否不同；
 - 2) 应核查资产管理制度是否明确资产的标识方法以及不同资产的管理措施要求；
 - 3) 应核查资产清单中的设备是否具有相应标识，标识方法是否符合 2) 相关要求。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.2.3 测评单元（L3-MMS1-06）

该测评单元包括以下要求：

- a) 测评指标：应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理；
- b) 测评对象：管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查信息分类文档是否规定了分类标识的原则和方法（如根据信息的重要程度、敏感程度或用途不同进行分类）；
 - 2) 核查信息资产管理办法是否规定了不同类信息的使用、传输和存储等。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.3 介质管理

8.1.8.3.1 测评单元（L3-MMS1-07）

该测评单元包括以下要求：

- a) 测评指标：应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储介质专人管理，并根据存档介质的目录清单定期盘点；
- b) 测评对象：资产管理、记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈资产管理介质存放于何种环境中，是否对存放介质实施专人管理；
 - 2) 应核查介质使用管理记录是否记录介质归档和使用等情况。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.3.2 测评单元（L3-MMS1-08）

该测评单元包括以下要求：

- a) 测评指标：应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录；
- b) 测评对象：资产管理、记录表单类文档；
- c) 测评实施包括以下内容：

- 1) 应访谈资产管理介质在物理传输过程中的人员、打包交付等情况是否进行控制;
- 2) 应核查是否有对介质的归档和查询等的登记记录。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.8.4 设备维护管理

8.1.8.4.1 测评单元 (L3-MMS1-09)

该测评单元包括以下要求:

- a) 测评指标: 应对各种设备 (包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理;
- b) 测评对象: 设备管理员和管理制度类文档;
- c) 测评实施包括以下内容:
 - 1) 应访谈设备管理员是否对各类设施、设备指定专人或专门部门进行定期维护;
 - 2) 应核查部门或人员岗位职责文档是否明确设备维护管理的责任部门。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.8.4.2 测评单元 (L3-MMS1-10)

该测评单元包括以下要求:

- a) 测评指标: 应对配套设施、软硬件维护管理做出规定, 包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等;
- b) 测评对象: 管理制度类文档和记录表单类文档;
- c) 测评实施包括以下内容:
 - 1) 应核查设备维护管理制度是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容;
 - 2) 应核查是否留有维修和服务的审批、维修过程等记录, 审批、记录内容是否与制度相符。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.8.4.3 测评单元 (L3-MMS1-11)

该测评单元包括以下要求:

- a) 测评指标: 应确保信息处理设备必须经过审批才能带离机房或办公地点, 含有存储介质的设备带出工作环境时其中重要数据必须加密;
- b) 测评对象: 设备管理员和记录表单类文档;
- c) 测评实施包括以下内容:
 - 1) 应访谈设备管理员对带离机房的设备是否经过审批, 由何人审批;
 - 2) 应核查是否具有设备带离机房或办公地点的审批记录;
 - 3) 应访谈设备管理员含有重要数据的存储介质带出工作环境是否有加密措施, 采取什么加密措施。
- d) 单元判定: 如果 1) -3) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.1.8.4.4 测评单元 (L3-MMS1-12)

该测评单元包括以下要求：

- a) 测评指标：含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用；
- b) 测评对象：设备管理员；
- c) 测评实施：应访谈设备管理员含有存储介质的设备在报废或重用前，是否采取措施进行完全清除或被安全覆盖；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.5 漏洞和风险管理

8.1.8.5.1 测评单元（L3-MMS1-13）

该测评单元包括以下要求：

- a) 测评指标：应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；
- b) 测评对象：安全管理员和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否定期进行漏洞扫描，对发现的漏洞是否及时进行修补或评估可能的影响后进行修补；
 - 2) 应核查漏洞扫描报告是否描述了存在的漏洞、严重级别、原因分析和改进意见等方面。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.5.2 测评单元（L3-MMS1-14）

该测评单元包括以下要求：

- a) 测评指标：应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题；
- b) 测评对象：安全管理员和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否定期开展安全测评；
 - 2) 应核查是否具有安全测评报告；
 - 3) 应核查是否具有安全整改应对措施文档。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.6 网络和系统安全管理

8.1.8.6.1 测评单元（L3-MMS1-15）

该测评单元包括以下要求：

- a) 测评指标：应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查网络和系统安全管理文档是否明确要求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）；

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.6.2 测评单元（L3-MMS1-16）

该测评单元包括以下要求：

- a) 测评指标：应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人是否指定专门的部门或人员进行账户管理；
 - 2) 应核查相关审批记录或流程是否对申请账户、建立账户、删除账户等进行控制。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.6.3 测评单元（L3-MMS1-17）

该测评单元包括以下要求：

- a) 测评指标：应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略，账户管理（用户责任、义务、风险、权限审批、权限分配、账户注销等），配置文件的生成、备份，变更审批、符合性检查等，授权访问，最小服务，升级与打补丁，审计日志，登录设备和系统的口令更新周期等方面；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.6.4 测评单元（L3-MMS1-18）

该测评单元包括以下要求：

- a) 测评指标：应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
- b) 测评对象：操作规程类文档；
- c) 测评实施：应核查重要设备（如操作系统、数据库、网络设备、安全设备、应用和组件）的配置和操作手册是否明确操作步骤、维护记录、参数配置等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.6.5 测评单元（L3-MMS1-19）

该测评单元包括以下要求：

- a) 测评指标：应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查运维操作日志，查看是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修改等内容。

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.6.6 测评单元（L3-MMS1-20）

该测评单元包括以下要求：

- a) 测评指标：应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络和系统相关人员是否指定专门部门或人员对日志、监测和报警数据等进行分析统计；
 - 2) 应核查是否具有对日志、监测和报警数据等进行分析统计的报告。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.6.7 测评单元（L3-MMS1-21）

该测评单元包括以下要求：

- a) 测评指标：应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络和系统相关人员调整配置参数结束后是否同步更新配置信息库，并核实配置信息库是否为最新版本；
 - 2) 应核查是否具有变更运维的审批记录，如系统连接、安装系统组件或调整配置参数等活动；
 - 3) 应核查是否具有变更运维的操作过程记录。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.6.8 测评单元（L3-MMS1-22）

该测评单元包括以下要求：

- a) 测评指标：应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；
- b) 测评对象：系统管理员和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员使用运维工具结束后是否删除工具中的敏感数据；
 - 2) 应核查是否具有运维工具接入系统的审批记录；
 - 3) 应核查运维工具的审计日志记录，审计日志是否不可以更改。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.6.9 测评单元（L3-MMS1-23）

该测评单元包括以下要求：

- a) 测评指标：应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；
- b) 测评对象：系统管理员和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员日常运维过程中是否存在远程运维，如存在则远程运维结束后是否立即关闭了接口或通道；
 - 2) 应核查是否具有开通远程运维的审批记录；
 - 3) 应核查针对远程运维的操作过程记录，查看审计日志是否不可以更改。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.6.10 测评单元（L3-MMS1-24）

该测评单元包括以下要求：

- a) 测评指标：应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为；
- b) 测评对象：网络管理员和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络管理员外联种类（互联网、合作伙伴企业网、上级部门网络等）是否都得到授权与批准，由何人、何部门批准；
 - 2) 应访谈网络管理员是否定期核查违规联网行为；
 - 3) 应核查是否具有外联授权的记录文件。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.7 恶意代码防范管理

8.1.8.7.1 测评单元（L3-MMS1-25）

该测评单元包括以下要求：

- a) 测评指标：应提高所有用户的防恶意代码意识，告知对外来计算机或存储设备接入系统前进行恶意代码检查等；
- b) 测评对象：运维负责人；
- c) 测评实施：应访谈运维负责人是否采取告知方式提升员工的防病毒意识；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.7.2 测评单元（L3-MMS1-26）

该测评单元包括以下要求：

- a) 测评指标：应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查恶意代码防范管理制度是否明确防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容。

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.7.3 测评单元（L3-MMS1-27）

该测评单元包括以下要求：

- a) 测评指标：应定期验证防范恶意代码攻击的技术措施的有效性；
- b) 测评对象：安全管理员和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否定期对恶意代码库进行升级，且对升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报，是否出现过大规模的病毒事件，如何处理；
 - 2) 应核查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告；
 - 3) 应核查是否定期采用技术手段测试验证恶意代码防范技术措施的有效性。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.8 配置管理

8.1.8.8.1 测评单元（L3-MMS1-28）

该测评单元包括以下要求：

- a) 测评指标：应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；
- b) 测评对象：系统管理员；
- c) 测评实施：应访谈系统管理员是否对基本配置信息进行记录和保存；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.8.2 测评单元（L3-MMS1-29）

该测评单元包括以下要求：

- a) 测评指标：应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库；
- b) 测评对象：系统管理员和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈配置管理人员基本配置信息改变后是否及时更新基本配置信息库；
 - 2) 应核查配置信息的变更流程是否具有相应的申报审批程序。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.9 密码管理

8.1.8.9.1 测评单元（L3-MMS1-30）

该测评单元包括以下要求：

- a) 测评指标：应使用符合国家密码管理规定的密码技术和产品；
- b) 测评对象：安全管理员；

- c) 测评实施:应核查相关产品是否获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书;
- d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

8.1.8.10 变更管理

8.1.8.10.1 测评单元 (L3-MMS1-31)

该测评单元包括以下要求:

- a) 测评指标:应明确变更需求,变更前根据变更需求制定变更方案,变更方案经过评审、审批后方可实施;
- b) 测评对象:记录表单类文档。
- c) 测评实施包括以下内容:
 - 1) 应核查变更方案,查看其是否包含变更类型、变更原因、变更过程、变更前评估等内容;
 - 2) 应核查是否具有变更方案评审记录和变更过程记录文档。
- d) 单元判定:如果 1) -2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.8.10.2 测评单元 (L3-MMS1-32)

该测评单元包括以下要求:

- a) 测评指标:应建立变更的申报和审批控制程序,依据程序控制所有的变更,记录变更实施过程;
- b) 测评对象:记录表单类文档;
- c) 测评实施包括以下内容:
 - 1) 应核查变更控制的申报、审批程序其是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容;
 - 2) 应核查是否具有变更实施过程的记录文档;
 - 3) 应核查是否针对发生变更的事件进行了影响分析。
- d) 单元判定:如果 1) -3) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.8.10.3 测评单元 (L3-MMS1-33)

该测评单元包括以下要求:

- a) 测评指标:应建立中止变更并从失败变更中恢复的程序,明确过程控制方法和人员职责,必要时对恢复过程进行演练;
- b) 测评对象:运维负责人和记录表单类文档;
- c) 测评实施包括以下内容:
 - 1) 应访谈运维负责人变更失败后的恢复程序、工作方法和职责是否文档化,恢复过程是否经过演练;
 - 2) 应核查是否具有变更恢复演练记录;
 - 3) 应核查变更失败恢复程序是否规定变更失败后的恢复流程。
- d) 单元判定:如果 1) -3) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

8.1.8.11 备份与恢复管理

8.1.8.11.1 测评单元（L3-MMS1-34）

该测评单元包括以下要求：

- a) 测评指标：应识别需要定期备份的重要业务信息、系统数据及软件系统等；
- b) 测评对象：系统管理员、数据库管理员和网络管理员和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员、数据库管理员和网络管理员是否识别需定期备份的业务信息、系统数据及软件系统；
 - 2) 应核查是否具有定期备份的重要业务信息、系统数据、软件系统的列表或清单。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.11.2 测评单元（L3-MMS1-35）

该测评单元包括以下要求：

- a) 测评指标：应规定备份信息的备份方式、备份频度、存储介质、保存期等；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查备份与恢复管理制度是否明确备份方式、频度、介质、保存期等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.11.3 测评单元（L3-MMS1-36）

该测评单元包括以下要求：

- a) 测评指标：应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查备份和恢复的策略是否明确备份策略和恢复策略文档规范了数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.12 安全事件处置

8.1.8.12.1 测评单元（L3-MMS1-37）

该测评单元包括以下要求：

- a) 测评指标：应及时向安全管理部门报告所发现的安全弱点和可疑事件；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人是否告知用户在发现安全弱点和可疑事件时应及时向安全管理部门报告；
 - 2) 应核查是否有运维过程中发现的安全弱点和可疑事件对应的报告或相关文档，内容是否详实。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.12.2 测评单元（L3-MMS1-38）

该测评单元包括以下要求：

- a) 测评指标：应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查安全事件报告和处置管理制度是否明确了与安全事件有关的工作职责，包括报告单位（人）、接报单位（人）和处置单位等职责；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.12.3 测评单元（L3-MMS1-39）

该测评单元包括以下要求：

- a) 测评指标：应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查安全事件报告和响应处置记录是否记录引发安全事件的系统弱点、不同安全事件发生的原因、处置过程、经验教训总结、补救措施等内容。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.12.4 测评单元（L3-MMS1-40）

该测评单元包括以下要求：

- a) 测评指标：对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人是否针对不同安全事件形成不同的报告流程；
 - 2) 应核查安全事件报告和处理程序文档是否根据不同安全事件制定不同的处理和报告程序，是否明确具体报告方式、报告内容、报告人等方面内容。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.13 应急预案管理

8.1.8.13.1 测评单元（L3-MMS1-41）

该测评单元包括以下要求：

- a) 测评指标：应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查应急预案框架是否覆盖启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等方面；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.13.2 测评单元（L3-MMS1-42）

该测评单元包括以下要求：

- a) 测评指标：应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；
- b) 测评对象：管理制度类文档。
- c) 测评实施：应核查是否具有重要事件的应急预案（如针对机房、系统、网络等各个层面）；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.13.3 测评单元（L3-MMS1-43）

该测评单元包括以下要求：

- a) 测评指标：应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人是否定期对相关人员进行应急预案培训和演练；
 - 2) 应核查应急预案培训记录是否明确培训对象、培训内容、培训结果等；
 - 3) 应核查应急预案演练记录是否记录演练时间、主要操作内容、演练结果等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.8.13.4 测评单元（L3-MMS1-44）

该测评单元包括以下要求：

- a) 测评指标：应定期对原有的应急预案重新评估，修订完善；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查应急预案修订记录是否明确修订时间、修订内容等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.14 外包运维管理

8.1.8.14.1 测评单元（L3-MMS1-45）

该测评单元包括以下要求：

- a) 测评指标：应确保外包运维服务商的选择符合国家的有关规定；
- b) 测评对象：运维负责人；
- c) 测评实施：应访谈运维负责人是否有外包运维服务情况，若有，进行外包运维服务的服务单位是否符合国家有关规定；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.14.2 测评单元（L3-MMS1-46）

该测评单元包括以下要求：

- a) 测评指标：应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查外包运维服务协议是否明确约定外包运维的范围和工作内容；

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.14.3 测评单元（L3-MMS1-47）

该测评单元包括以下要求：

- a) 测评指标：应确保选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查与外包运维服务商签订的协议中是否明确其具有等级保护要求的服务能力要求；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.1.8.14.4 测评单元（L3-MMS1-48）

该测评单元包括以下要求：

- a) 测评指标：应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查外包运维服务协议是否包含可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.2 云计算安全测评扩展要求

8.2.1 物理和环境安全

8.2.1.1 物理位置选择

8.2.1.1.1 测评单元（L3-PES2-01）

该测评单元包括以下要求：

- a) 测评指标：应确保云计算基础设施位于中国境内；
- b) 测评对象：机房管理员、办公场地、机房和平台建设方案；
- c) 测评实施包括以下内容：
 - 1) 应访谈机房管理员云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和数据的软硬件是否均位于中国境内；
 - 2) 应核查云平台建设方案是否明确云计算服务器、云管理平台、信息系统上重要信息的处理、存储、业务的运行需位于中国境内。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2 网络和通信安全

8.2.2.1 网络架构

8.2.2.1.1 测评单元（L3-NCS2-01）

该测评单元包括以下要求：

- a) 测评指标：应确保云计算平台不承载高于其安全保护等级的业务应用系统；
- b) 测评对象：云计算平台和业务应用系统定级材料；
- c) 测评实施：应核查云计算平台和云计算平台承载的业务应用系统相关定级材料，查看云计算平台安全保护等级是否不低于其承载的业务应用系统；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

8.2.2.1.2 测评单元（L3-NCS2-02）

该测评单元包括以下要求：

- a) 测评指标：应绘制与当前运行情况相符的虚拟化网络拓扑结构图，并能对虚拟化网络资源、网络拓扑进行实时更新；
- b) 测评对象：综合网管系统、云管理平台、网络拓扑图、网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务商综合网管系统、云管理平台或云服务客户管理平台是否对虚拟化网络资源（如虚拟交换机、虚拟防火墙等）、虚拟网络拓扑进行实时更新；
 - 2) 应核查网络拓扑结构图是否与当前运行情况相符。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2.1.3 测评单元（L3-NCS2-03）

该测评单元包括以下要求：

- a) 测评指标：应实现不同云服务客户虚拟网络之间的隔离；
- b) 测评对象：网络资源隔离措施、综合网管系统和云管理平台；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户之间虚拟网络隔离措施；
 - 2) 应核查云服务客户之间虚拟网络资源隔离策略是否有效；
 - 3) 应测试不同云服务客户之间的网络隔离措施是否生效。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2.1.4 测评单元（L3-NCS2-04）

该测评单元包括以下要求：

- a) 测评指标：应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；
- b) 测评对象：防火墙、入侵检测系统、入侵保护系统和抗 APT 系统等安全设备；
- c) 测评实施包括以下内容：
 - 1) 核查向云服务客户提供的通信传输、边界防护、入侵防范等安全机制是否有效；
 - 2) 核查虚拟防火墙、虚拟入侵保护系统等安全机制是否满足客户业务安全需求。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2.1.5 测评单元（L3-NCS2-05）

该测评单元包括以下要求：

- a) 测评指标：应具有根据云服务客户业务需求自主设置安全策略集的能力，包括定义访问路径、选择安全组件、配置安全策略；
- b) 测评对象：云管理平台、网络管理平台、网络设备和安全访问路径；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务商的云管理平台或网络设备是否支持云服务客户业务自定义安全策略集、安全访问路径、安全组件和安全策略；
 - 2) 应核查云服务客户的网络管理平台或网络设备是否已定义安全访问路径、安全策略和安全组件；
 - 3) 核查云服务商管理员进行远程管理时，管理终端与管理服务器之间是否建立了安全访问路径。
- d) 单元判定：如果 2) 或 1)、3) 为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2.1.6 测评单元（L3-NCS2-06）

该测评单元包括以下要求：

- a) 测评指标：应保证云计算平台管理流量与云服务客户业务流量分离；
- b) 测评对象：网络架构和云管理平台；
- c) 测评实施包括以下内容：
 - 1) 应核查网络架构和配置策略能否采用带外管理或策略配置等方式实现管理流量和业务流量分离；
 - 2) 应核查云平台管理流量与云服务客户业务流量是否分离，核查所采取的技术手段和流量分离手段；
 - 3) 应测试云计算平台管理流量与业务流量是否分离。
- d) 单元判定：如果 1)~3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2.1.7 测评单元（L3-NCS2-07）

该测评单元包括以下要求：

- a) 测评指标：应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云平台选择第三方安全服务；
- b) 测评对象：系统管理员、相关接口和相关服务；
- c) 测评实施包括以下内容：
 - 1) 应核查接口设计文档或开放性服务技术文档是否符合开放性、安全性要求；
 - 2) 如果提供开放接口，应核查内部通信网络（虚拟网络）为第三方安全产品所提供的开放接口安全保障机制、接口配置或参数是否符合安全需求；
 - 3) 如果提供开放性安全产品、服务，应核查开放性安全产品及服务的服务内容和实现开放性安全服务所采用的技术手段、安全保障机制是否符合安全需求。
- d) 单元判定：如果 1)、2) 或 1)、3) 为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2.2 访问控制

8.2.2.2.1 测评单元（L3-NCS2-08）

该测评单元包括以下要求：

- a) 测评指标：应禁止云服务客户虚拟机访问宿主机；
- b) 测评对象：云管理平台和虚拟机监视器；
- c) 测评实施包括以下内容：
 - 1) 应核查云管理平台等能否检测到云服务客户虚拟机对宿主机的访问；
 - 2) 应测试虚拟机监视器和云管理平台，验证是否能够及时检测到云服务客户虚拟机访问宿主机资源等行为并进行报警，如利用虚机逃逸漏洞验证是否触发报警。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2.2.2 测评单元（L3-NCS2-09）

该测评单元包括以下要求：

- a) 测评指标：应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；
- b) 测评对象：访问控制机制、网络边界设备和虚拟化网络边界设备；
- c) 测评实施包括以下内容：
 - 1) 应核查云平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略是否有效；
 - 2) 应核查云平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等是否有效；
 - 3) 应核查不同云服务客户间访问控制规则和访问控制策略是否有效；
 - 4) 应核查云服务客户业务系统不同区域间访问控制规则和访问控制策略是否有效；
 - 5) 应测试虚拟化网络边界访问控制设备，验证是否可以正确拒绝违反访问控制规则的非法访问。
- d) 单元判定：如果 1) -5) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2.2.3 测评单元（L3-NCS2-10）

该测评单元包括以下要求：

- a) 测评指标：应保证当虚拟机迁移时，访问控制策略随其迁移；
- b) 测评对象：虚拟机、虚拟机迁移记录和相关配置；
- c) 测评实施包括以下内容：
 - 1) 应核查虚拟机迁移时访问控制策略随之迁移的措施或手段；
 - 2) 应核查虚拟机迁移记录及相关配置，查看虚拟机迁移后访问控制策略是否部署；
 - 3) 应测试虚拟机迁移，验证访问控制措施是否随其迁移。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2.2.4 测评单元（L3-NCS2-11）

该测评单元包括以下要求：

- a) 测评指标：应允许云服务客户设置不同虚拟机之间的访问控制策略；
- b) 测评对象：云服务商管理平台、云服务客户管理系统和虚拟化网络边界访问控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务商的云管理平台等是否允许云服务客户设置不同虚拟机间访问控制策略；

- 2) 应核查云服务商的云管理平台是否存在不同虚拟机间的访问控制管理模块,是否开启该访问控制功能;
 - 3) 应核查云服务客户管理系统,不同虚拟机间访问控制策略是否安全;
 - 4) 应测试虚拟化网络边界访问控制设备是否可以正确拒绝违反虚拟机间访问控制策略的非法访问。
- d) 单元判定:如果 1)、2)、4)或 3)、4)为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

8.2.2.2.5 测评单元 (L3-NCS2-12)

该测评单元包括以下要求:

- a) 测评指标:应在不同等级的网络区域边界部署访问控制机制,设置访问控制规则;
- b) 测评对象:网闸、防火墙、路由器和交换机等提供访问控制功能的设备;
- c) 测评实施包括以下内容:
 - 1) 应核查不同安全等级网络区域边界的访问控制规则和访问控制策略是否有效;
 - 2) 应测试不同安全等级的网络区域间进行非法访问时,是否可以正确拒绝该非法访问。
- d) 单元判定:如果 1)-2)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

8.2.2.3 入侵防范

8.2.2.3.1 测评单元 (L3-NCS2-13)

该测评单元包括以下要求:

- a) 测评指标:应能检测到云服务客户发起的网络攻击行为,并能记录攻击类型、攻击时间、攻击流量等;
- b) 测评对象:网络入侵检测系统、入侵保护系统、国家认可的相关机制和入侵防范措施;
- c) 测评实施包括以下内容:
 - 1) 应核查是否有专门设备对网络入侵进行防范,核查网络入侵防范规则库的升级方式;
 - 2) 应核查网络入侵检测系统、入侵保护系统或机制,当采用网络入侵防范机制时所采取的机制是否已被测试是安全的(如第三方测试报告),核查入侵检测系统、入侵保护系统或机制的规则库是否为最新;
 - 3) 应测试网络入侵检测系统、入侵保护系统或机制,当采用网络入侵防范机制时所采取的机制是否已被测试是安全的(如第三方测试报告),验证入侵检测系统、入侵保护系统或机制对异常流量和未知威胁的监控策略是否有效(如模拟产生攻击动作,验证网络入侵检测系统、入侵保护系统的反应,是否能记录攻击类型、攻击时间、攻击流量);
 - 4) 应核查系统是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能、报警功能和清洗处置功能;
 - 5) 应核查是否具有对 SQL 注入、跨站脚本等攻击进行检测发现并阻断的能力;
 - 6) 应具有对恶意虚拟机,如具有恶意行为、过分占用计算资源和带宽资源等的虚拟机,进行检测的能力;
 - 7) 应核查云管理平台等对云服务客户攻击的防范措施,核查对云服务客户的网络攻击行为的记录情况,记录应包括攻击类型、攻击时间、攻击流量等;

- 8) 应测试网络入侵检测系统、入侵保护系统或机制,验证其云服务客户网络攻击报警报警策略是否有效(如模拟产生攻击动作,验证网络入侵检测系统、入侵保护系统是否能实时报警);
 - 9) 应对云平台内部发起的恶意攻击或恶意对外连接的行为进行限制,核查是否对内部行为进行监控且保存相关日志记录;
 - 10) 应通过对外攻击发生器伪造对外攻击行为,核查云租的网络攻击的日志记录,确认是否正确记录到相应攻击行为,攻击行为日志记录是否包含攻击类型、攻击时间、攻击者 IP、攻击流量规模等;
 - 11) 应核查运行虚拟机监控器(VMM)和云管理平台软件的物理主机,核查其安全加固手段是是否能够应对虚拟化共享带来的安全漏洞。
- d) 单元判定:如果 1)~11)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

8.2.2.3.2 测评单元(L3-NCS2-14)

该测评单元包括以下要求:

- a) 测评指标:应能检测到对虚拟网络节点的网络攻击行为,并能记录攻击类型、攻击时间、攻击流量等;
- b) 测评对象:网络入侵检测系统、入侵保护系统、国家认可的相关机制和入侵防范措施;
- c) 测评实施包括以下内容:
 - 1) 应核查是否有专门设备对虚拟网络节点的网络攻击行为进行防范,核查网络入侵防范规则库的升级方式;
 - 2) 应核查网络入侵检测系统、入侵保护系统或机制,当对虚拟网络节点采用网络入侵防范机制时所采取的机制是否已被测试是安全的(如第三方测试报告),核查入侵检测系统、入侵保护系统或机制的规则库是否为最新;
 - 3) 应测试网络入侵检测系统、入侵保护系统或机制,当对虚拟网络节点采用网络入侵防范机制时所采取的机制是否已被测试是安全的(如第三方测试报告),验证入侵检测系统、入侵保护系统或机制对异常流量和未知威胁的监控策略是否有效(如模拟产生攻击动作,验证网络入侵检测系统、入侵保护系统的反应,是否能记录攻击类型、攻击时间、攻击流量)。
- d) 单元判定:如果 1)~3)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

8.2.2.3.3 测评单元(L3-NCS2-15)

该测评单元包括以下要求:

- a) 测评指标:应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量,并进行告警;
- b) 测评对象:虚拟机、宿主机、入侵检测系统和入侵保护系统;
- c) 测评实施包括以下内容:
 - 1) 应核查系统是否具备虚拟机与宿主机之间、虚拟机与虚拟机之间的异常流量、大规模攻击流量、高级持续性攻击的检测功能和告警功能;
 - 2) 应核查网络入侵检测系统、入侵保护系统的告警策略和告警记录;
 - 3) 应测试网络入侵检测系统、入侵保护系统,验证其对异常流量和未知威胁的监控策略是否有效(如模拟产生攻击动作,验证网络入侵检测系统、入侵保护系统是否能记录攻击类型、攻击时间、攻击流量)。

- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2.3.4 测评单元 (L3-NCS2-16)

该测评单元包括以下要求：

- a) 测评指标：应向云服务客户提供互联网发布内容监测功能，便于云服务客户对其发布内容中的有害信息进行实时监测和告警；
- b) 测评对象：安全服务、安全组件、监测信息和有害信息过滤规则；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务商安全服务是否可为云服务客户提供互联网发布内容监测功能；
 - 2) 应核查云服务客户能否对其发布到互联网的有害信息进行实时监测并告警；
 - 3) 应核查云服务客户对其发布到互联网有害信息的实时监测情况、历史告警信息。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2.4 安全审计

8.2.2.4.1 测评单元 (L3-NCS2-17)

该测评单元包括以下要求：

- a) 测评指标：应对云服务商和云服务客户远程管理时执行特权命令进行审计，至少包括虚拟机删除、虚拟机重启；
- b) 测评对象：边界网络设备、网络虚拟化设备和相关审计数据；
- c) 测评实施包括以下内容：
 - 1) 应核查对云服务商和云服务客户远程管理时执行的远程特权命令后是否有相关审计记录；
 - 2) 当云服务商采用第三方运维时，应核查第三方运维方是否向云服务商提供审计数据，或云服务商是否可采取措施收集相关审计数据；
 - 3) 应核查边界网络设备、网络虚拟化设备远程执行特权命令的限制措施，核查是否对远程执行特权命令的行为进行安全审计，至少包括虚拟机删除、虚拟机重启；
 - 4) 应测试云服务商或云服务客户远程删除或重启虚拟机后，是否有产生相应审计记录。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2.4.2 测评单元 (L3-NCS2-18)

该测评单元包括以下要求：

- a) 测评指标：应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；
- b) 测评对象：审计数据收集系统、收集设备、云管理平台和审计数据；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务商审计数据收集系统或设备是否根据云服务商和云服务客户的职责划分，实现各自控制部分审计数据的收集；
 - 2) 如果云服务客户授权云服务商收集部分云服务客户控制的审计数据，应核查云服务商是否在不影响其他云服务客户安全的前提下将云服务客户审计数据提供给云服务客户；
 - 3) 应核查云服务商审计数据是否不包括云服务客户控制部分的审计数据。

- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.2.5 集中管控

8.2.2.5.1 测评单元（L3-CMS2-19）

该测评单元包括以下要求：

- a) 测评指标：应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测；
- b) 测评对象：云平台和监控信息汇集接口；
- c) 测评实施包括以下内容：
 - 1) 应核查云平台是否为虚拟化网络、虚拟机、虚拟化安全设备等运行状况监控信息的汇集提供了接口，并实现集中监控；
 - 2) 应核查虚拟化网络、虚拟机、虚拟化安全设备等监控信息汇集接口配置或参数，核查集中监控措施和记录。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.3 设备和计算安全

8.2.3.1 身份鉴别

8.2.3.1.1 测评单元（L3-ECS2-01）

该测评单元包括以下要求：

- a) 测评指标：应在网络策略控制器和网络设备（或设备代理）之间建立通信时验证身份；
- b) 测评对象：网络管理员、网络策略控制器和网络设备（代理设备）；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络管理员是否在网络策略控制器和网络设备（或设备代理）之间建立通信时建立身份验证机制；
 - 2) 应核查网络策略控制器和网络设备（或设备代理）之间的身份验证机制；
 - 3) 应对网络策略控制器和网络设备（代理设备）进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）对网络设备进行渗透测试，验证网络设备防护能力是否符合要求，是否在网络策略控制器和网络设备（或设备代理）之间建立通信时建立身份验证机制。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.3.1.2 测评单元（L3-ECS2-02）

该测评单元包括以下要求：

- a) 测评指标：当进行远程管理时，管理终端和云计算平台边界设备之间应建立双向身份验证机制；
- b) 测评对象：管理终端和云计算平台；
- c) 测评实施包括以下内容：
 - 1) 应核查当进行远程管理时，是否建立双向身份验证机制；

- 2) 应对管理终端和云计算平台进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）对网络设备进行渗透测试，验证网络设备防护能力是否符合要求，是否在管理终端和云计算平台之间建立双向身份验证机制。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.3.2 访问控制

8.2.3.2.1 测评单元（L3-ECS2-03）

该测评单元包括以下要求：

- a) 测评指标：应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；
- b) 测评对象：云平台、数据库、相关授权文档和管理文档；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户数据管理权限授权流程、授权方式、授权内容；
 - 2) 应核查云计算平台是否具有云服务客户数据的管理权限，如果具有，核查相关授权证明及数据管理权限保护措施；
 - 3) 应测试数据库系统，验证云服务商是否不能对云服务客户非授权数据进行管理。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.3.2.2 测评单元（L3-ECS2-04）

该测评单元包括以下要求：

- a) 测评指标：提供云计算平台管理用户权限分离机制，为网络管理员、系统管理员建立不同账户并分配相应的权限；
- b) 测评对象：云管理平台和相关文档；
- c) 测评实施包括以下内容：
 - 1) 应核查云平台运维管理员和云服务运营管理员的权限是否分离，网络管理员、系统管理员是否建立不同账户并分配相应的权限；
 - 2) 应核查云服务商的云管理平台是否提供云平台管理用户权限分离机制，是否能为网络管理、系统管理建立不同账户并分配相应的权限。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.3.3 安全审计

8.2.3.3.1 测评单元（L3-ECS2-05）

该测评单元包括以下要求：

- a) 测评指标：应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计；
- b) 测评对象：安全审计策略、审计设备和审计数据；
- c) 测评实施包括以下内容：
 - 1) 应核查安全审计配置是否能够保证云服务商对云服务客户系统和数据的操作（如增、删、改、查等操作）可被云服务客户审计；

- 2) 应核查是否支持云服务客户部署第三方安全审计设备,保证云服务商对云服务客户系统和数据的操作可被租户审计;
- 3) 应核查云服务商与云服务客户收集的审计数据,查看云服务商对云服务客户系统和数据的操作是否可被云服务客户审计。
- d) 单元判定:如果 1)~3) 均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

8.2.3.4 入侵防范

8.2.3.4.1 测评单元 (L3-ECS2-06)

该测评单元包括以下要求:

- a) 测评指标:应能检测虚拟机之间的资源隔离失效,并进行告警;
- b) 测评对象:系统管理员、服务器、宿主机、虚拟机、操作系统、数据库系统、虚拟机监视器和云平台;
- c) 测评实施包括以下内容:
 - 1) 应核查服务器、宿主机及虚拟机,虚拟机监视器,云平台是否采取措施对不同虚拟机的 CPU、内存和磁盘资源进行隔离,是否实现不同云服务客户自有数据库之间的隔离;是否采取措施能够检测到虚拟机之间的资源隔离失效,并进行告警;
 - 2) 应访谈系统管理员是否采取措施对不同虚拟机资源进行了安全隔离,是否采取措施能够检测到虚拟机之间的资源隔离失效,并进行告警。
- d) 单元判定:如果 1)~2) 均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

8.2.3.4.2 测评单元 (L3-ECS2-07)

该测评单元包括以下要求:

- a) 测评指标:应能检测非授权新建虚拟机或者重新启用虚拟机,并进行告警;
- b) 测评对象:系统管理员、服务器、宿主机、虚拟机、操作系统、数据库系统、虚拟机监视器和云平台;
- c) 测评实施:应核查服务器、宿主机及虚拟机,操作系统,数据库系统,虚拟机监视器,云平台是否能够检测到非授权新建虚拟机或者重新启用虚拟机,并进行告警;
- d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

8.2.3.4.3 测评单元 (L3-ECS2-08)

该测评单元包括以下要求:

- a) 测评指标:应能够检测恶意代码感染及在虚拟机间蔓延的情况,并提出告警;
- b) 测评对象:服务器、宿主机、虚拟机、终端、虚拟机监视器和云平台;
- c) 测评实施包括以下内容:
 - 1) 应核查服务器、宿主机、虚拟机、终端、虚拟机监视器、云平台是否建立恶意代码传播路径追踪机制,是否可以检测查看恶意代码的感染情况,并提出告警。
 - 2) 应核查服务器、宿主机、虚拟机、终端,虚拟机监视器,云平台是否能够检测恶意代码感染及在虚拟机间蔓延的情况,是否能够检测出虚拟机的恶意行为,并提出告警。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.3.5 资源控制

8.2.3.5.1 测评单元 (L3-ECS2-09)

该测评单元包括以下要求：

- a) 测评指标：应屏蔽虚拟资源故障，某个虚拟机宕机后不影响虚拟机监视器及其他虚拟机；
- b) 测评对象：资源控制相关平台和云平台；
- c) 测评实施包括以下内容：
 - 1) 应核查资源控制相关平台所采取的屏蔽虚拟资源故障措施、相关虚拟机故障记录，核查是否不存在虚拟机崩溃后影响虚拟机监视器及其他虚拟机的历史记录；
 - 2) 应核查云平台所采取的屏蔽虚拟资源故障的技术手段是否能在某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.3.5.2 测评单元 (L3-ECS2-10)

该测评单元包括以下要求：

- a) 测评指标：应对物理资源和虚拟资源按照策略做统一管理调度与分配；
- b) 测评对象：运营管理平台、资源调度平台和云管理平台；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户的运营管理平台或资源调度平台的资源调度策略、资源调度分配情况；
 - 2) 应核查云服务商云管理平台所提供策略能否对物理资源和虚拟资源做统一管理调度与分配。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.3.5.3 测评单元 (L3-ECS2-11)

该测评单元包括以下要求：

- a) 测评指标：应确保云计算平台具有虚拟机内存隔离措施；
- b) 测评对象：云管理平台和虚拟机监视器；
- c) 测评实施包括以下内容：
 - 1) 应核查云管理平台和虚拟机监视器的计算资源分配情况、资源分配的审计记录或告警记录是否不存在内存资源过量占用警告；
 - 2) 应核查云计算平台和虚拟机监视器的虚拟机内存隔离措施或机制。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.3.5.4 测评单元 (L3-ECS2-12)

该测评单元包括以下要求：

- a) 测评指标：应确保云服务客户的虚拟机使用独占的内存空间；
- b) 测评对象：云管理平台和虚拟机监视器；

- c) 测评实施包括以下内容：
 - 1) 应核查内存空间分配策略和内存空间分配情况、内存隔离相关审计记录或告警记录是否不存在内存资源过量占用警告，核查是否为云服务客户业务应用系统的虚拟机分配可独占内存空间；
 - 2) 应核查云服务客户虚拟机内存隔离措施或机制是否有效。
- d) 单元判定：如果 1)-2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.3.5.5 测评单元（L3-ECS2-13）

该测评单元包括以下要求：

- a) 测评指标：应对虚拟机的网络接口的带宽进行设置，并进行监测；
- b) 测评对象：云管理平台或其他安全组件；
- c) 测评实施包括以下内容：
 - 1) 应核查云管理平台或其他安全组件是否能对虚拟机网络接口带宽进行设置，是否能对其进行监控；
 - 2) 应核查云管理平台上虚拟机的网络接口带宽的配置及参数、带宽监控记录。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.3.6 镜像和快照保护

8.2.3.6.1 测评单元（L3-ECS2-14）

该测评单元包括以下要求：

- a) 测评指标：应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
- b) 测评对象：云管理平台、虚拟机监视器和虚拟机镜像文件；
- c) 测评实施包括以下内容：
 - 1) 应核查虚拟机监视器是否有对镜像文件定期进行有效性验证的记录；
 - 2) 应核查虚拟机监视器，云管理平台是否提供有效的虚拟机镜像和快照文件管理机制，虚拟机是否能够及时被备份和快照，以及是否准确地恢复到所需还原点；
 - 3) 应核查虚拟机监视器，云管理平台是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。
- d) 单元判定：如果 1)-3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.3.6.2 测评单元（L3-ECS2-15）

该测评单元包括以下要求：

- a) 测评指标：应针对重要业务系统提供加固的操作系统镜像；
- b) 测评对象：云管理平台、虚拟机监视器和虚拟机镜像文件；
- c) 测评实施：应核查虚拟机监视器，云管理平台是否对生成的虚拟机镜像进行必要的加固措施，如关闭不必要的端口、服务及进行安全加固配置；
- d) 单元判定：如果以上测评实施内容均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.3.6.3 测评单元（L3-ECS2-16）

该测评单元包括以下要求：

- a) 测评指标：应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；
- b) 测评对象：云管理平台、虚拟机监视器和虚拟机镜像文件；
- c) 测评实施：应核查虚拟机监视器，云管理平台是否对虚拟机镜像或快照中的敏感资源，通过加密、访问控制、权限控制等技术手段进行保护，防止可能存在的针对快照的非法访问；
- d) 单元判定：如果以上测评实施内容均为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

8.2.4 应用和数据安全

8.2.4.1 数据完整性

8.2.4.1.1 测评单元（L3-ADS2-01）

该测评单元包括以下要求：

- a) 测评指标：应使用校验码或密码技术确保虚拟机迁移过程中，重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；
- b) 测评对象：虚拟机；
- c) 测评实施包括以下内容：
 - 1) 应核查虚拟资源迁移过程中采用的数据完整性保障措施及恢复措施；
 - 2) 应核查在虚拟资源迁移过程中，是否采取校验码或密码技术等措施保证虚拟资源数据及重要数据的完整性，并在检测到完整性受到破坏时是否采取必要的恢复措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.4.2 数据保密性

8.2.4.2.1 测评单元（L3-ADS2-02）

该测评单元包括以下要求：

- a) 测评指标：应使用密码技术确保虚拟机迁移过程中，重要数据的保密性，防止在迁移过程中的重要数据泄露；
- b) 测评对象：系统管理数据（如镜像文件、快照）、鉴别信息和重要业务数据（如用户隐私数据）；
- c) 测评实施包括以下内容：
 - 1) 应核查虚拟机迁移过程中重要数据的保密措施是否能有效防止迁移过程中重要数据的泄露；
 - 2) 应核查是否采取加密或其他保护措施实现系统管理数据（如镜像文件、快照），鉴别信息和重要业务数据（如用户隐私数据）来保证虚拟机迁移过程中重要数据的保密性，防止迁移过程中重要数据的泄露；
 - 3) 应核查是否使用密码技术确保虚拟机迁移过程中，重要数据的保密性。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.4.2.2 测评单元（L3-ADS2-03）

该测评单元包括以下要求：

- a) 测评指标：应支持云服务客户部署密钥管理解决方案，确保云服务客户自行实现数据的加解密过程；
- b) 测评对象：密钥管理解决方案；
- c) 测评实施包括以下内容：
 - 1) 当云服务客户已部署密钥管理解决方案，应核查密钥管理解决方案是否能确保云服务客户自行实现数据的加解密过程；
 - 2) 应核查云服务商支持云服务客户部署密钥管理解决方案所采取的技术手段或管理措施是否能确保云服务客户自行实现数据的加解密过程。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.4.3 数据备份恢复

8.2.4.3.1 测评单元（L3-ADS2-04）

该测评单元包括以下要求：

- a) 测评指标：应提供查询云服务客户数据及备份存储位置的方式；
- b) 测评对象：云管理平台、云平台和相关技术文档；
- c) 测评实施包括以下内容：
 - 1) 应核查云管理平台或云平台为云服务客户提供数据及备份存储位置的查询记录；
 - 2) 应核查云服务商是否为云服务客户提供数据及备份存储位置查询的接口或其他技术、管理手段。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.4.3.2 测评单元（L3-ADS2-05）

该测评单元包括以下要求：

- a) 测评指标：云服务客户应在本地保存其业务数据的备份；
- b) 测评对象：虚拟机、虚拟机监视器和云平台；
- c) 测评实施包括以下内容：应核查是否提供备份措施保证云服务客户可以在本地保存其业务数据；
- d) 单元判定：如果以上测评实施内容均为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

8.2.4.3.3 测评单元（L3-ADS2-06）

该测评单元包括以下要求：

- a) 测评指标：应保证不同云服务客户的审计数据隔离存放；
- b) 测评对象：云服务客户审计数据；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户是否不能访问其他云服务客户审计数据；
 - 2) 应核查是否采取云服务客户审计数据隔离存放措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.4.3.4 测评单元（L3-ADS2-07）

该测评单元包括以下要求：

- a) 测评指标：应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程；
- b) 测评对象：相关技术措施和手段；
- c) 测评实施包括以下内容：
 - 1) 应核查相关技术手段是否能保障云服务客户将业务系统及数据迁移到其他云计算平台和本地系统；
 - 2) 应核查云服务商是否提供措施、手段或人员协助云服务客户完成迁移过程。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.4.3.5 测评单元（L3-ADS2-08）

该测评单元包括以下要求：

- a) 测评指标：云服务商的云存储服务应确保云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；
- b) 测评对象：云存储、相关技术措施和手段；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户数据副本存储方式，核查是否存在若干个可用的副本；
 - 2) 应核查各副本内容保持一致的技术措施或手段是否能保障云服务客户将业务系统及数据迁移到其他云计算平台和本地系统；
 - 3) 应核查云服务商是否提供措施、手段或人员协助云服务客户完成迁移过程。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.4.4 剩余信息保护

8.2.4.4.1 测评单元（L3-ADS2-09）

该测评单元包括以下要求：

- a) 测评指标：应保证虚拟机所使用的内存和存储空间回收时得到完全清除；
- b) 测评对象：系统管理员、虚拟机、虚拟机监视器系统、云管理平台系统、操作系统技术开发手册或产品检测报告、数据库系统技术开发手册和产品检测报告；
- c) 测评实施包括以下内容：
 - 1) 应核查资源抽象层用户的鉴别信息存储空间在回收时的数据清除策略；
 - 2) 应核查系统和数据库系统技术开发手册或产品检测报告，查看用户的鉴别信息存储空间回收时是否得到完全清除；
 - 3) 应核查操作系统和数据库系统技术开发手册或产品检测报告，查看文件、目录和数据库记录等资源所在的存储空间回收时是否得到完全清除；
 - 4) 应核查虚拟机监视器和云管理平台内的文件、目录、数据库记录和虚拟资源等所在的存储空间回收时是否得到完全清除；
 - 5) 应核查虚拟机的内存和存储空间回收时，是否得到完全清除；
 - 6) 应核查在迁移或删除虚拟机后，数据以及备份数据（如镜像文件、快照文件等）是否已清理。

- d) 单元判定：如果 1) -6) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.4.4.2 测评单元 (L3-ADS2-10)

该测评单元包括以下要求：

- a) 测评指标：云服务客户删除业务应用数据时，云计算平台应确保云存储中所有副本被删除；
- b) 测评对象：云存储和云计算平台；
- c) 测评实施包括以下内容：
 - 1) 应核查云平台中云服务客户业务应用数据备份方式和备份管理方式，当云服务客户删除业务应用数据时，核查是否支持所有副本删除；
 - 2) 应核查云计算平台，当云服务客户删除业务应用数据时，云存储中所有副本是否被删除。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.4.5 个人信息保护

8.2.4.5.1 测评单元 (L3-ADS2-11)

该测评单元包括以下要求：

- a) 测评指标：应确保云服务客户账户信息、鉴别信息、系统信息存储于中国境内，如需出境应遵循国家相关规定；
- b) 测评对象：数据库服务器、数据存储设备和管理文档记录；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户账户信息、鉴别信息、系统信息所在的服务器及数据存储设备是否存储于中国境内；
 - 2) 应核查相关管理文档或记录，核查云服务客户账户信息、鉴别信息、系统信息及其备份是否存储于中国境内。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.5 安全建设管理

8.2.5.1 云服务商选择

8.2.5.1.1 测评单元 (L3-CMS2-01)

该测评单元包括以下要求：

- a) 测评指标：应选择安全合规的云服务商，其所提供的云平台应为其所承载的业务应用系统提供相应等级的安全保护能力；
- b) 测评对象：系统建设负责人、安全责任合同书、保密协议和服务合同；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统建设负责人是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云平台及云服务商；
 - 2) 应核查云服务商提供的相关服务合同是否明确其云平台具有与所承载的业务应用系统相应或高于的安全保护能力。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.5.1.2 测评单元 (L3-CMS2-02)

该测评单元包括以下要求：

- a) 测评指标：应在服务水平协议中规定云服务的各项服务内容和具体技术指标；
- b) 测评对象：服务水平协议；
- c) 测评实施包括以下内容：
 - 1) 应核查服务水平协议是否规定了云服务的各项服务内容和具体指标、服务期限、双方签字或盖章等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

8.2.5.1.3 测评单元 (L3-CMS2-03)

该测评单元包括以下要求：

- a) 测评指标：应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；
- b) 测评对象：服务水平协议；
- c) 测评实施：应核查服务水平协议中是否规范了安全服务商和云服务供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

8.2.5.1.4 测评单元 (L3-CMS2-04)

该测评单元包括以下要求：

- a) 测评指标：应在服务水平协议中规定服务合约到期时，完整地返还云服务客户信息，并承诺相关信息在云计算平台上清除；
- b) 测评对象：服务水平协议；
- c) 测评实施包括以下内容：
 - 1) 应核查服务水平协议是否明确服务合约到期时，云服务商完整地返还云服务客户信息，并承诺相关信息在云平台上清除；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

8.2.5.1.5 测评单元 (L3-CMS2-05)

该测评单元包括以下要求：

- a) 测评指标：应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据和业务系统的相关重要信息；
- b) 测评对象：安全责任合同书、保密协议和服务合同；
- c) 测评实施：应核查安全责任合同书、保密协议或服务合同是否包含对云服务商不得泄露云服务客户数据和业务系统的相关重要信息的要求；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

8.2.5.1.6 测评单元（L3-CMS2-06）

该测评单元包括以下要求：

- a) 测评指标：应对可能接触到云服务客户数据的员工进行背景调查，并签署保密协议；
- b) 测评对象：系统建设负责人、调查文件或调查报告、保密协议；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统建设负责人是否与云服务商可接触到云服务客户数据的员工签订保密协议，并进行背景调查；
 - 2) 应核查员工保密协议是否明确相关保密义务；
 - 3) 应核查背景调查报告是否明确人员相关背景调查情况。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.5.2 供应链管理

8.2.5.2.1 测评单元（L3-CMS2-07）

该测评单元包括以下要求：

- a) 测评指标：应确保供应商的选择符合国家有关规定；
- b) 测评对象：系统建设负责人；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统建设负责人云服务商的选择是否符合国家的有关规定；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

8.2.5.2.2 测评单元（L3-CMS2-08）

该测评单元包括以下要求：

- a) 测评指标：应确保供应链安全事件信息或威胁信息能够及时传达到云服务客户；
- b) 测评对象：系统建设负责人、供应链安全事件或威胁报告；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统建设负责人云服务商供应商是否及时传达安全事件或威胁信息；
 - 2) 应核查供应链安全事件或威胁报告是否明确相关事件信息或威胁信息。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.5.2.3 测评单元（L3-CMS2-09）

该测评单元包括以下要求：

- a) 测评指标：应保证供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取有关措施对风险进行控制；
- b) 测评对象：供应商重要变更记录、安全风险评估报告和风险预案；
- c) 测评实施：应核查安全风险评估报告和风险预案，确认对每次供应商的重要变更都进行评估与风险预案设计；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

8.2.6 安全运维管理

8.2.6.1 云计算环境管理

8.2.6.1.1 测评单元（L3-MMS2-01）

该测评单元包括以下要求：

- a) 测评指标：云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定；
- b) 测评对象：运维设备、运维地点、运维记录和相关管理文档；
- c) 测评实施包括以下内容：
 - 1) 应核查运维地点是否位于中国境内，是否不存在从境外对境内云计算平台实施远程运维的设备、地点和相关内容；
 - 2) 应核查云计算平台远程运维记录中境外对境内云计算平台实施运维操作是否遵循国家相关规定。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.2.6.1.2 测评单元（L3-MMS2-02）

该测评单元包括以下要求：

- a) 测评指标：云计算平台运维过程产生的配置数据、日志信息等存储于中国境内，如需出境应遵循国家相关规定；
- b) 测评对象：云计算平台运行管理设计文档和管理文档；
- c) 测评实施包括以下内容：
 - 1) 应核查云计算平台运维过程产生的配置数据、日志信息等是否存储于中国境内；
 - 2) 对于有出境需求的配置数据和日志信息，应核查数据出境是否遵循国家相关规定。
- d) 单元判定：如果 1) 或 2) 为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

8.3 移动互联安全测评扩展要求

8.3.1 物理和环境安全

8.3.1.1 无线接入点的物理位置

8.3.1.1.1 测评单元（L3-PES3-01）

该测评单元包括以下要求：

- a) 测评指标：应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰；
- b) 测评对象：无线接入设备；
- c) 测评实施包括以下内容：
 - 1) 应核查物理位置与无线信号的覆盖范围；
 - 2) 应测试无线信号的覆盖范围并测试在一定范围内是否可以进行电磁干扰。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.2 网络和通信安全

8.3.2.1 边界防护

8.3.2.1.1 测评单元（L3-NCS3-01）

该测评单元包括以下要求：

- a) 测评指标：应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备；
- b) 测评对象：无线接入网关设备；
- c) 测评实施：应核查有线网络与无线网络边界之间是否部署无线接入网关设备；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.2.2 访问控制

8.3.2.2.1 测评单元（L3-NCS3-02）

该测评单元包括以下要求：

- a) 测评指标：无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证；
- b) 测评对象：无线接入设备；
- c) 测评实施：应核查无线接入设备是否开启接入认证功能，是否采用认证服务器或国家密码管理机构批准的密码模块进行认证；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.2.3 入侵防范

8.3.2.3.1 测评单元（L3-NCS3-03）

该测评单元包括以下要求：

- a) 测评指标：应能够检测、记录、定位非授权无线接入设备；
- b) 测评对象：入侵防范设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否能够检测、记录、定位非授权无线接入设备；
 - 2) 应测试是否能够检测、记录、定位非授权无线接入设备。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.2.3.2 测评单元（L3-NCS3-04）

该测评单元包括以下要求：

- a) 测评指标：应能够对非授权移动终端接入的行为进行检测、记录、定位；
- b) 测评对象：入侵防范设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否能够检测、记录、定位非授权移动终端接入；
 - 2) 应测试是否能够检测、记录、定位非授权移动终端接入。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.2.3.3 测评单元 (L3-NCS3-05)

该测评单元包括以下要求：

- a) 测评指标：应具备对针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位；
- b) 测评对象：入侵防范设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否能够对网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位；
 - 2) 应核查规则库版本，查看其规则库是否及时更新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.2.3.4 测评单元 (L3-NCS3-06)

该测评单元包括以下要求：

- a) 测评指标：应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；
- b) 测评对象：入侵防范设备；
- c) 测评实施：应核查入侵防范设备，是否能够检测无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.2.3.5 测评单元 (L3-NCS3-07)

该测评单元包括以下要求：

- a) 测评指标：应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等；
- b) 测评对象：无线接入设备和无线接入网关设备；
- c) 测评实施：应核查是否关闭了 SSID 广播、WEP 认证等存在风险的功能；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.2.3.6 测评单元 (L3-NCS3-08)

该测评单元包括以下要求：

- a) 测评指标：应禁止多个 AP 使用同一个鉴别密钥；
- b) 测评对象：无线接入设备；
- c) 测评实施：应核查是否分别使用了不同的鉴别密钥；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.3 设备和计算安全

8.3.3.1 移动终端管控

8.3.3.1.1 测评单元 (L3-ECS3-01)

该测评单元包括以下要求：

- a) 测评指标：应保证移动终端安装、注册并运行终端管理客户端软件；
- b) 测评对象：移动终端和移动终端管理系统；
- c) 测评实施：应核查移动终端管理系统，查看移动终端客户端软件的安装、注册与管理策略；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.3.1.2 测评单元（L3-ECS3-02）

该测评单元包括以下要求：

- a) 测评指标：移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等；
- b) 测评对象：移动终端和移动终端管理系统；
- c) 测评实施包括以下内容：
 - 1) 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等安全策略；
 - 2) 应测试是否能够对移动终端进行远程锁定和远程擦除等。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.3.2 移动应用管控

8.3.3.2.1 测评单元（L3-ECS3-03）

该测评单元包括以下要求：

- a) 测评指标：应具有选择应用软件安装、运行的功能；
- b) 测评对象：移动终端管理客户端；
- c) 测评实施：应核查是否具有选择应用软件安装、运行的功能；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.3.2.2 测评单元（L3-ECS3-04）

该测评单元包括以下要求：

- a) 测评指标：应具有软件白名单功能，应能根据白名单控制应用软件安装、运行；
- b) 测评对象：移动终端管理客户端；
- c) 测评实施包括以下内容：
 - 1) 应核查是否具有软件白名单功能；
 - 2) 应测试使用白名单控制应用软件安装、运行。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.3.2.3 测评单元（L3-ECS3-05）

该测评单元包括以下要求：

- a) 测评指标：应具有应用软件权限控制功能，应能控制应用软件对移动终端中资源的访问；
- b) 测评对象：移动终端管理客户端；
- c) 测评实施包括以下内容：

- 1) 应核查是否具有应用软件权限控制功能;
- 2) 应测试是否可以对移动终端中资源的访问进行限制。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

8.3.3.2.4 测评单元 (L3-ECS3-06)

该测评单元包括以下要求:

- a) 测评指标: 应只允许系统管理者指定证书签名的应用软件安装和运行;
- b) 测评对象: 移动终端管理客户端;
- c) 测评实施: 应核查允许使用的签名证书, 且证书是否由系统管理者指定;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

8.3.3.2.5 测评单元 (L3-ECS3-07)

该测评单元包括以下要求:

- a) 测评指标: 应具有接受移动终端管理服务端推送的移动应用软件管理策略, 并根据该策略对软件实施管控的能力;
- b) 测评对象: 移动终端管理客户端;
- c) 测评实施: 应核查是否具有接受移动终端管理服务端远程管控的能力;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

8.3.3.3 资源控制

8.3.3.3.1 测评单元 (L3-ECS3-08)

该测评单元包括以下要求:

- a) 测评指标: 应保证移动终端处理不同等级系统业务的运行环境进行操作系统级隔离;
- b) 测评对象: 移动终端;
- c) 测评实施: 应核查是否采用安装双系统或其它安全隔离措施进行操作系统级隔离;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

8.3.3.3.2 测评单元 (L3-ECS3-09)

该测评单元包括以下要求:

- a) 测评指标: 应限制用户或进程对移动终端系统资源的最大使用限度, 防止移动终端被提权;
- b) 测评对象: 移动终端;
- c) 测评实施: 应核查是否可以对用户或进程等可访问资源进行限定, 是否可以防止移动终端被提权;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

8.3.4 安全管理

8.3.4.1 移动应用软件采购

8.3.4.1.1 测评单元 (L3-CMS3-01)

该测评单元包括以下要求：

- a) 测评指标：应保证移动终端安装、运行的应用软件来自系统管理者指定证书签名或可靠分发渠道；
- b) 测评对象：安全管理员；
- c) 测评实施：应访谈安全管理员，移动应用软件是否采用系统管理者指定的证书签名或使用可靠的分发渠道；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.4.1.2 测评单元 (L3-CMS3-02)

该测评单元包括以下要求：

- a) 测评指标：应保证移动终端安装、运行的移动应用软件由经审核的开发者开发；
- b) 测评对象：安全管理员；
- c) 测评实施：应访谈安全管理员，移动应用软件是否由经审核的开发者开发；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.4.2 移动应用软件开发

8.3.4.2.1 测评单元 (L3-CMS3-03)

该测评单元包括以下要求：

- a) 测评指标：应要求对移动业务应用软件开发进行资格审查；
- b) 测评对象：系统建设负责人；
- c) 测评实施：应访谈系统建设负责人，是否对开发者进行资格审查；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.4.2.2 测评单元 (L3-CMS3-04)

该测评单元包括以下要求：

- a) 测评指标：应确保开发移动业务应用软件的签名证书合法性；
- b) 测评对象：软件的签名证书；
- c) 测评实施：应核查开发移动业务应用软件的签名证书是否具有合法性；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.3.5 安全运维管理

8.3.5.1 配置管理

8.3.5.1.1 测评单元 (L3-MMS3-01)

该测评单元包括以下要求：

- a) 测评指标：应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别；

- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查记录表单类文档，是否建立无线接入设备和合法移动终端配置库，并通过配置库识别非法设备；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.4 物联网安全测评扩展要求

8.4.1 物理和环境安全

8.4.1.1 感知节点设备物理防护

8.4.1.1.1 测评单元（L3-PES4-01）

该测评单元包括以下要求：

- a) 测评指标：感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；
- b) 测评对象：感知节点设备所处物理环境和设计或验收文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈物理安全负责人现有感知节点设备的环境条件是否具有防挤压、防强振动等防物理破坏的能力；
 - 2) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备所处物理环境具有防挤压、防强振动等能力的说明，是否与实际情况一致；
 - 3) 应核查感知节点设备所处物理环境是否采取了防挤压、防强振动等的防护措施。
- d) 单元判定：如果 1)～3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.1.1.2 测评单元（L3-PES4-02）

该测评单元包括以下要求：

- a) 测评指标：感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）；
- b) 测评对象：感知节点设备所处物理环境和设计或验收文档；
- c) 测评实施包括以下内容：
 - 1) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备在工作状态所处物理环境的说明，是否与实际情况一致；
 - 2) 应核查感知节点设备在工作状态所处物理环境是否能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。
- d) 单元判定：如果 1)～2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.1.1.3 测评单元（L3-PES4-03）

该测评单元包括以下要求：

- a) 测评指标：感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等；
- b) 测评对象：感知节点设备所处物理环境和设计或验收文档；
- c) 测评实施包括以下内容：

- 1) 应访谈物理安全负责人现有感知节点设备的环境条件是否对感知节点设备的正常工作造成影响，是否采取了防强干扰、防阻挡屏蔽等措施；
 - 2) 应核查感知节点设备所处物理环境的设计或验收文档，是否具有感知节点设备所处物理环境防强干扰、防阻挡屏蔽等能力的说明，是否与实际情况一致；
 - 3) 应核查感知节点设备所处物理环境是否采取了防强干扰、防阻挡屏蔽等防护措施。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.1.1.4 测评单元 (L3-PES4-04)

该测评单元包括以下要求：

- a) 测评指标：关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久的、稳定的电力供应能力）；
- b) 测评对象：关键感知节点设备的供电设备（关键网关节点设备的供电设备）和设计或验收文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈物理安全负责人现有关键感知节点设备（关键网关节点设备）是否设置了可供长时间工作的电力供应措施（持久的、稳定的电力供应措施），供电时间是否满足设备的电力供应需求；
 - 2) 应核查关键感知节点设备（关键网关节点设备）电力供应设计或验收文档是否标明电力供应要求，其中是否明确保障关键感知节点设备长时间工作的电力供应措施（关键网关节点设备持久的、稳定的电力供应措施）；
 - 3) 应核查是否具有相关电力供应措施的运行维护记录，是否与电力供应设计一致。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.2 网络和通信安全

8.4.2.1 入侵防范

8.4.2.1.1 测评单元 (L3-NCS4-01)

该测评单元包括以下要求：

- a) 测评指标：应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为；
- b) 测评对象：感知节点设备和设计文档；
- c) 测评实施包括以下内容：
 - 1) 应核查感知层安全设计文档，是否有对感知节点通信目标地址的控制措施说明；
 - 2) 应核查感知节点设备，是否配置了对感知节点通信目标地址的控制措施，相关参数配置是否符合设计要求；
 - 3) 应对感知节点设备进行渗透测试，测试是否能够限制感知节点设备对违反访问控制策略的通信目标地址进行访问或攻击。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.2.1.2 测评单元 (L3-NCS4-02)

该测评单元包括以下要求：

- a) 测评指标：应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为；

- b) 测评对象：网关节点设备和设计文档；
- c) 测评实施包括以下内容：
 - 1) 应核查感知层安全设计文档，是否有对网关节点通信目标地址的控制措施说明；
 - 2) 应核查网关节点设备，是否配置了对网关节点通信目标地址的控制措施，相关参数配置是否符合设计要求；
 - 3) 应对感知节点设备进行渗透测试，测试是否能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.2.2 接入控制

8.4.2.2.1 测评单元（L3-NCS4-03）

该测评单元包括以下要求：

- a) 测评指标：应确保只有授权的感知节点可以接入；
- b) 测评对象：感知节点设备和设计文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术、身份鉴别技术等，具体措施有哪些；
 - 2) 应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述；
 - 3) 应对边界和感知层网络进行渗透测试，测试是否不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3 设备和计算安全

8.4.3.1 感知节点设备安全

8.4.3.1.1 测评单元（L3-ECS4-01）

该测评单元包括以下要求：

- a) 测评指标：应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更；
- b) 测评对象：感知节点设备；
- c) 测评实施包括以下内容：
 - 1) 应核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更；
 - 2) 应测试通过试图接入和控制传感网访问未授权的资源，验证感知节点设备的访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3.1.2 测评单元（L3-ECS4-02）

该测评单元包括以下要求：

- a) 测评指标：应具有对连接的网关节点设备（包括读卡器）设备进行身份标识和鉴别的能力；
- b) 测评对象：网关节点设备（包括读卡器）；
- c) 测评实施包括以下内容：
 - 1) 应核查是否对连接的网关节点设备（包括读卡器）设备进行身份标识与鉴别，是否配置了符合安全策略的参数；
 - 2) 应进行渗透测试，验证是否不存在绕过身份标识与鉴别功能的方法。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3.1.3 测评单元（L3-ECS4-03）

该测评单元包括以下要求：

- a) 测评指标：应具有对连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力；
- b) 测评对象：其他感知节点设备（包括路由节点）；
- c) 测评实施包括以下内容：
 - 1) 应核查是否对连接的其他感知节点设备（包括路由节点）设备进行身份标识与鉴别，是否配置了符合安全策略的参数；
 - 2) 应进行渗透测试，验证是否不存在绕过身份标识与鉴别功能的方法。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3.2 网关节点设备安全

8.4.3.2.1 测评单元（L3-ECS4-04）

该测评单元包括以下要求：

- a) 测评指标：应设置最大并发连接数；
- b) 测评对象：网关节点设备；
- c) 测评实施：应核查网关节点设备是否配置了最大并发连接数参数；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3.2.2 测评单元（L3-ECS4-05）

该测评单元包括以下要求：

- a) 测评指标：应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力；
- b) 测评对象：网关节点设备；
- c) 测评实施包括以下内容：
 - 1) 应核查网关节点设备是否能够对连接设备（包括终端节点、路由节点、数据处理中心）进行标识并配置了鉴别功能；
 - 2) 应进行渗透测试，验证是否不存在绕过身份标识与鉴别功能的方法。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3.2.3 测评单元（L3-ECS4-06）

该测评单元包括以下要求：

- a) 测评指标：应具备过滤非法节点和伪造节点所发送的数据的能力；
- b) 测评对象：网关节点设备；
- c) 测评实施包括以下内容：
 - 1) 应核查网关节点设备是否配置了过滤非法节点和伪造节点发送的数据的功能；
 - 2) 应测试网关节点设备，是否能够过滤非法节点和伪造节点发送的数据。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3.2.4 测评单元（L3-ECS4-07）

该测评单元包括以下要求：

- a) 测评指标：授权用户应能够在设备使用过程中对关键密钥进行在线更新；
- b) 测评对象：感知节点设备；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员有哪些感知节点设备需要采用密钥进行通信，是否对设备的关键密钥进行在线更新；
 - 2) 应核查感知节点设备是否对其关键密钥进行在线更新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.3.2.5 测评单元（L3-ECS4-08）

该测评单元包括以下要求：

- a) 测评指标：授权用户应能够在设备使用过程中对关键配置参数进行在线更新；
- b) 测评对象：感知节点设备；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员感知节点设备是否支持对其关键配置参数进行在线更新；
 - 2) 应核查感知节点设备在线更新方式是否有效。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.4 应用和数据安全

8.4.4.1 抗数据重放

8.4.4.1.1 测评单元（L3-ADS4-01）

该测评单元包括以下要求：

- a) 测评指标：应能够鉴别数据的新鲜性，避免历史数据的重放攻击；
- b) 测评对象：感知节点设备；
- c) 测评实施包括以下内容：
 - 1) 应核查感知节点设备鉴别数据新鲜性的措施，是否能够避免历史数据重放；
 - 2) 应将感知节点设备历史数据进行重放测试，验证其保护措施是否生效。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.4.1.2 测评单元（L3-ADS4-02）

该测评单元包括以下要求：

- a) 测评指标：应能够鉴别历史数据的非法修改，避免数据的修改重放攻击；
- b) 测评对象：感知节点设备；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员针对感知节点设备历史数据的保护措施，具体措施有哪些，是否具有对历史数据被非法修改的检测措施，检测措施有哪些；
 - 2) 应核查感知层是否配备检测感知节点设备历史数据被非法篡改的措施，在检测到被修改时是否能采取必要的恢复措施；
 - 3) 应测试检测措施的有效性，是否能够避免数据的修改重放攻击。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.4.2 数据融合处理

8.4.4.2.1 测评单元（L3-ADS4-03）

该测评单元包括以下要求：

- a) 测评指标：应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用；
- b) 测评对象：物联网应用系统；
- c) 测评实施包括以下内容：
 - 1) 应访谈应用系统管理员来自传感网的数据的类型和数据格式等；
 - 2) 应核查是否提供对来自传感网的数据进行数据融合处理的功能；
 - 3) 应测试数据融合处理功能是否能够处理不同种类的数据。
- d) 单元判定：如果 2) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.5 安全运维管理

8.4.5.1 感知节点管理

8.4.5.1.1 测评单元（L3-MMS4-01）

该测评单元包括以下要求：

- a) 测评指标：应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；
- b) 测评对象：维护记录；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统运维负责人是否有专门的人员对感知节点设备、网关节点设备进行定期维护，由何部门或何人负责，维护周期多长；
 - 2) 应核查感知节点设备、网关节点设备部署环境维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.5.1.2 测评单元（L3-MMS4-02）

该测评单元包括以下要求：

- a) 测评指标：应记录感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息），对网关设备进行现场维护（除尘、充电、修理等）；
- b) 测评对象：维护记录；
- c) 测评实施：应核查感知节点设备、网关节点设备部署环境维护记录是否包括了感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息）核查、对网关设备进行现场维护（除尘、充电、修理等）等方面内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.5.1.3 测评单元（L3-MMS4-03）

该测评单元包括以下要求：

- a) 测评指标：应对感知节点和网关节点设备部署环境的评估方法作出明确规定；
- b) 测评对象：感知节点和网关节点设备部署环境的评估说明文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统运维负责人是否明确规定需对感知节点和网关节点设备部署环境进行评估；
 - 2) 应核查感知节点和网关节点设备部署环境的评估说明文档内容是否包含可操作的评估方法。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.5.1.4 测评单元（L3-MMS4-04）

该测评单元包括以下要求：

- a) 测评指标：应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；
- b) 测评对象：感知节点和网关节点设备安全管理文档；
- c) 测评实施：
 - 1) 应访谈系统运维负责人是否明确规定需对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程进行全程管理；
 - 2) 应核查感知节点和网关节点设备安全管理文档是否覆盖感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等方面。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.5.1.5 测评单元（L3-MMS4-05）

该测评单元包括以下要求：

- a) 测评指标：应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等；
- b) 测评对象：感知节点设备、网关节点设备部署环境的管理制度；
- c) 测评实施：

- 1) 应核查感知节点设备、网关节点设备部署环境管理文档是否包括负责核查和维护的人员调离工作岗位立即交还相关核查工具和核查维护记录等方面内容；
- 2) 应核查是否具有感知节点设备、网关节点设备部署环境的相关保密性管理记录。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5 工业控制系统安全测评扩展要求

8.5.1 物理和环境安全

8.5.1.1 室外控制设备物理防护

8.5.1.1.1 测评单元 (L3-PES5-01)

该测评单元包括以下要求：

- a) 测评指标：室外控制设备应放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；控制设备应安装在金属或其它绝缘板上(非木质板)，并紧固于箱体或装置中；
- b) 测评对象：室外控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；
 - 2) 应核查是否安装在金属或其它绝缘板上(非木质板)，并紧固于箱体或装置中。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.1.1.2 测评单元 (L3-PES5-02)

该测评单元包括以下要求：

- a) 测评指标：室外控制设备放置应远离强电磁干扰、热源和应远离极端天气环境等，如无法避免，在遇到极端天气时应及时做好应急处置及检修确保设备正常运行；
- b) 测评对象：室外控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否远离极端天气环境；
 - 2) 应核查是否有极端天气时的应急处置及检修维护记录；
 - 3) 应核查位置放置是否远离强电磁干扰和热源。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.2 网络和通信安全

8.5.2.1 网络架构

8.5.2.1.1 测评单元 (L3-NCS5-01)

该测评单元包括以下要求：

- a) 测评指标：工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用单向的技术隔离手段；

- b) 测评对象：网闸、路由器、交换机和防火墙等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查工业控制系统的网络是否部署单向隔离设备；
 - 2) 应核查在网络边界处是否采用了有效的单向隔离策略实施访问控制；
 - 3) 应核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离强度相同的措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.2.1.2 测评单元（L3-NCS5-02）

该测评单元包括以下要求：

- a) 测评指标：工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；
- b) 测评对象：路由器、交换机和防火墙等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查工业控制系统内部不同的子系统类型，是否按照安全等级和安全防护强度等业务特点划分了不同的安全域；
 - 2) 应核查各安全域之间交换机和防火墙是否配置了有效的访问控制策略。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.2.1.3 测评单元（L3-NCS5-03）

该测评单元包括以下要求：

- a) 测评指标：涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其它数据网及外部公共信息网的安全隔离；
- b) 测评对象：路由器和交换机等提供网络通信功能的设备；
- c) 测评实施：应核查工业控制系统关键区域的传输数据要求，涉及实时传输数据与控制要求的，核查是否采用独立的网络和设备组网实现关键部位安全防护；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.5.2.2 通信传输

8.5.2.2.1 测评单元（L3-NCS5-04）

该测评单元包括以下要求：

- a) 测评指标：在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输；
- b) 测评对象：加密认证设备、路由器、交换机和防火墙等提供访问控制功能的设备；
- c) 测评实施：应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术手段实现身份认证、访问控制和数据加密传输；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.5.2.3 访问控制

8.5.2.3.1 测评单元（L3-NCS5-05）

该测评单元包括以下要求：

- a) 测评指标：工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查在工业控制系统与企业其他系统之间的网络边界是否部署访问控制设备，是否配置访问控制策略；
 - 2) 应核查设备安全策略，是否禁止 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越边界。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.2.3.2 测评单元（L3-NCS5-06）

该测评单元包括以下要求：

- a) 测评指标：应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备，监控预警设备；
- c) 测评实施包括以下内容：
 - 1) 应核查设备是否可以在策略失效的时候进行告警；
 - 2) 应核查是否部署监控预警系统或相关模块，在边界防护机制失效时可及时告警。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.2.4 拨号使用控制

8.5.2.4.1 测评单元（L3-NCS5-07）

该测评单元包括以下要求：

- a) 测评指标：工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量；并采取用户身份鉴别和访问控制等措施；
- b) 测评对象：拨号服务类设备；
- c) 测评实施包括以下内容：
 - 1) 应核查工业控制系统是否确需使用拨号服务；
 - 2) 应核查拨号设备是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用账户/口令等身份鉴别方式，是否采用控制账户权限等访问控制措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.2.4.2 测评单元（L3-NCS5-08）

该测评单元包括以下要求：

- a) 测评指标：拨号服务器和客户端均应使用经安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施；
- b) 测评对象：拨号服务类设备；

- c) 测评实施：应核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.5.2.5 无线使用控制

8.5.2.5.1 测评单元（L3-NCS5-09）

该测评单元包括以下要求：

- a) 测评指标：应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；
- b) 测评对象：无线通信网络及设备；
- c) 测评实施包括以下内容：
 - 1) 应核查无线通信的用户在登录时是否采用了身份鉴别措施；
 - 2) 应核查无线通信的用户列表，核查用户身份标识是否具有唯一性。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.2.5.2 测评单元（L3-NCS5-10）

- a) 测评指标：应对所有参与无线通信的用户（人员、软件进程或者设备）进行授权以及执行使用进行限制；
- b) 测评对象：无线通信网络及设备；
- c) 测评实施：应核查无线通信过程中是否对用户进行授权，核查具体权限是否合理；核查未授权的使用是否可以被发现及告警；
- d) 单元判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.5.2.5.3 测评单元（L3-NCS5-11）

该测评单元包括以下要求：

- a) 测评指标：应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护；
- b) 测评对象：无线通信网络及设备；
- c) 测评实施：应核查无线通信传输中是否采用加密措施保证传输报文的机密性；
- d) 单元判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.5.2.5.4 测评单元（L3-NCS5-12）

该测评单元包括以下要求：

- a) 测评指标：对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统行为；
- b) 测评对象：无线通信网络及设备 and 监测设备；
- c) 测评实施：应核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备应及时发出告警并可以对试图接入的无线设备进行屏蔽；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.5.3 设备和计算安全

8.5.3.1 控制设备安全

8.5.3.1.1 测评单元（L3-ECS5-01）

该测评单元包括以下要求：

- a) 测评指标：控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等设备和计算方面的安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；
- b) 测评对象：控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；
 - 2) 如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。
- d) 单元判定：如果 2) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.5.3.1.2 测评单元（L3-ECS5-02）

该测评单元包括以下要求：

- a) 测评指标：应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；
- b) 测评对象：控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查测试环境或测试报告，核查是否有测试评估记录；
 - 2) 应核查控制设备版本、补丁及固件是否经过充分测试后进行了更新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.3.1.3 测评单元（L3-ECS5-03）

该测评单元包括以下要求：

- a) 测评指标：应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口等，确需保留的必须通过相关的技术措施实施严格的监控管理；
- b) 测评对象：控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查控制设备是否关闭或拆除设备的软盘驱动、光盘驱动、USB 接口、串行口等；
 - 2) 应核查保留的软盘驱动、光盘驱动、USB 接口、串行口等是否通过相关的措施实施严格的监控管理。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.3.1.4 测评单元（L3-ECS5-04）

该测评单元包括以下要求：

- a) 测评指标：应使用专用设备和专用软件对控制设备进行更新；

- b) 测评对象：控制设备；
- c) 测评实施：应核查更新控制设备时是否为专用设备和专用软件；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.5.3.1.5 测评单元（L3-ECS5-05）

该测评单元包括以下要求：

- a) 测评指标：应保证控制设备在上线前经过安全性检测，确保控制设备固件中不存在恶意代码程序；
- b) 测评对象：控制设备；
- c) 测评实施：应核查控制设备在上线前的检测报告，明确控制设备固件中是否不存在恶意代码程序；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.5.4 安全建设管理

8.5.4.1 产品采购和使用

8.5.4.1.1 测评单元（L3-CMS5-01）

该测评单元包括以下要求：

- a) 测评指标：工业控制系统重要设备及专用信息安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用；
- b) 测评对象：安全管理员和检测报告类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员系统使用的工业控制系统重要设备及专用信息安全产品是否通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测；
 - 2) 应核查工业控制系统是否有通过国家及行业监管部门认可的专业机构出具的安全性及电磁兼容性检测的检测报告。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.4.2 外包软件开发

8.5.4.2.1 测评单元（L3-CMS5-02）

该测评单元包括以下要求：

- a) 测评指标：应在外包开发合同中包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款；
- b) 测评对象：外包合同；
- c) 测评实施：应核查外包开发合同中是否包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.5.5 安全运维管理

8.5.5.1 漏洞和风险管理

8.5.5.1.1 测评单元（L3-MMS5-01）

该测评单元包括以下要求：

- a) 测评指标：应采取必要的措施识别安全漏洞和隐患，并根据风险分析的后果，对发现的安全漏洞和隐患在确保安全生产的情况下及时进行修补；或评估可能的影响后采取必要的补救措施，补救措施宜在系统维护期间开展；
- b) 测评对象：安全管理员、管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否采取必要的措施识别安全漏洞隐患，并根据风险分析的后果，对发现的安全漏洞和隐患在确保安全生产的情况下及时进行修补；
 - 2) 应核查是否有文档描述了存在的漏洞、严重级别、原因分析和改进意见等方面；
 - 3) 应核查是否有维护期间设备检修记录，查阅相关修补说明。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.5.1.2 测评单元（L3-MMS5-02）

该测评单元包括以下要求：

- a) 测评指标：应按照工业控制系统类别，建立控制设备漏洞台账或漏洞库，通过扫描机制或情报共享机制定期更新；通过漏洞台账或漏洞库，建立漏洞测试验证机制，定期对不影响生产环境的高危漏洞进行修补；对不能修复的漏洞，应建立补偿措施，弥补漏洞对工业控制系统带来的风险；
- b) 测评对象：安全管理员、控制设备、漏洞台账和漏洞库系统；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否建设了漏洞台账或漏洞库；
 - 2) 应核查漏洞台账或漏洞库内容是否更新；
 - 3) 应核查是否对漏洞有测试验证机制；
 - 4) 应核查是否对控制设备做过漏洞修复，提供相关变更文档；
 - 5) 应核查存在高危漏洞的控制设备是否采用了相关弥补措施。
- d) 单元判定：如果 1) -5) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.5.2 恶意代码防范管理

8.5.5.2.1 测评单元（L3-MMS5-03）

该测评单元包括以下要求：

- a) 测评指标：在更新恶意代码库、木马库以及规则库前，应首先在测试环境中测试通过，对隔离区域恶意代码更新应有专人负责，更新操作应离线进行，并保存更新记录；
- b) 测评对象：安全管理员、管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否在更新恶意代码库、木马库以及规则库前在实验环境进行测试，对隔离区域恶意代码更新是否有专人负责，更新操作是否离线进行，是否保存更新记录；
 - 2) 应核查恶意代码防范管理制度中是否对恶意代码库升级测试及更新等流程提出相关要求；

- 3) 应核查恶意代码库升级测试及更新记录是否与制度要求相符。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.5.5.2.2 测评单元 (L3-MMS5-04)

该测评单元包括以下要求：

- a) 测评指标：工业控制系统重要软硬件系统、设备及专用信息安全产品应采用符合国家及行业相关要求的产品及服务；
- b) 测评对象：安全管理员和检测报告类文档；
- c) 测评实施：应访谈安全管理员系统使用的工业控制系统重要软硬件系统、设备及专用信息安全产品是否为国家及行业监管部门认可的产品及服务；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

8.5.5.3 安全事件处置

8.5.5.3.1 测评单元 (L3-MMS5-05)

该测评单元包括以下要求：

- a) 测评指标：应建立工业控制系统联合防护和应急机制，负责处置跨单位工业控制系统安全事件；
- b) 测评对象：安全管理员、管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否建立跨单位处置工业控制系统安全事件流程；
 - 2) 应核查跨单位安全事件报告和处置管理制度，核查是否含有工业控制系统联合防护和应急的相关内容。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9 第四级测评要求

9.1 安全测评通用要求

9.1.1 物理和环境安全

9.1.1.1 物理位置选择

9.1.1.1.1 测评单元 (L4-PES1-01)

该测评单元包括以下要求：

- a) 测评指标：机房场地应选择在具有防震、防风和防雨等能力的建筑内；
- b) 测评对象：机房和相关文档；
- c) 测评实施包括以下内容：
 - 1) 应核查所在建筑物是否具有建筑物抗震设防审批文档；
 - 2) 应核查是否不存在雨水渗漏；
 - 3) 应核查门窗是否不存在因风导致的尘土严重；
 - 4) 应核查屋顶、墙体、门窗和地面等是否不存在破损开裂。

- d) 单元判定：如果 1)~4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.1.2 测评单元 (L4-PES1-02)

该测评单元包括以下要求：

- a) 测评指标：机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施；
- b) 测评对象：机房；
- c) 测评实施：应核查机房是否不位于所在建筑物的顶层或地下室，如果否，则核查机房是否采取了防水和防潮措施；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.1.2 物理访问控制

9.1.1.2.1 测评单元 (L4-PES1-03)

该测评单元包括以下要求：

- a) 测评指标：机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员；
- b) 测评对象：机房电子门禁系统；
- c) 测评实施包括以下内容：
 - 1) 应核查出入口是否配置电子门禁系统；
 - 2) 应核查电子门禁系统是否可以鉴别、记录进入的人员信息。
- d) 单元判定：如果 1)~2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.2.2 测评单元 (L4-PES1-04)

该测评单元包括以下要求：

- a) 测评指标：重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员；
- b) 测评对象：机房电子门禁系统；
- c) 测评实施包括以下内容：
 - 1) 应核查重要区域出入口是否配置第二道电子门禁系统；
 - 2) 应核查电子门禁系统是否可以鉴别、记录进入的人员信息。
- d) 单元判定：如果 1)~2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.3 防盗窃和防破坏

9.1.1.3.1 测评单元 (L4-PES1-05)

该测评单元包括以下要求：

- a) 测评指标：应将机房设备或主要部件进行固定，并设置明显的不易除去的标记；
- b) 测评对象：机房设备或主要部件；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内设备或主要部件是否固定；
 - 2) 应核查机房内设备或主要部件上是否设置了明显且不易除去的标记。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.3.2 测评单元 (L4-PES1-06)

该测评单元包括以下要求：

- a) 测评指标：应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
- b) 测评对象：机房通信线缆；
- c) 测评实施：应核查机房内通信线缆是否铺设在隐蔽处或桥架中；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.1.3.3 测评单元 (L4-PES1-07)

该测评单元包括以下要求：

- a) 测评指标：应设置机房防盗报警系统或设置有专人值守的视频监控系统；
- b) 测评对象：机房防盗报警系统或视频监控系统；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否配置防盗报警系统或有专人值守的视频监控系统；
 - 2) 应核查防盗报警系统或视频监控系统是否启用。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.4 防雷击

9.1.1.4.1 测评单元 (L4-PES1-08)

该测评单元包括以下要求：

- a) 测评指标：应将各类机柜、设施和设备等通过接地系统安全接地；
- b) 测评对象：机房；
- c) 测评实施：应核查机房内机柜、设施和设备等是否进行接地处理；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.1.4.2 测评单元 (L4-PES1-09)

该测评单元包括以下要求：

- a) 测评指标：应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等；
- b) 测评对象：机房防雷设施；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否设置防感应雷措施；
 - 2) 应核查防雷装置是否通过验收或国家有关部门的技术检测。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.5 防火

9.1.1.5.1 测评单元 (L4-PES1-10)

该测评单元包括以下要求：

- a) 测评指标：机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
- b) 测评对象：机房防火设施；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否设置火灾自动消防系统；
 - 2) 应核查火灾自动消防系统是否可以自动检测火情、自动报警并自动灭火。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.5.2 测评单元（L4-PES1-11）

该测评单元包括以下要求：

- a) 测评指标：机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
- b) 测评对象：机房验收类文档；
- c) 测评实施：应核查机房验收文档是否明确相关建筑材料的耐火等级；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.1.5.3 测评单元（L4-PES1-12）

该测评单元包括以下要求：

- a) 测评指标：应对机房划分区域进行管理，区域和区域之间设置隔离防火措施；
- b) 测评对象：机房管理员和机房；
- c) 测评实施包括以下内容：
 - 1) 应访谈机房管理员是否进行了区域划分；
 - 2) 应核查各区域间是否采取了防火措施进行隔离。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.6 防水和防潮

9.1.1.6.1 测评单元（L4-PES1-13）

该测评单元包括以下要求：

- a) 测评指标：应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- b) 测评对象：机房；
- c) 测评实施：应核查机房的窗户、屋顶和墙壁是否采取了防雨水渗透的措施；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.1.6.2 测评单元（L4-PES1-14）

该测评单元包括以下要求：

- a) 测评指标：应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
- b) 测评对象：机房；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否采取了防止水蒸气结露的措施；

- 2) 应核查机房内是否采取了排泄地下积水，防止地下积水渗透的措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.6.3 测评单元 (L4-PES1-15)

该测评单元包括以下要求：

- a) 测评指标：应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警；
- b) 测评对象：机房漏水检测设施；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否安装了对水敏感的检测装置；
 - 2) 应核查防水检测和报警装置是否启用。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.7 防静电

9.1.1.7.1 测评单元 (L4-PES1-16)

该测评单元包括以下要求：

- a) 测评指标：应安装防静电地板并采用必要的接地防静电措施；
- b) 测评对象：机房；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否安装了防静电地板；
 - 2) 应核查机房内是否采用了接地防静电措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.7.2 测评单元 (L4-PES1-17)

该测评单元包括以下要求：

- a) 测评指标：应采取防止静电的产生，例如采用静电消除器、佩戴防静电手环等；
- b) 测评对象：机房；
- c) 测评实施：应核查机房内是否配备了防静电设备；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.1.8 温湿度控制

9.1.1.8.1 测评单元 (L4-PES1-18)

该测评单元包括以下要求：

- a) 测评指标：应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内；
- b) 测评对象：机房温湿度调节设施；
- c) 测评实施包括以下内容：
 - 1) 应核查机房是否配备了专用空调；
 - 2) 应核查机房内温湿度是否在设备运行所允许的范围之内。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.9 电力供应

9.1.1.9.1 测评单元 (L4-PES1-19)

该测评单元包括以下要求：

- a) 测评指标：应在机房供电线路上配置稳压器和过电压防护设备；
- b) 测评对象：机房供电设施；
- c) 测评实施：应核查机房供电线路上是否配置了稳压器和过电压防护设备；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.1.9.2 测评单元 (L4-PES1-20)

该测评单元包括以下要求：

- a) 测评指标：应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；
- b) 测评对象：机房供电设施；
- c) 测评实施包括以下内容：
 - 1) 应核查是否配备 UPS 等后备电源系统；
 - 2) 应核查 UPS 等后备电源系统是否满足设备在断电情况下的正常运行要求。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.9.3 测评单元 (L4-PES1-21)

该测评单元包括以下要求：

- a) 测评指标：应设置冗余或并行的电力电缆线路为计算机系统供电；
- b) 测评对象：机房管理员和机房；
- c) 测评实施包括以下内容：
 - 1) 应访谈机房管理员机房供电是否来自两个不同的变电站；
 - 2) 应核查机房内是否设置了冗余或并行的电力电缆线路为计算机系统供电。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.9.4 测评单元 (L4-PES1-22)

该测评单元包括以下要求：

- a) 测评指标：应提供应急供电设施；
- b) 测评对象：机房应急供电设施；
- c) 测评实施包括以下内容：
 - 1) 应核查是否配置了应急供电设施；
 - 2) 应核查应急供电设施是否可用。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.1.10 电磁防护

9.1.1.10.1 测评单元（L4-PES1-23）

该测评单元包括以下要求：

- a) 测评指标：电源线和通信线缆应隔离铺设，避免互相干扰；
- b) 测评对象：机房线缆；
- c) 测评实施：应核查机房内电源线缆和通信线缆是否隔离铺设；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.1.10.2 测评单元（L4-PES1-24）

该测评单元包括以下要求：

- a) 测评指标：应对关键设备或关键区域实施电磁屏蔽；
- b) 测评对象：机房关键设备或区域；
- c) 测评实施包括以下内容：
 - 1) 应核查机房内是否划分了电磁屏蔽关键区域；
 - 2) 应核查机房内是否为关键设备配备了电磁屏蔽装置。
- d) 单元判定：如果 1) 或 2) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.2 网络和通信安全

9.1.2.1 网络架构

9.1.2.1.1 测评单元（L4-NCS1-01）

该测评单元包括以下要求：

- a) 测评指标：应保证网络设备的业务处理能力满足业务高峰期需要；
- b) 测评对象：路由器、交换机和防火墙等提供网络通信功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查业务高峰时期一段时间内主要网络设备的 CPU 使用率和内存使用率是否满足需要；
 - 2) 应核查网络设备是否从未出现过宕机情况。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.1.2 测评单元（L4-NCS1-02）

该测评单元包括以下要求：

- a) 测评指标：应保证网络各个部分的带宽满足业务高峰期需要；
- b) 测评对象：综合网管系统；
- c) 测评实施：应核查综合网管系统各通信链路带宽是否满足高峰时段的业务流量需要；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.2.1.3 测评单元（L4-NCS1-03）

该测评单元包括以下要求：

- a) 测评指标：应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

- b) 测评对象：路由器、交换机和防火墙等提供网络通信功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否依据某种原则划分不同的网络区域；
 - 2) 应核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.1.4 测评单元（L4-NCS1-04）

该测评单元包括以下要求：

- a) 测评指标：应避免将重要网络区域部署在网络边界处且没有边界防护措施；
- b) 测评对象：网络管理员和网络拓扑图；
- c) 测评实施包括以下内容：
 - 1) 应核查网络拓扑图是否与实际网络运行环境一致；
 - 2) 应核查重要网络区域未部署在网络边界处且无边界防护措施；
 - 3) 应核查重要网络区域与其他网络区域之间是否采取可靠的技术隔离手段，如网闸、防火墙和设备访问控制列表（ACL）等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.1.5 测评单元（L4-NCS1-05）

该测评单元包括以下要求：

- a) 测评指标：应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性；
- b) 测评对象：网络管理员和网络拓扑图；
- c) 测评实施：应核查系统是否有主要网络设备、安全设备的硬件冗余和通信线路冗余；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.2.1.6 测评单元（L4-NCS1-06）

该测评单元包括以下要求：

- a) 测评指标：应可按照业务服务的重要程度分配带宽，优先保障重要业务；
- b) 测评对象：路由器、交换机和流量控制设备等提供带宽控制功能的设备；
- c) 测评实施：应核查带宽控制设备是否按照业务服务的重要程度配置并启用了带宽策略；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.2.2 通信传输

9.1.2.2.1 测评单元（L4-NCS1-07）

该测评单元包括以下要求：

- a) 测评指标：应采用密码技术保证通信过程中数据的完整性；
- b) 测评对象：提供密码技术功能的设备或组件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否在数据传输过程中使用密码技术来保证其完整性；

2) 应测试验证密码技术设备或组件是否保证通信过程中数据的完整性。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.2.2 测评单元 (L4-NCS1-08)

该测评单元包括以下要求：

- a) 测评指标：应采用密码技术保证通信过程中敏感信息字段或整个报文的保密性；
- b) 测评对象：提供密码技术功能的设备或组件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否在通信过程中采取保密措施，具体采用哪些技术措施；
 - 2) 应测试验证在通信过程中是否对敏感信息字段或整个报文进行加密。
- d) 单元判定：如果 1) -2) 为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.2.3 测评单元 (L4-NCS1-09)

该测评单元包括以下要求：

- a) 测评指标：应在通信前基于密码技术对通信的双方进行验证或认证；
- b) 测评对象：提供密码技术功能的设备或组件；
- c) 测评实施：应核查是否能在通信双方建立连接之前利用密码技术进行会话初始化验证或认证；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.2.2.4 测评单元 (L4-NCS1-10)

该测评单元包括以下要求：

- a) 测评指标：应基于密码模块对重要通信过程进行密码运算和密钥管理；
- b) 测评对象：提供密码技术功能的设备或组件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否基于密码模块产生密钥并进行密码运算；
 - 2) 应核查相关证书或证明材料，确认采用的密码算法是否符合国家有关部门的要求。
- d) 单元判定：如果 1) -2) 为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.3 边界防护

9.1.2.3.1 测评单元 (L4-NCS1-11)

该测评单元包括以下要求：

- a) 测评指标：应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查在网络边界处是否部署访问控制设备；
 - 2) 应核查设备配置信息是否指定端口进行跨越边界的网络通信，该端口配置并启用了安全策略；

- 3) 应采用其他技术手段（如非法无线网络设备定位检查、核查设备配置信息等）核查是否不存在其他未受控端口进行跨越边界的网络通信。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.3.2 测评单元（L4-NCS1-12）

该测评单元包括以下要求：

- a) 测评指标：应能够对非授权设备私自联到内部网络的行为进行限制或检查，并对其进行有效阻断；
- b) 测评对象：终端管理系统和网络设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否采用技术措施防止非授权设备接入内部网络，并进行有效阻断；
 - 2) 应核查所有路由器和交换机等相关设备闲置端口是否均已关闭。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.3.3 测评单元（L4-NCS1-13）

该测评单元包括以下要求：

- a) 测评指标：应能够对内部用户非授权联到外部网络的行为进行限制或检查，并对其进行有效阻断；
- b) 测评对象：终端管理系统或设备；
- c) 测评实施：应核查是否采用技术措施防止内部用户非法外联行为；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.2.3.4 测评单元（L4-NCS1-14）

该测评单元包括以下要求：

- a) 测评指标：应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络；
- b) 测评对象：网络拓扑图和无线网络设备；
- c) 测评实施包括以下内容：
 - 1) 应核查无线网络的部署方式，是否单独组网后再连接到有线网络；
 - 2) 应核查无线网络是否通过受控的边界防护设备接入到内部有线网络。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.3.5 测评单元（L4-NCS1-15）

该测评单元包括以下要求：

- a) 测评指标：应采用可信验证机制对接入到网络中的设备进行可信验证，确保接入网络的设备真实可信；
- b) 测评对象：终端管理系统或设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否采用可信验证机制对接入到网络中的设备进行可信验证；
 - 2) 应测试验证是否能够对连接到内部网络的设备进行可信验证。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.4 访问控制

9.1.2.4.1 测评单元 (L4-NCS1-16)

该测评单元包括以下要求：

- a) 测评指标：应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查在网络边界或区域之间是否部署访问控制设备，是否启用访问控制策略；
 - 2) 应核查设备的最后一条访问控制策略是否为禁止所有网络通信。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.4.2 测评单元 (L4-NCS1-17)

该测评单元包括以下要求：

- a) 测评指标：应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否不存在多余或无效的访问控制策略；
 - 2) 应核查设备的不同访问控制策略之间的逻辑关系及前后排列顺序是否合理。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.4.3 测评单元 (L4-NCS1-18)

该测评单元包括以下要求：

- a) 测评指标：应不允许数据带通用协议通过；
- b) 测评对象：网闸等提供网络协议转换功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查设备是否采取协议转换或其他相应的控制措施来实现禁止数据带通用协议通过；
 - 2) 应通过发送带通用协议的数据等测试方式，测试验证设备是否能够有效阻断。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.5 入侵防范

9.1.2.5.1 测评单元 (L4-NCS1-19)

该测评单元包括以下要求：

- a) 测评指标：应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
- b) 测评对象：抗 APT 攻击系统、网络回溯系统、抗 DDoS 攻击系统和入侵保护系统；
- c) 测评实施包括以下内容：

- 1) 应核查相关系统或设备是否能够检测从外部发起的网络攻击行为;
 - 2) 应核查相关系统或设备的规则库版本是否已经更新到最新版本;
 - 3) 应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点。
 - 4) 应测试相关系统或设备, 测试验证其安全策略是否有效。
- d) 单元判定: 如果 1) -4) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

9.1.2.5.2 测评单元 (L4-NCS1-20)

该测评单元包括以下要求:

- a) 测评指标: 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为;
- b) 测评对象: 抗 APT 攻击系统、网络回溯系统、抗 DDoS 攻击系统和入侵保护系统;
- c) 测评实施包括以下内容:
 - 1) 应核查相关系统或设备是否能够检测到从内部发起的网络攻击行为;
 - 2) 应核查相关系统或设备的规则库版本是否已经更新到最新版本;
 - 3) 应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点;
 - 4) 应测试相关系统或设备, 测试验证其安全策略是否有效。
- d) 单元判定: 如果 1) -4) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

9.1.2.5.3 测评单元 (L4-NCS1-21)

该测评单元包括以下要求:

- a) 测评指标: 应采取技术措施对网络行为进行分析, 实现对网络攻击特别是新型网络攻击行为的分析;
- b) 测评对象: 抗 APT 攻击系统和网络回溯系统;
- c) 测评实施包括以下内容:
 - 1) 应核查是否部署网络回溯系统或抗 APT 攻击系统对新型网络攻击进行检测和分析;
 - 2) 应测试验证是否对网络行为进行分析, 实现对网络攻击特别是未知的新型网络攻击的检测和分析。
- d) 单元判定: 如果 1) - 2) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

9.1.2.5.4 测评单元 (L4-NCS1-22)

该测评单元包括以下要求:

- a) 测评指标: 当检测到攻击行为时, 记录攻击源 IP、攻击类型、攻击目的、攻击时间, 在发生严重入侵事件时应提供报警;
- b) 测评对象: 抗 APT 攻击系统、网络回溯系统、抗 DDoS 攻击系统和入侵保护系统;
- c) 测评实施包括以下内容:
 - 1) 应核查相关系统或设备的记录是否包括入侵源 IP、攻击类型、攻击目的、攻击时间等相关内容;
 - 2) 应测试验证相关系统或设备报警策略是否有效。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

9.1.2.6 恶意代码防范

9.1.2.6.1 测评单元（L4-NCS1-23）

该测评单元包括以下要求：

- a) 测评指标：应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；
- b) 测评对象：防病毒网关和 UTM 等提供防恶意代码功能的设备或系统；
- c) 测评实施包括以下内容：
 - 1) 应核查在关键网络节点处是否有防恶意代码技术措施；
 - 2) 应核查防恶意代码产品运行是否正常，恶意代码库是否已经更新到最新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.6.2 测评单元（L4-NCS1-24）

该测评单元包括以下要求：

- a) 测评指标：应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新；
- b) 测评对象：反垃圾邮件网关提供防垃圾邮件功能的设备或系统；
- c) 测评实施包括以下内容：
 - 1) 应核查在关键网络节点处是否部署了防垃圾邮件设备或系统；
 - 2) 应核查防垃圾邮件产品运行是否正常，防垃圾邮件规则库是否已经更新到最新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.7 安全审计

9.1.2.7.1 测评单元（L4-NCS1-25）

该测评单元包括以下要求：

- a) 测评指标：应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
- b) 测评对象：综合安全审计系统、路由器、交换机和防火墙等设备；
- c) 测评实施包括以下内容：
 - 1) 应核查设备是否开启了日志记录或安全审计功能；
 - 2) 应核查是否部署了综合安全审计系统或类似功能的系统平台；
 - 3) 应核查安全审计范围是否覆盖到每个用户；
 - 4) 应核查是否对重要的用户行为和重要安全事件进行了审计。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.7.2 测评单元（L4-NCS1-26）

该测评单元包括以下要求：

- a) 测评指标：审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

- b) 测评对象：综合安全审计系统、路由器、交换机和防火墙等设备；
- c) 测评实施：应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.7.3 测评单元（L4-NCS1-27）

该测评单元包括以下要求：

- a) 测评指标：应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
- b) 测评对象：综合安全审计系统、路由器、交换机和防火墙等设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否采取了技术措施能够对审计记录进行保护；
 - 2) 应核查审计记录的备份机制和备份策略是否合理。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.7.4 测评单元（L4-NCS1-28）

该测评单元包括以下要求：

- a) 测评指标：应确保审计记录的留存时间符合法律法规要求；
- b) 测评对象：综合安全审计系统、路由器、交换机和防火墙等设备；
- c) 测评实施：应核查审计记录的留存时间是否至少为 6 个月；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.2.7.5 测评单元（L4-NCS1-29）

该测评单元包括以下要求：

- a) 测评指标：审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性；
- b) 测评对象：综合安全审计系统、路由器、交换机和防火墙等设备；
- c) 测评实施：应核查是否在系统范围内统一使用了唯一确定的时钟源，以确保审计分析的正确性；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.8 集中管控

9.1.2.8.1 测评单元（L4-NCS1-30）

该测评单元包括以下要求：

- a) 测评指标：应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
- b) 测评对象：网络拓扑图；
- c) 测评实施包括以下内容：
 - 1) 应核查是否划分出单独的网络区域用于部署安全管理系统；
 - 2) 应核查各个安全管理系统是否集中部署在单独的网络区域内。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.8.2 测评单元 (L4-NCS1-31)

该测评单元包括以下要求：

- a) 测评指标：应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
- b) 测评对象：路由器、交换机和防火墙等设备；
- c) 测评实施包括以下内容：
 - 1) 应核查网络中是否划分单独的管理 VLAN 用于对安全设备或安全组件进行管理；
 - 2) 应核查网络是否使用独立的带外管理网络对安全设备或安全组件进行管理。
- d) 单元判定：如果 1) -2) 其中之一为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.2.8.3 测评单元 (L4-NCS1-32)

该测评单元包括以下要求：

- a) 测评指标：应对网络链路、安全设备、网络设备和服务器等运行状况进行集中监测；
- b) 测评对象：综合网管系统等提供运行状态监测功能的系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否部署了具备运行状态监测功能的系统或设备，能够对网络链路、安全设备、网络设备和服务器等运行状况进行集中监测；
 - 2) 应测试验证运行状态监测系统是否根据网络链路、安全设备、网络设备和服务器等的工作状态、依据设定的阈值（或默认阈值）实时报警。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.8.4 测评单元 (L4-NCS1-33)

该测评单元包括以下要求：

- a) 测评指标：应对分散在各个设备上的审计数据进行收集汇总和集中分析；
- b) 测评对象：综合安全审计系统、数据库审计系统等提供集中审计功能的系统；
- c) 测评实施包括以下内容：
 - 1) 应核查各个设备是否配置并启用了相关策略，将审计数据发送到独立于设备自身的外部相关系统平台中；
 - 2) 应核查是否部署统一的集中安全审计平台，统一收集和存储各设备日志，并根据需要进行集中审计分析。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.8.5 测评单元 (L4-NCS1-34)

该测评单元包括以下要求：

- a) 测评指标：应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
- b) 测评对象：提供集中安全管控功能的系统；
- c) 测评实施包括以下内容：

- 1) 应核查是否能够对安全策略（如防火墙访问控制策略、入侵保护系统防护策略、WAF 安全防护策略等）进行集中管理；
 - 2) 应核查是否实现对操作系统防恶意代码系统及网络恶意代码防护设备的集中管理，实现防恶意代码病毒规则库的升级进行集中管理；
 - 3) 应核查是否能够实现对各设备的补丁升级进行集中管理。
- d) 单元判定：如果 1)～3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.2.8.6 测评单元（L4-NCS1-35）

该测评单元包括以下要求：

- a) 测评指标：应能对网络中发生的各类安全事件进行识别、报警和分析；
 - b) 测评对象：提供集中安全管控功能的系统；
 - c) 测评实施包括以下内容：
 - 1) 应核查是否部署了相关系统平台能够对各类安全事件进行分析并通过声光等方式实时报警；
 - 2) 应核查安全事件的监测范围是否能够覆盖网络所有关键路径。
- d) 单元判定：如果 1)～2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3 设备和计算安全

9.1.3.1 身份鉴别

9.1.3.1.1 测评单元（L4-ECS1-01）

该测评单元包括以下要求：

- a) 测评指标：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
 - b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
 - c) 测评实施包括以下内容：
 - 1) 应核查用户在登录时是否采用了身份鉴别措施；
 - 2) 应核查用户列表，核查用户身份标识是否具有唯一性；
 - 3) 应核查用户配置信息或访谈系统管理员，核查是否存在空口令用户；
 - 4) 应核查用户鉴别信息是否具有复杂度要求并定期更换。
- d) 单元判定：如果 1)～4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.1.2 测评单元（L4-ECS1-02）

该测评单元包括以下要求：

- a) 测评指标：应具有登录失败处理功能，配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：

- 1) 应核查是否配置并启用了登录失败处理功能;
- 2) 应核查是否配置并启用了限制非法登录达到一定次数后实现账户锁定功能;
- 3) 应核查是否配置并启用了远程登录连接超时并自动退出功能。
- d) 单元判定: 如果 1) -3) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

9.1.3.1.3 测评单元 (L4-ECS1-03)

该测评单元包括以下要求:

- a) 测评指标: 当进行远程管理时, 应采取必要措施, 防止鉴别信息在网络传输过程中被窃听;
- b) 测评对象: 终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备;
- c) 测评实施: 应核查是否采用加密等安全方式对系统进行远程管理, 防止鉴别信息在网络传输过程中被窃听;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

9.1.3.1.4 测评单元 (L4-ECS1-04)

该测评单元包括以下要求:

- a) 测评指标: 应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别, 且其中一种鉴别技术至少应使用密码技术或生物技术来实现;
- b) 测评对象: 终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备;
- c) 测评实施: 应核查系统是否采用两种或两种以上组合的鉴别技术对用户身份进行鉴别, 其中一种鉴别技术至少应使用密码技术或生物技术来实现;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

9.1.3.2 访问控制

9.1.3.2.1 测评单元 (L4-ECS1-05)

该测评单元包括以下要求:

- a) 测评指标: 应对登录的用户分配账户和权限;
- b) 测评对象: 终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备;
- c) 测评实施包括以下内容:
 - 1) 应测试网络管理员、安全管理员、系统管理员或核查用户账户和权限设置情况;
 - 2) 应核查是否已禁用或限制匿名、默认账户的访问权限。
- d) 单元判定: 如果 1) -2) 为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

9.1.3.2.2 测评单元 (L4-ECS1-06)

该测评单元包括以下要求:

- a) 测评指标: 应重命名或删除默认账户, 修改默认账户的默认口令;

- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否已经重命名默认账户或默认账户已被删除；
 - 2) 应核查是否已修改默认账户的默认口令。
- d) 单元判定：如果 1) 或 2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.2.3 测评单元（L4-ECS1-07）

该测评单元包括以下要求：

- a) 测评指标：应及时删除或停用多余的、过期的账户，避免共享账户的存在；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否不存在多余或过期账户；
 - 2) 应访谈网络管理员、安全管理员、系统管理员不同用户是否采用不同账户登录系统。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.2.4 测评单元（L4-ECS1-08）

该测评单元包括以下要求：

- a) 测评指标：应进行角色划分，授予管理用户所需的最小权限，实现管理用户的权限分离；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否进行角色划分；
 - 2) 应核查访问控制策略，查看管理用户的权限是否已进行分离；
 - 3) 应核查管理用户权限是否为其工作任务所需的最小权限。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.2.5 测评单元（L4-ECS1-09）

该测评单元包括以下要求：

- a) 测评指标：应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否有管理用户负责配置访问控制策略；
 - 2) 应核查授权主体是否依据安全策略配置了主体对客体的访问规则；
 - 3) 应测试用户是否有可越权访问情形。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.2.6 测评单元（L4-ECS1-10）

该测评单元包括以下要求：

- a) 测评指标：访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施：应核查访问控制策略的控制粒度是否达到主体为用户级或进程级，客体为文件、数据库表、记录或字段级；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.3.2.7 测评单元（L4-ECS1-11）

该测评单元包括以下要求：

- a) 测评指标：应对所有主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否依据安全策略对所有主体、客体设置了安全标记机制；
 - 2) 应测试是否依据主体、客体安全标记控制主体对客体访问的强制访问控制策略。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.3 安全审计

9.1.3.3.1 测评单元（L4-ECS1-12）

该测评单元包括以下要求：

- a) 测评指标：应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否开启了安全审计功能；
 - 2) 应核查安全审计范围是否覆盖到每个用户；
 - 3) 应核查是否对重要的用户行为和重要安全事件进行审计。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.3.2 测评单元（L4-ECS1-13）

该测评单元包括以下要求：

- a) 测评指标：审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应核查审计记录信息是否包括事件的日期和时间、主体标识、客体标识、事件类型、事件是否成功及其他与审计相关的信息；

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.3.3.3 测评单元（L4-ECS1-14）

该测评单元包括以下要求：

- a) 测评指标：应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否采取了保护措施对审计记录进行保护；
 - 2) 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.3.3.4 测评单元（L4-ECS1-15）

该测评单元包括以下要求：

- a) 测评指标：应确保审计记录的留存时间符合法律法规要求；
- b) 测评对象：综合安全审计系统、终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应核查审计记录的留存时间是否至少为 6 个月；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.3.3.5 测评单元（L4-ECS1-16）

该测评单元包括以下要求：

- a) 测评指标：应对审计进程进行保护，防止未经授权的中断；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应测试通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.3.3.6 测评单元（L4-ECS1-17）

该测评单元包括以下要求：

- a) 测评指标：审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应核查是否统一使用系统范围内唯一确定的时钟源，以确保审计分析的正确性。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.3.4 入侵防范

9.1.3.4.1 测评单元（L4-ECS1-18）

该测评单元包括以下要求：

- a) 测评指标：应遵循最小安装的原则，仅安装需要的组件和应用程序；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否遵循最小安装原则；
 - 2) 应确认是否已经关闭非必要的组件和应用程序。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.4.2 测评单元（L4-ECS1-19）

该测评单元包括以下要求：

- a) 测评指标：应关闭不需要的系统服务、默认共享和高危端口；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否定期对系统服务进行梳理，关闭了非必要的系统服务和默认共享；
 - 2) 应核查是否不存在非必要的高危端口。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.4.3 测评单元（L4-ECS1-20）

该测评单元包括以下要求：

- a) 测评指标：应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施：应核查配置文件是否对终端接入范围进行限制；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.3.4.4 测评单元（L4-ECS1-21）

该测评单元包括以下要求：

- a) 测评指标：应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应进行漏洞扫描，核查是否不存在高风险漏洞；
 - 2) 应访谈系统管理员，核查是否在经过充分测试评估后及时修补漏洞。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.4.5 测评单元（L4-ECS1-22）

该测评单元包括以下要求：

- a) 测评指标：应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应访谈并核查是否有入侵检测的措施；
 - 2) 应核查在发生严重入侵事件时是否提供报警。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.5 恶意代码防范

9.1.3.5.1 测评单元 (L4-ECS1-23)

该测评单元包括以下要求：

- a) 测评指标：应采用基准库比对或其他可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证，并在检测到其完整性受到破坏时采取恢复措施；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否采用基准库比对或其他可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证；
 - 2) 应核查是否有保护重要系统程序或文件完整性的措施；
 - 3) 当检测到程序或文件受到破坏后，核查是否具备恢复的措施。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.6 资源控制

9.1.3.6.1 测评单元 (L4-ECS1-24)

该测评单元包括以下要求：

- a) 测评指标：应限制单个用户或进程对系统资源的最大使用限度
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否存在系统资源控制的措施，如核查配置参数是否设置最大进程数；
 - 2) 应引用产品（应用）测试结果或核查数据库表空间，确认目前系统资源利用率是否在允许范围之内或目前总体数据库表空间占用率是否不超过阈值；
 - 3) 应核查是否存在对数据库资源过大或最小的用户的限制措施。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.6.2 测评单元 (L4-ECS1-25)

该测评单元包括以下要求：

- a) 测评指标：应提供重要节点设备的硬件冗余，保证系统的可用性；
- b) 测评对象：终端和服务器等设备；
- c) 测评实施：核查重要节点设备是否有硬件冗余；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.3.6.3 测评单元 (L4-ECS1-26)

该测评单元包括以下要求：

- a) 测评指标：应对重要节点进行监视，包括监视 CPU、硬盘、内存等资源的使用情况；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；

- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否有保证上述安全功能的措施（包括通过第三方工具或增强功能实现）；
 - 2) 应核查是否对重要节点的系统 CPU、硬盘、内存、磁盘容量、网络服务等进行监视。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.3.6.4 测评单元（L4-ECS1-27）

该测评单元包括以下要求：

- a) 测评指标：应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否有保证上述安全功能的措施（包括通过第三方工具或增强功能实现）；
 - 2) 应核查重要节点的服务水平降低到预设的最小值时是否进行报警。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4 应用和数据安全

9.1.4.1 身份鉴别

9.1.4.1.1 测评单元（L4-ADS1-01）

该测评单元包括以下要求：

- a) 测评指标：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查用户在登录时是否采用了身份鉴别措施；
 - 2) 应测试身份鉴别措施是否能够不被绕过；
 - 3) 应测试用户登录时是否使用唯一性身份标识；
 - 4) 应核查鉴别信息是否具有复杂度要求并定期更换；
 - 5) 应测试应用系统是否不存在空口令用户。
- d) 单元判定：如果 1) -5) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.1.2 测评单元（L4-ADS1-02）

该测评单元包括以下要求：

- a) 测评指标：应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否提供并启用登录失败处理功能；
 - 2) 应核查登录失败反馈信息是否进行模糊处理；
 - 3) 应测试用户连续多次登录失败时应用系统是否采取必要的保护措施。

- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.1.3 测评单元 (L4-ADS1-03)

该测评单元包括以下要求：

- a) 测评指标：应强制用户首次登录时修改初始口令；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应测试用户首次登录时是否被强制修改初始口令；
 - 2) 应测试用户强制修改后的口令是否满足鉴别信息复杂度要求。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.1.4 测评单元 (L4-ADS1-04)

该测评单元包括以下要求：

- a) 测评指标：用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查用户身份鉴别信息丢失时，是否采用鉴别信息重置或其他技术措施保证安全；
 - 2) 应核查用户身份鉴别信息失效时，是否采用鉴别信息重置或其他技术措施保证安全。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.1.5 测评单元 (L4-ADS1-05)

该测评单元包括以下要求：

- a) 测评指标：应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术或生物技术来实现；
- b) 测评对象：业务应用系统；
- c) 测评实施：应核查系统是否采用两种或两种以上组合的鉴别技术对用户身份进行鉴别，其中一种鉴别技术至少应使用密码技术或生物技术来实现；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.4.1.6 测评单元 (L4-ADS1-06)

该测评单元包括以下要求：

- a) 测评指标：登录用户执行重要操作时应再次进行身份鉴别；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否提供用户执行重要操作时再次身份鉴别的机制；
 - 2) 应测试用户执行重要操作时应用系统是否再次进行身份鉴别。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.2 访问控制

9.1.4.2.1 测评单元（L4-ADS1-07）

该测评单元包括以下要求：

- a) 测评指标：应提供访问控制功能，对登录的用户分配账户和权限；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否提供访问控制功能；
 - 2) 应核查是否有管理用户负责对系统用户进行账户分配和权限管理；
 - 3) 应测试账户分配和权限管理功能是否有效；
 - 4) 应测试不同角色用户是否具有系统规定的权限。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.2.2 测评单元（L4-ADS1-08）

该测评单元包括以下要求：

- a) 测评指标：应重命名或删除默认账户，修改默认账户的默认口令；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否已经重命名默认账户或默认账户已被删除；
 - 2) 应核查并测试是否已修改默认账户的默认口令。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.2.3 测评单元（L4-ADS1-09）

该测评单元包括以下要求：

- a) 测评指标：应及时删除或停用多余的、过期的账户，避免共享账户的存在；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应访谈应用系统管理员用户与账户之间是否一一对应；
 - 2) 应核查并测试多余的、过期的账户是否被删除或停用。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.2.4 测评单元（L4-ADS1-10）

该测评单元包括以下要求：

- a) 测评指标：应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查并测试不同岗位用户是否仅拥有其工作任务所需的最小权限；
 - 2) 应核查并测试业务岗位与管理岗位用户操作权限相互之间是否相互制约；
 - 3) 应核查并测试关键业务岗位用户操作权限相互之间是否相互制约；

- 4) 应核查并测试关键管理岗位用户操作权限相互之间是否相互制约。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.2.5 测评单元（L4-ADS1-11）

该测评单元包括以下要求：

- a) 测评指标：应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否由授权主体负责配置访问控制策略；
 - 2) 应核查授权主体是否依据安全策略配置了主体对客体的访问规则；
 - 3) 应测试非授权主体是否不能配置访问控制策略；
 - 4) 应测试是否不存在可越权访问情形。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.2.6 测评单元（L4-ADS1-12）

该测评单元包括以下要求：

- a) 测评指标：访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级；
- b) 测评对象：业务应用系统；
- c) 测评实施：应核查并测试访问控制策略的控制粒度是否达到主体为用户级，客体为文件、数据库表、记录或字段级；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.4.2.7 测评单元（L4-ADS1-13）

该测评单元包括以下要求：

- a) 测评指标：应对所有主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否依据安全策略对所有主体和客体设置了安全标记；
 - 2) 应测试是否依据安全标记和强制访问控制规则确定主体对客体的访问。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.3 安全审计

9.1.4.3.1 测评单元（L4-ADS1-14）

该测评单元包括以下要求：

- a) 测评指标：应提供并启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
- b) 测评对象：业务应用系统；

- c) 测评实施包括以下内容：
 - 1) 应核查是否提供并启用了安全审计功能；
 - 2) 应核查审计范围是否覆盖到每个用户；
 - 3) 应核查并测试是否对重要的用户行为和重要安全事件进行审计。
- d) 单元判定：如果 1)–3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.3.2 测评单元（L4-ADS1-15）

该测评单元包括以下要求：

- a) 测评指标：审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
- b) 测评对象：业务应用系统；
- c) 测评实施：应核查并测试审计记录信息是否包括事件的日期、时间、类型、主体标识、客体标识和结果等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.3.3 测评单元（L4-ADS1-16）

该测评单元包括以下要求：

- a) 测评指标：应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
- b) 测评对象：业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查是否采取了保护措施对审计记录进行保护；
 - 2) 应核查审计记录的备份机制及备份策略是否有效。
- d) 单元判定：如果 1)–2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.3.4 测评单元（L4-ADS1-17）

该测评单元包括以下要求：

- a) 测评指标：应确保审计记录的留存时间符合法律法规要求；
- b) 测评对象：综合安全审计系统和业务应用系统；
- c) 测评实施：应核查审计记录的留存时间是否至少为 6 个月；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.4.3.5 测评单元（L4-ADS1-18）

该测评单元包括以下要求：

- a) 测评指标：应对审计进程进行保护，防止未经授权的中断；
- b) 测评对象：业务应用系统；
- c) 测评实施：应测试应用系统，可试图通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.3.6 测评单元（L4-ADS1-19）

该测评单元包括以下要求：

- a) 测评指标：审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性；
- b) 测评对象：业务应用系统；
- c) 测评实施：应核查是否在系统范围内统一使用了唯一确定的时钟源，以确保审计分析的正确性；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.4.4 软件容错

9.1.4.4.1 测评单元（L4-ADS1-20）

该测评单元包括以下要求：

- a) 测评指标：应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
- b) 测评对象：业务应用系统和系统设计文档等；
- c) 测评实施包括以下内容：
 - 1) 应核查系统设计文档的内容是否包括数据有效性检验功能的内容或模块；
 - 2) 应测试是否对人机接口或通信接口输入的内容进行有效性检验。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.4.2 测评单元（L4-ADS1-21）

该测评单元包括以下要求：

- a) 测评指标：在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施；
- b) 测评对象：系统设计文档和维护文档等；
- c) 测评实施包括以下内容：
 - 1) 应核查应用系统设计文档和维护文档，应用系统有故障发生时是否能继续提供一部分功能；
 - 2) 应核查应用系统设计文档和维护文档，应用系统有故障发生后，是否能够实施必要的措施使系统恢复功能。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.4.3 测评单元（L4-ADS1-22）

该测评单元包括以下要求：

- a) 测评指标：在故障发生时，应自动保存易失性数据和所有状态，保证系统能够进行恢复；
- b) 测评对象：系统设计文档和维护文档等；
- c) 测评实施包括以下内容：
 - 1) 应核查应用系统设计文档和维护文档，当故障发生时应用系统是否能自动保存易失性数据和当前所有状态；
 - 2) 应核查应用系统设计文档和维护文档，应用系统发生故障后能够恢复故障时的状态。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.5 资源控制

9.1.4.5.1 测评单元（L4-ADS1-23）

该测评单元包括以下要求：

- a) 测评指标：当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；
- b) 测评对象：业务应用系统；
- c) 测评实施：应测试应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.5.2 测评单元（L4-ADS1-24）

该测评单元包括以下要求：

- a) 测评指标：应能够对系统的最大并发会话连接数进行限制；
- b) 测评对象：业务应用系统或中间件等；
- c) 测评实施包括以下内容：
 - 1) 应核查应用系统配置信息是否对最大并发会话连接数进行限制；
 - 2) 应核查中间件配置信息是否对最大并发会话连接数进行限制。
- d) 单元判定：如果 1) 或 2) 为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.5.3 测评单元（L4-ADS1-25）

该测评单元包括以下要求：

- a) 测评指标：应能够对单个账户的多重并发会话进行限制；
- b) 测评对象：业务应用系统；
- c) 测评实施：应测试是否能够正确地限制单个账户的多重并发会话数；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.4.6 数据完整性

9.1.4.6.1 测评单元（L4-ADS1-26）

该测评单元包括以下要求：

- a) 测评指标：应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
- b) 测评对象：系统设计文档和业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查系统设计文档，鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了密码技术保证完整性；
 - 2) 应测试在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.6.2 测评单元 (L4-ADS1-27)

该测评单元包括以下要求：

- a) 测评指标：应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
- b) 测评对象：系统设计文档、业务应用系统和数据安全保护系统，终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备中的重要配置数据；
- c) 测评实施包括以下内容：
 - 1) 应核查设计文档，是否采用了密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；
 - 2) 应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；
 - 3) 应测试在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.6.3 测评单元 (L4-ADS1-28)

该测评单元包括以下要求：

- a) 测评指标：在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖；
- b) 测评对象：系统设计文档、业务应用系统和数据安全保护系统，终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备中的重要配置数据；
- c) 测评实施包括以下内容：
 - 1) 应核查设计文档，是否采用了密码技术保证数据发送和数据接收操作的不可抵赖性；
 - 2) 应核查数据安全保护系统是否能够保证数据发送和数据接收操作的不可抵赖性；
 - 3) 应测试是否能够检测到数据在传输过程中不能被篡改。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.7 数据保密性

9.1.4.7.1 测评单元 (L4-ADS1-29)

该测评单元包括以下要求：

- a) 测评指标：应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
- b) 测评对象：系统设计文档和业务应用系统；
- c) 测评实施包括以下内容：
 - 1) 应核查系统设计文档，重鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性；

- 2) 应通过嗅探等方式抓取传输过程中的数据包,查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。
- d) 单元判定:如果1)~2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.1.4.7.2 测评单元 (L4-ADS1-30)

该测评单元包括以下要求:

- a) 测评指标:应采用密码技术保证重要数据在存储过程中的保密性,包括但不限于鉴别数据、重要业务数据和重要个人信息等;
- b) 测评对象:系统设计文档、业务应用系统和数据安全保护系统,终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备中的重要配置数据;
- c) 测评实施包括以下内容:
 - 1) 应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性;
 - 2) 应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性。
- d) 单元判定:如果1)~2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.1.4.8 数据备份恢复

9.1.4.8.1 测评单元 (L4-ADS1-31)

该测评单元包括以下要求:

- a) 测评指标:应提供重要数据的本地数据备份与恢复功能;
- b) 测评对象:配置数据和业务数据;
- c) 测评实施包括以下内容:
 - 1) 应核查是否按照备份策略进行本地备份;
 - 2) 应核查备份策略设置是否合理、配置是否正确;
 - 3) 应核查备份结果是否与备份策略一致;
 - 4) 应核查近期恢复测试记录,查看是否能够进行正常的数据恢复。
- d) 单元判定:如果1)~4)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.1.4.8.2 测评单元 (L4-ADS1-32)

该测评单元包括以下要求:

- a) 测评指标:应提供异地实时备份功能,利用通信网络将重要数据实时备份至备份场地;
- b) 测评对象:配置数据和业务数据;
- c) 测评实施:应核查是否提供异地实时备份功能,并通过网络将重要配置数据、重要业务数据实时备份至备份场地;
- d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

9.1.4.8.3 测评单元 (L4-ADS1-33)

该测评单元包括以下要求：

- a) 测评指标：应提供重要数据处理系统的热冗余，保证系统的高可用性；
- b) 测评对象：重要数据处理系统；
- c) 测评实施：应核查重要数据处理系统（包括边界交换机、边界防火墙、核心路由器、应用服务器和数据库服务器等）是否采用热冗余方式部署；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.4.8.4 测评单元（L4-ADS1-34）

该测评单元包括以下要求：

- a) 测评指标：应建立异地灾难备份中心，提供业务应用的实时切换；
- b) 测评对象：灾难备份中心及相关组件；
- c) 测评实施包括以下内容：
 - 1) 应核查是否建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备；
 - 2) 应核查是否提供业务应用的实时切换功能。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.9 剩余信息保护

9.1.4.9.1 测评单元（L4-ADS1-35）

该测评单元包括以下要求：

- a) 测评指标：应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及业务应用系统；
- c) 测评实施：应核查相关配置信息或访谈应用系统管理员，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.9.2 测评单元（L4-ADS1-36）

该测评单元包括以下要求：

- a) 测评指标：应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除；
- b) 测评对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及业务应用系统；
- c) 测评实施：应核查相关配置信息或访谈应用系统管理员，敏感数据所在的存储空间被释放或重新分配给其他用户前是否得到完全清除；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.10 个人信息保护

9.1.4.10.1 测评单元（L4-ADS1-37）

该测评单元包括以下要求：

- a) 测评指标：应仅采集和保存业务必需的用户个人信息；
- b) 测评对象：用户数据和业务应用系统；
- c) 测评实施：应核查采集的用户信息是否是业务应用必需的；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.4.10.2 测评单元（L4-ADS1-38）

该测评单元包括以下要求：

- a) 测评指标：应禁止未授权访问和非法使用用户个人信息；
- b) 测评对象：用户数据和业务应用系统；
- c) 测评实施：应核查是否采用技术措施限制对用户信息的访问和使用；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.5 安全策略和管理制度

9.1.5.1 安全策略

9.1.5.1.1 测评单元（L4-PSS1-01）

该测评单元包括以下要求：

- a) 测评指标：应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
- b) 测评对象：总体方针策略类文档；
- c) 测评实施：应核查信息安全工作的总体方针和安全策略文件是否明确机构安全工作的总体目标、范围、原则和各类安全策略。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.5.2 管理制度

9.1.5.2.1 测评单元（L4-PSS1-02）

该测评单元包括以下要求：

- a) 测评指标：应对安全管理活动中的各类管理内容建立安全管理制度；
- b) 测评对象：安全管理制度类文档；
- c) 测评实施：应核查各项安全管理制度是否覆盖物理、网络、主机系统、数据、应用、建设和运维等层面的管理内容。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.5.2.2 测评单元（L4-PSS1-03）

该测评单元包括以下要求：

- a) 测评指标：应对要求管理人员或操作人员执行的日常管理操作建立操作规程；
- b) 测评对象：操作规程类文档；

- c) 测评实施：应核查是否具有日常管理操作的操作规程，如系统维护手册和用户操作规程等。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.5.2.3 测评单元（L4-PSS1-04）

该测评单元包括以下要求：

- a) 测评指标：应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的信息安全管理制度体系；
- b) 测评对象：总体方针策略类文档、管理制度类文档、操作规程类文档和记录表单类文档；
- c) 测评实施：应核查总体方针策略文件、管理制度和操作规程是否形成体系化；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.5.3 制定和发布

9.1.5.3.1 测评单元（L4-PSS1-05）

该测评单元包括以下要求：

- a) 测评指标：应指定或授权专门的部门或人员负责安全管理制度的制定；
- b) 测评对象：信息安全主管；
- c) 测评实施：应访谈信息安全主管是否由专门的部门或人员负责制定安全管理制度；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.5.3.2 测评单元（L4-PSS1-06）

该测评单元包括以下要求：

- a) 测评指标：安全管理制度应通过正式、有效的方式发布，并进行版本控制；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查制度制定和发布要求管理文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容；
 - 2) 应核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导签署和单位盖章等，是否注明发布范围。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.5.4 评审和修订

9.1.5.4.1 测评单元（L4-PSS1-07）

该测评单元包括以下要求：

- a) 测评指标：应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否定期对安全管理制度体系的合理性和适用性进行审定；

- 2) 应核查是否具有安全管理制度的审定或论证记录,如果对制度做过修订,核查是否有修订版本的安全管理制度。
- d) 单元判定:如果 1)~2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.1.6 安全管理机构和人员

9.1.6.1 岗位设置

9.1.6.1.1 测评单元 (L4-ORS1-01)

该测评单元包括以下要求:

- a) 测评指标:应设立信息安全管理工作的职能部门,设立安全主管、安全管理各个方面的负责人岗位,并定义各负责人的职责;
- b) 测评对象:信息安全主管和管理制度类文档;
- c) 测评实施包括以下内容:
 - 1) 应访谈信息安全主管是否进行了信息安全管理职能部门的划分;
 - 2) 应核查部门职责文档是否明确信息安全管理工作的职能部门和各负责人职责;
 - 3) 应核查岗位职责文档是否明确岗位划分情况和岗位职责。
- d) 单元判定:如果 1)~2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.1.6.1.2 测评单元 (L4-ORS1-02)

该测评单元包括以下要求:

- a) 测评指标:应设立系统管理员、网络管理员、安全管理员等岗位,并定义部门及各个工作岗位的职责;
- b) 测评对象:信息安全主管和管理制度类文档;
- c) 测评实施包括以下内容:
 - 1) 应访谈信息安全主管是否进行了信息安全管理岗位的划分;
 - 2) 应核查岗位职责文档是否明确了各岗位职责。
- d) 单元判定:如果 1)~2) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.1.6.1.3 测评单元 (L4-ORS1-03)

该测评单元包括以下要求:

- a) 测评指标:应成立指导和管理信息安全工作的委员会或领导小组,其最高领导由单位主管领导委任或授权;
- b) 测评对象:信息安全主管、管理制度类文档和记录表单类文档;
- c) 测评实施包括以下内容:
 - 1) 应访谈信息安全主管是否成立了指导和管理信息安全工作的委员会或领导小组;
 - 2) 应核查部门职责文档是否明确信息安全工作委员会或领导小组构成情况和相关职责;
 - 3) 应核查是否具有信息安全工作的委员会或领导小组开展工作的会议纪要或相关记录。
- d) 单元判定:如果 1)~3) 均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.1.6.2 人员配备

9.1.6.2.1 测评单元 (L4-ORS1-04)

该测评单元包括以下要求：

- a) 测评指标：应配备一定数量的系统管理员、网络管理员、安全管理员等；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否配备系统管理员、网络管理员和安全管理员；
 - 2) 应核查人员配备文档是否明确各岗位人员配备情况。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.2.2 测评单元 (L4-ORS1-05)

该测评单元包括以下要求：

- a) 测评指标：应配备专职安全管理员，不可兼任；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查人员配备文档是否明确配备了专职安全管理员；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.6.2.3 测评单元 (L4-ORS1-06)

该测评单元包括以下要求：

- a) 测评指标：关键事务岗位应配备多人共同管理；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否对关键岗位配备了多人；
 - 2) 应核查人员配备文档是否针对关键岗位配备多人。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.3 授权和审批

9.1.6.3.1 测评单元 (L4-ORS1-07)

该测评单元包括以下要求：

- a) 测评指标：应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查部门职责文档是否明确各部门的职责和授权范围；
 - 2) 应核查岗位职责文档是否明确各岗位的职责和授权范围；
 - 3) 应核查审批记录是否针对审批事项、审批部门和批准人等内容与相关制度一致。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.3.2 测评单元 (L4-ORS1-08)

该测评单元包括以下要求：

- a) 测评指标：应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
- b) 测评对象：操作规程类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查系统变更、重要操作、物理访问和系统接入等事项的操作规范是否明确建立了逐级审批程序。
 - 2) 应核查审批记录、操作记录是否与相关制度一致。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.3.3 测评单元（L4-ORS1-09）

该测评单元包括以下要求：

- a) 测评指标：应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
- b) 测评对象：信息安全主管；
- c) 测评实施：应访谈信息安全主管是否对各类审批事项进行更新。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.6.4 沟通和合作

9.1.6.4.1 测评单元（L4-ORS1-10）

该测评单元包括以下要求：

- a) 测评指标：应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理信息安全问题；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否建立了各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通机制；
 - 2) 应核查会议记录是否明确在各类管理人员之间、组织内部机构之间以及信息安全职能部门内部开展了合作与沟通。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.4.2 测评单元（L4-ORS1-11）

该测评单元包括以下要求：

- a) 测评指标：应加强与公安机关、各类供应商、业界专家及安全组织的合作与沟通；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否建立了与公安机关、各类供应商、业界专家及安全组织的合作与沟通机制；
 - 2) 应核查会议记录是否与公安机关、各类供应商、业界专家及安全组织开展了合作与沟通。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.4.3 测评单元 (L4-ORS1-12)

该测评单元包括以下要求：

- a) 测评指标：应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查外联单位联系列表否记录了外联单位名称、合作内容、联系人和联系方式等信息；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.6.5 审核和检查

9.1.6.5.1 测评单元 (L4-ORS1-13)

该测评单元包括以下要求：

- a) 测评指标：应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否定期进行常规安全核查；
 - 2) 应核查常规安全检查记录是否包括了系统日常运行、系统漏洞和数据备份等情况。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.5.2 测评单元 (L4-ORS1-14)

该测评单元包括以下要求：

- a) 测评指标：应进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
- b) 测评对象：信息安全主管和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈信息安全主管是否定期进行全面安全核查；
 - 2) 应核查全面安全检查记录是否包括了现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.5.3 测评单元 (L4-ORS1-15)

该测评单元包括以下要求：

- a) 测评指标：应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；
- b) 测评对象：记录表单类文档；

- c) 测评实施：应核查是否具有安全检查表格、安全检查记录、安全检查报告、安全检查结果通报记录；
- d) 单元判定：如果以上测评实施为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.6.6 人员录用

9.1.6.6.1 测评单元（L4-ORS1-16）

该测评单元包括以下要求：

- a) 测评指标：应指定或授权专门的部门或人员负责人员录用；
- b) 测评对象：信息安全主管；
- c) 测评实施：应访谈信息安全主管是否由专门的部门或人员负责人员的录用工作。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.6.6.2 测评单元（L4-ORS1-17）

该测评单元包括以下要求：

- a) 测评指标：应对被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查人员安全管理文档是否说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）；
 - 2) 应核查是否具有人员录用时对录用人身份、背景、专业资格和资质等进行审查的相关文档或记录等；
 - 3) 应核查人员录用时的技能考核文档或记录是否记录考核内容和考核结果等。
- d) 单元判定：如果 1)～3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.6.3 测评单元（L4-ORS1-18）

该测评单元包括以下要求：

- a) 测评指标：应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查保密协议是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容；
 - 2) 应核查岗位安全协议是否有岗位安全责任定义、协议的有效期限和责任人签字等内容。
- d) 单元判定：如果 1)～2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.6.4 测评单元（L4-ORS1-19）

该测评单元包括以下要求：

- a) 测评指标：应从内部人员中选拔从事关键岗位的人员；

- b) 测评对象：人事负责人；
- c) 测评实施：应访谈人事负责人从事关键岗位的人员是否是从内部人员选拔担任；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.6.7 人员离岗

9.1.6.7.1 测评单元（L4-ORS1-20）

该测评单元包括以下要求：

- a) 测评指标：应及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有离岗人员交还身份证件、设备等的登记记录；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.6.7.2 测评单元（L4-ORS1-21）

该测评单元包括以下要求：

- a) 测评指标：应办理严格的调离手续，并承诺调离后的保密义务后方可离开；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查人员离岗的管理文档是否规定了人员调离手续和离岗要求等；
 - 2) 应核查是否具有按照离岗程序办理调离手续的记录；
 - 3) 应核查保密承诺文档是否有调离人员的签字。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.8 安全意识教育和培训

9.1.6.8.1 测评单元（L4-ORS1-22）

该测评单元包括以下要求：

- a) 测评指标：应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
- b) 测评对象：管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查信息安全教育及技能培训文档是否明确培训周期、培训方式、培训内容和考核方式等相关内容；
 - 2) 应核查安全责任和惩戒措施管理文档是否包含具体的安全责任和惩戒措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.8.2 测评单元（L4-ORS1-23）

该测评单元包括以下要求：

- a) 测评指标：应针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查安全教育和培训计划文档是否具有不同岗位的培训计划，培训内容是否包含信息安全基础知识、岗位操作规程等；
 - 2) 应核查安全教育和培训记录是否有培训人员、培训内容、培训结果等的描述。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.8.3 测评单元（L3-ORS1-24）

该测评单元包括以下要求：

- a) 测评指标：应定期对不同岗位的人员进行技能考核；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有针对各岗位人员的技能考核记录。
- d) 单元判定：如果以上测评实施为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.9 外部人员访问管理

9.1.6.9.1 测评单元（L4-ORS1-25）

该测评单元包括以下要求：

- a) 测评指标：应确保在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查外部人员访问管理文档是否明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等；
 - 2) 应核查外部人员访问重要区域的书面申请文档，是否具有批准人允许访问的批准签字等；
 - 3) 应核查外部人员访问重要区域的登记记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.9.2 测评单元（L4-ORS1-26）

该测评单元包括以下要求：

- a) 测评指标：应确保在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查外部人员访问管理文档是否明确外部人员接入网络前的申请审批流程；
 - 2) 应核查外部人员访问系统的书面申请文档是否明确外部人员的访问权限，是否具有允许访问的批准签字等；

- 3) 应核查外部人员访问系统的登记记录是否记录了外部人员访问的权限、时限、账户等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.9.3 测评单元 (L4-ORS1-27)

该测评单元包括以下要求：

- a) 测评指标：外部人员离场后应及时清除其所有的访问权限；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查外部人员访问管理文档是否明确外部人员离开后及时清除其所有访问权限；
 - 2) 应核查外部人员访问系统的登记记录是否记录了访问权限清除时间。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.6.9.4 测评单元 (L4-ORS1-28)

该测评单元包括以下要求：

- a) 测评指标：获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查外部人员访问保密协议是否明确人员的保密义务(如不得进行非授权操作，不得复制信息等)；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.6.9.5 测评单元 (L4-ORS1-29)

该测评单元包括以下要求：

- a) 测评指标：对关键区域或关键系统不允许外部人员访问；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查外部人员访问管理文档是否明确不允许外部人员访问关键区域或关键业务系统。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7 安全建设管理

9.1.7.1 定级和备案

9.1.7.1.1 测评单元 (L4-CMS1-01)

该测评单元包括以下要求：

- a) 测评指标：应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查定级文档是否明确保护对象的安全保护等级，是否说明定级的方法和理由。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.1.2 测评单元（L4-CMS1-02）

该测评单元包括以下要求：

- a) 测评指标：应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查定级结果的论证评审会议记录是否有相关部门和有关安全技术专家对定级结果的论证意见；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.1.3 测评单元（L4-CMS1-03）

该测评单元包括以下要求：

- a) 测评指标：应确保定级结果经过相关部门的批准；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查定级结果部门审批文档是否有上级主管部门或本单位相关部门的审批意见。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.1.4 测评单元（L4-CMS1-04）

该测评单元包括以下要求：

- a) 测评指标：应将备案材料报主管部门和相应公安机关备案；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有公安机关出具的备案证明文档；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.2 安全方案设计

9.1.7.2.1 测评单元（L4-CMS1-05）

该测评单元包括以下要求：

- a) 测评指标：应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
- b) 测评对象：安全规划设计类文档；
- c) 测评实施：应核查安全设计文档是否根据安全等级选择安全措施，是否根据安全需求调整安全措施；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.2.2 测评单元（L4-CMS1-06）

该测评单元包括以下要求：

- a) 测评指标：应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码相关内容，并形成配套文件；
- b) 测评对象：安全规划设计类文档；
- c) 测评实施：应核查是否有总体规划和安全设计方案等配套文件，设计方案中应保护密码相关内容；

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.2.3 测评单元（L4-CMS1-07）

该测评单元包括以下要求：

- a) 测评指标：应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查配套文件的论证评审记录或文档是否有相关部门和有关安全技术专家对总体安全规划、安全设计方案等相关配套文件的论证意见；
 - 2) 应核查是否有总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件，各个文件是否有机构管理层的批准。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.7.3 产品采购和使用

9.1.7.3.1 测评单元（L4-CMS1-08）

该测评单元包括以下要求：

- a) 测评指标：应确保信息安全产品采购和使用符合国家的有关规定；
- b) 测评对象：建设负责人。
- c) 测评实施：应访谈建设负责人系统使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.3.2 测评单元（L4-CMS1-09）

该测评单元包括以下要求：

- a) 测评指标：应确保密码产品采购和使用符合国家密码主管部门的要求；
- b) 测评对象：建设负责人；
- c) 测评实施：应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.3.3 测评单元（L4-CMS1-10）

该测评单元包括以下要求：

- a) 测评指标：应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有产品选型测试结果文档、候选产品采购清单及审定或更新的记录

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.3.4 测评单元（L4-CMS1-11）

该测评单元包括以下要求：

- a) 测评指标：应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有重要产品专项测试记录；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.4 自行软件开发

9.1.7.4.1 测评单元（L4-CMS1-12）

该测评单元包括以下要求：

- a) 测评指标：应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
- b) 测评对象：建设负责人；
- c) 测评实施包括以下内容：
 - 1) 应访谈建设负责人自主开发软件是否在独立的物理环境中完成编码和调试，与实际运行环境分开；
 - 2) 应核查测试数据和结果是否受控使用。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.7.4.2 测评单元（L4-CMS1-13）

该测评单元包括以下要求：

- a) 测评指标：应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查软件开发管理制度是否明确软件设计、开发、测试、验收过程的控制方法和人员行为准则，是否明确哪些开发活动应经过授权、审批。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.4.3 测评单元（L4-CMS1-14）

该测评单元包括以下要求：

- a) 测评指标：应制定代码编写安全规范，要求开发人员参照规范编写代码；
- b) 测评对象：管理制度类文档。
- c) 测评实施：应核查代码编写安全规范是否明确代码安全编写规则；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.4.4 测评单元（L4-CMS1-15）

该测评单元包括以下要求：

- a) 测评指标：应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有软件开发文档和使用指南；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.4.5 测评单元（L4-CMS1-16）

该测评单元包括以下要求：

- a) 测评指标：应确保在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有软件安全测试报告，明确软件存在的安全问题及可能存在的恶意代码；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.4.6 测评单元（L4-CMS1-17）

该测评单元包括以下要求：

- a) 测评指标：应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查对程序资源库的修改、更新、发布进行授权和审批的文档或记录是否有批准人的签字；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.4.7 测评单元（L4-CMS1-18）

该测评单元包括以下要求：

- a) 测评指标：应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查；
- b) 测评对象：建设负责人；
- c) 测评实施：应访谈建设负责人开发人员是否为专职，是否对开发人员活动进行控制等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.5 外包软件开发

9.1.7.5.1 测评单元（L4-CMS1-19）

该测评单元包括以下要求：

- a) 测评指标：应在软件交付前检测其中可能存在的恶意代码；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有交付前的恶意代码检测报告。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.5.2 测评单元（L4-CMS1-20）

该测评单元包括以下要求：

- a) 测评指标：应要求开发单位提供软件设计文档和使用指南；
- b) 测评对象：记录表单类文档。
- c) 测评实施：应核查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.5.3 测评单元（L4-CMS1-21）

该测评单元包括以下要求：

- a) 测评指标：应要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道；
- b) 测评对象：建设负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈建设负责人委托开发单位是否提供软件源代码；
 - 2) 应核查软件测试报告是否明确审查了软件可能存在的后门和隐蔽信道并记录。
- d) 单元判定：如果1)~2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.7.6 工程实施

9.1.7.6.1 测评单元（L4-CMS1-22）

该测评单元包括以下要求：

- a) 测评指标：应指定或授权专门的部门或人员负责工程实施过程的管理；
- b) 测评对象：建设负责人；
- c) 测评实施：应访谈建设负责人是否指定专门部门或人员对工程实施过程进行进度和质量控制，由何部门/何人负责；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.6.2 测评单元（L4-CMS1-23）

该测评单元包括以下要求：

- a) 测评指标：应制定工程实施方案控制安全工程实施过程；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查工程实施方案是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.6.3 测评单元（L4-CMS1-24）

该测评单元包括以下要求：

- a) 测评指标：应通过第三方工程监理控制项目的实施过程；
- b) 测评对象：记录表单类文档；

- c) 测评实施：如果安全建设为第三方实施时，应核查工程监理报告是否明确了工程进展、时间计划、控制措施等方面内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.7 测试验收

9.1.7.7.1 测评单元（L4-CMS1-25）

该测评单元包括以下要求：

- a) 测评指标：应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查工程测试验收方案是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容；
 - 2) 应核查测试验收报告是否有相关部门和人员对测试验收报告进行审定的意见。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.7.7.2 测评单元（L4-CMS1-26）

该测评单元包括以下要求：

- a) 测评指标：应进行上线前的安全性测试，验证安全措施的有效性，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查是否具有上线前的安全测试报告，报告应包含密码应用安全性测试相关内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.8 系统交付

9.1.7.8.1 测评单元（L4-CMS1-27）

该测评单元包括以下要求：

- a) 测评指标：应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查交付清单是否说明系统交付的各类设备、软件、文档等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.8.2 测评单元（L4-CMS1-28）

该测评单元包括以下要求：

- a) 测评指标：应对负责运行维护的技术人员进行相应的技能培训；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查交付技术培训记录是否包括培训内容、培训时间和参与人员等。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.8.3 测评单元（L4-CMS1-29）

该测评单元包括以下要求：

- a) 测评指标：应确保提供建设过程中的文档和指导用户进行运行维护的文档；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查交付文档是否有指导用户进行运维的文档等，提交的文档是否符合管理规定的要求；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.9 等级测评

9.1.7.9.1 测评单元（L4-CMS1-30）

该测评单元包括以下要求：

- a) 测评指标：应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人本次测评是否为首次，若非首次，以往进行过几次测评，是否根据测评结果进行相应的安全整改；
 - 2) 应核查是否具有以往等级测评报告和安全整改方案。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.7.9.2 测评单元（L4-CMS1-31）

该测评单元包括以下要求：

- a) 测评指标：应在发生重大变更或级别发生变化时进行等级测评；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人系统是否有过重大变更或级别发生过变化，若有，是否进行相应的等级测评；
 - 2) 应核查是否具有相应情况下的等级测评报告。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.7.9.3 测评单元（L4-CMS1-32）

该测评单元包括以下要求：

- a) 测评指标：应确保测评机构的选择符合国家有关规定；
- b) 测评对象：运维负责人；
- c) 测评实施：应访谈运维负责人以往等级测评的测评单位是否具有国家相关等级测评资质的单位。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.10 服务供应商管理

9.1.7.10.1 测评单元（L4-CMS1-33）

该测评单元包括以下要求：

- a) 测评指标：应确保服务供应商的选择符合国家的有关规定；
- b) 测评对象：运维负责人；
- c) 测评实施：应访谈建设负责人选择的安全服务商是否符合国家有关规定；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.10.2 测评单元（L4-CMS1-34）

该测评单元包括以下要求：

- a) 测评指标：应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的信息安全相关义务；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查与安全服务商签订的服务合同或安全责任合同书是否明确了后期的技术支持和服务承诺等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.7.10.3 测评单元（L4-CMS1-35）

该测评单元包括以下要求：

- a) 测评指标：应定期监视、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查是否具有安全服务商定期提交的安全服务报告；
 - 2) 应核查是否定期审核评价安全服务供应商所提供的服务，是否具有服务审核报告；
 - 3) 应核查是否具有安全服务商评价审核管理制度，明确针对服务商的评价指标、考核内容等。
- d) 单元判定：如果1)~3)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8 安全运维管理

9.1.8.1 环境管理

9.1.8.1.1 测评单元（L4-MMS1-01）

该测评单元包括以下要求：

- a) 测评指标：应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
- b) 测评对象：物理安全负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈物理安全负责人是否指定部门和人员负责机房安全管理工作，对机房的出入进行管理、对基础设施（如空调、供配电设备、灭火设备等）进行定期维护，由何部门/何人负责；
 - 2) 应核查部门或人员岗位职责文档，查看是否明确机房安全的责任部门及人员；
 - 3) 应核查机房的出入登记记录，查看是否记录来访人员、来访时间、离开时间、携带物品等信息；

- 4) 应核查机房的基础设施的维护记录, 查看是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
- d) 单元判定: 如果 1) -4) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

9.1.8.1.2 测评单元 (L4-MMS1-02)

该测评单元包括以下要求:

- a) 测评指标: 应对机房的安全管理做出规定, 包括机房物理访问、物品带进带出和机房环境安全等;
- b) 测评对象: 管理制度类文档和记录表单类文档;
- c) 测评实施包括以下内容:
 - 1) 应核查机房安全管理制度是否覆盖机房物理访问、物品带进、带出机房和机房环境安全等方面内容;
 - 2) 应核查机房环境和物理访问、物品带进、带出机房等的登记记录, 是否与制度相符。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

9.1.8.1.3 测评单元 (L4-MMS1-03)

该测评单元包括以下要求:

- a) 测评指标: 应不在重要区域接待来访人员和桌面上没有包含敏感信息的纸档文件、移动介质等;
- b) 测评对象: 管理制度类文档和办公环境;
- c) 测评实施包括以下内容:
 - 1) 应核查机房安全管理制度是否明确来访人员的接待区域;
 - 2) 应核查办公桌面上是否不包含敏感信息的纸档文件和移动介质等。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

9.1.8.1.4 测评单元 (L4-MMS1-04)

该测评单元包括以下要求:

- a) 测评指标: 应对出入人员进行相应级别的授权, 对进入重要安全区域的人员和活动实时监视等;
- b) 测评对象: 记录表单类文档;
- c) 测评实施包括以下内容:
 - 1) 应核查出入人员授权审批记录是否明确对人员授权是否有不同的授权;
 - 2) 应核查重要区域是否安装监控系统, 实时监控进入人员活动。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

9.1.8.2 资产管理

9.1.8.2.1 测评单元 (L4-MMS1-05)

该测评单元包括以下要求:

- a) 测评指标: 应编制并保存与保护对象相关的资产清单, 包括资产责任部门、重要程度和所处位置等内容;

- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查资产清单是否覆盖资产范围（含设备设施、软件、文档等）、资产责任部门、重要程度和所处位置等内容。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.2.2 测评单元（L4-MMS1-06）

该测评单元包括以下要求：

- a) 测评指标：应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
- b) 测评对象：资产管理单、管理制度类文档和设备；
- c) 测评实施包括以下内容：
 - 1) 应访谈资产管理单是否依据资产的重要程度对资产进行标识，不同类别的资产在管理措施的选取上是否不同；
 - 2) 应核查资产管理制度是否明确资产的标识方法以及不同资产的管理措施要求；
 - 3) 应核查资产清单中的设备是否具有相应标识，标识方法是否符合 2) 中相关要求。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.2.3 测评单元（L4-MMS1-07）

该测评单元包括以下要求：

- a) 测评指标：应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理；
- b) 测评对象：管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查信息分类文档是否规定了分类标识的原则和方法（如根据信息的重要程度、敏感程度或用途不同进行分类）；
 - 2) 应核查信息资产管理办法是否规定了不同类信息的使用、传输和存储等。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.3 介质管理

9.1.8.3.1 测评单元（L4-MMS1-08）

该测评单元包括以下要求：

- a) 测评指标：应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储介质专人管理，并根据存档介质的目录清单定期盘点；
- b) 测评对象：资产管理单和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈资产管理单介质存放于何种环境中，是否对存放环境实施专人管理；
 - 2) 应核查介质使用管理记录是否记录介质归档和使用等情况。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.3.2 测评单元（L4-MMS1-09）

该测评单元包括以下要求：

- a) 测评指标：应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录；
- b) 测评对象：资产管理类和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈资产管理类介质在物理传输过程中的人员、打包交付等情况是否进行控制；
 - 2) 应核查是否有对介质的归档和查询等的登记记录。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.4 设备维护管理

9.1.8.4.1 测评单元（L4-MMS1-10）

该测评单元包括以下要求：

- a) 测评指标：应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
- b) 测评对象：设备管理类和管理制度类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈设备管理员是否对各类设施、设备指定专人或专门部门进行定期维护；
 - 2) 应核查部门或人员岗位职责文档是否明确设备维护管理的责任部门。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.4.2 测评单元（L4-MMS1-11）

该测评单元包括以下要求：

- a) 测评指标：应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；
- b) 测评对象：管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查设备维护管理制度是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容；
 - 2) 应核查是否具有维修和服务的审批、维修过程等记录，审批、记录内容是否与制度相符。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.4.3 测评单元（L4-MMS1-12）

该测评单元包括以下要求：

- a) 测评指标：应确保信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密；
- b) 测评对象：设备管理类和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈设备管理员含有重要数据的存储介质带出工作环境是否有加密措施，采取什么加密措施；

- 2) 应访谈设备管理员对带离机房的设备是否经过审批, 由何人审批;
- 3) 应核查是否具有设备带离机房或办公地点的审批记录。
- d) 单元判定: 如果 1) -3) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

9.1.8.4.4 测评单元 (L4-MMS1-13)

该测评单元包括以下要求:

- a) 测评指标: 含有存储介质的设备在报废或重用前, 应进行完全清除或被安全覆盖, 确保该设备上的敏感数据和授权软件无法被恢复重用;
- b) 测评对象: 设备管理员;
- c) 测评实施: 应访谈设备管理员含有存储介质的设备在报废或重用前, 是否采取措施进行完全清除或被安全覆盖;
- d) 单元判定: 如果以上测评实施内容为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

9.1.8.5 漏洞和风险管理

9.1.8.5.1 测评单元 (L4-MMS1-14)

该测评单元包括以下要求:

- a) 测评指标: 应采取必要的措施识别安全漏洞和隐患, 对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补;
- b) 测评对象: 安全管理员和记录表单类文档;
- c) 测评实施包括以下内容:
 - 1) 应访谈安全管理员是否定期进行漏洞扫描, 对发现的漏洞是否及时进行修补或评估可能的影响后进行修补;
 - 2) 应核查漏洞扫描报告是否描述了存在的漏洞、严重级别、原因分析和改进意见等方面。
- d) 单元判定: 如果 1) -2) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

9.1.8.5.2 测评单元 (L4-MMS1-15)

该测评单元包括以下要求:

- a) 测评指标: 应定期开展安全测评, 形成安全测评报告, 采取措施应对发现的安全问题;
- b) 测评对象: 安全管理员和记录表单类文档;
- c) 测评实施包括以下内容:
 - 1) 应访谈安全管理员是否定期开展安全测评;
 - 2) 应核查是否具有安全测评报告;
 - 3) 应核查是否具有安全整改应对措施文档。
- d) 单元判定: 如果 1) -3) 均为肯定, 则符合本测评单元指标要求, 否则不符合或部分符合本测评单元指标要求。

9.1.8.6 网络和系统安全管理

9.1.8.6.1 测评单元 (L4-MMS1-16)

该测评单元包括以下要求:

- a) 测评指标：应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查网络和系统安全管理文档，查看是否明确要求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.6.2 测评单元（L4-MMS1-17）

该测评单元包括以下要求：

- a) 测评指标：应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人是否指定专门的部门或人员进行账户管理；
 - 2) 应核查相关审批记录或流程是否对申请账户、建立账户、删除账户等进行控制。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.6.3 测评单元（L4-MMS1-18）

该测评单元包括以下要求：

- a) 测评指标：应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略，账户管理（用户责任、义务、风险、权限审批、权限分配、账户注销等），配置文件的生成、备份，变更审批、符合性核查等，授权访问，最小服务，升级与打补丁，审计日志，登录设备和系统的口令更新周期等方面；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.6.4 测评单元（L4-MMS1-19）

该测评单元包括以下要求：

- a) 测评指标：应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
- b) 测评对象：操作规程类文档。
- c) 测评实施：应核查重要设备（如操作系统、数据库、网络设备、安全设备、应用和组件）的配置和操作手册是否明确操作步骤、维护记录、参数配置等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.6.5 测评单元（L4-MMS1-20）

该测评单元包括以下要求：

- a) 测评指标：应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修改等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.6.6 测评单元（L3-MMS1-21）

该测评单元包括以下要求：

- a) 测评指标：应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络和系统相关人员是否指定专门部门或人员对日志、监测和报警数据等进行分析统计；
 - 2) 应核查是否具有对日志、监测和报警数据等进行分析统计的报告。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.6.7 测评单元（L4-MMS1-22）

该测评单元包括以下要求：

- a) 测评指标：应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络和系统相关人员调整配置参数结束后是否同步更新配置信息库，并核实配置信息库是否为最新版本；
 - 2) 应核查是否具有变更运维的审批记录，如系统连接、安装系统组件或调整配置参数等活动；
 - 3) 应核查是否具有针对变更运维的操作过程记录。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.6.8 测评单元（L4-MMS1-23）

该测评单元包括以下要求：

- a) 测评指标：应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统相关人员使用运维工具结束后是否删除工具中的敏感数据；
 - 2) 应核查是否具有运维工具接入系统的审批记录；
 - 3) 应核查运维工具的审计日志记录，审计日志是否不可以更改。

- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.6.9 测评单元 (L4-MMS1-24)

该测评单元包括以下要求：

- a) 测评指标：应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；
- b) 测评对象：记录表单类文档。
- c) 测评实施包括以下内容：
 - 1) 应访谈系统相关人员日常运维过程中是否存在远程运维，若存在，远程运维结束后是否立即关闭了接口或通道；
 - 2) 应核查开通远程运维的审批记录；
 - 3) 应核查针对远程运维的审计日志是否不可以更改。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.6.10 测评单元 (L4-MMS1-25)

该测评单元包括以下要求：

- a) 测评指标：应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为；
- b) 测评对象：安全管理员和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统相关人员外联种类（互联网、合作伙伴企业网、上级部门网络等）是否都得到授权与批准，由何人/何部门批准；
 - 2) 应访谈安全管理员是否定期核查违规联网行为；
 - 3) 应核查是否具有外联授权的记录文件。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.7 恶意代码防范管理

9.1.8.7.1 测评单元 (L4-MMS1-26)

该测评单元包括以下要求：

- a) 测评指标：应提高所有用户的防恶意代码意识，告知对外来计算机或存储设备接入系统前进行恶意代码检查等；
- b) 测评对象：运维负责人；
- c) 测评实施：应访谈运维负责人是否采取告知方式提升员工的防病毒意识；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.7.2 测评单元 (L4-MMS1-27)

该测评单元包括以下要求：

- a) 测评指标：应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查恶意代码防范管理制度是否明确防恶意代码软件的授权使用、恶意代码库升级、定期查杀等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.7.3 测评单元（L4-MMS1-28）

该测评单元包括以下要求：

- a) 测评指标：应定期验证防范恶意代码攻击的技术措施的有效性；
- b) 测评对象：安全管理员和记录表单类文档。
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否定期对恶意代码库进行升级，且对升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报，是否出现过大规模的病毒事件，如何处理；
 - 2) 应核查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告。
 - 3) 应核查是否定期采用技术手段测试验证恶意代码防范技术措施的有效性。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.8 配置管理

9.1.8.8.1 测评单元（L4-MMS1-29）

该测评单元包括以下要求：

- a) 测评指标：应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；
- b) 测评对象：系统管理员；
- c) 测评实施：应访谈系统管理员是否对基本配置信息进行记录和保存；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.8.2 测评单元（L4-MMS1-30）

该测评单元包括以下要求：

- a) 测评指标：应将基本配置信息改变纳入系统变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库；
- b) 测评对象：系统管理员和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈配置管理人员基本配置信息改变后是否及时更新基本配置信息库；
 - 2) 应核查配置信息的变更流程是否具有相应的申报审批程序。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.9 密码管理

9.1.8.9.1 测评单元（L4-MMS1-31）

该测评单元包括以下要求：

- a) 测评指标：应使用符合国家密码管理规定的密码技术和产品；
- b) 测评对象：安全管理员；
- c) 测评实施：应核查相关产品是否获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.9.2 测评单元（L4-MMS1-32）

该测评单元包括以下要求：

- a) 测评指标：应采用密码模块实现密码运算和密钥管理；
- b) 测评对象：安全管理员；
- c) 测评实施：应核查相关产品是否采用密码技术实现密码运算和密钥管理；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.10 变更管理

9.1.8.10.1 测评单元（L4-MMS1-33）

该测评单元包括以下要求：

- a) 测评指标：应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查变更方案是否包含变更类型、变更原因、变更过程、变更前评估等内容；
 - 2) 应核查是否具有变更方案评审记录和变更过程记录文档。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.10.2 测评单元（L4-MMS1-34）

该测评单元包括以下要求：

- a) 测评指标：应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应核查变更控制的申报、审批程序是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容；
 - 2) 应核查是否具有变更实施过程的记录文档；
 - 3) 应核查是否针对发生变更的事件进行了影响分析。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.10.3 测评单元（L4-MMS1-35）

该测评单元包括以下要求：

- a) 测评指标：应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人变更失败后的恢复程序、工作方法和职责是否文档化，恢复过程是否经过演练；
 - 2) 应核查是否具有变更恢复演练记录；
 - 3) 应核查变更失败恢复程序是否规定变更失败后的恢复流程。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.11 备份与恢复管理

9.1.8.11.1 测评单元（L4-MMS1-36）

该测评单元包括以下要求：

- a) 测评指标：应识别需要定期备份的重要业务信息、系统数据及软件系统等；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员、数据库管理员和网络管理员是否识别需定期备份的业务信息、系统数据及软件系统；
 - 2) 应核查是否具有定期备份的重要业务信息、系统数据、软件系统的列表或清单。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.11.2 测评单元（L4-MMS1-37）

该测评单元包括以下要求：

- a) 测评指标：应规定备份信息的备份方式、备份频度、存储介质、保存期等；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查备份与恢复管理制度是否明确备份方式、频度、介质、保存期等内容。
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.11.3 测评单元（L4-MMS1-38）

该测评单元包括以下要求：

- a) 测评指标：应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查备份和恢复的策略是否明确备份策略和恢复策略文档规范了数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.12 安全事件处置

9.1.8.12.1 测评单元（L4-MMS1-39）

该测评单元包括以下要求：

- a) 测评指标：应及时向安全管理部门报告所发现的安全弱点和可疑事件；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人是否告知用户在发现安全弱点和可疑事件时应及时向安全管理部门报告；
 - 2) 应核查是否有运维过程中发现的安全弱点和可疑事件对应的报告或相关文档，内容是否详实。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.12.2 测评单元（L4-MMS1-40）

该测评单元包括以下要求：

- a) 测评指标：应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查安全事件报告和处置管理制度是否明确了与安全事件有关的工作职责，各类事件的处置相应流程等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.12.3 测评单元（L4-MMS1-41）

该测评单元包括以下要求：

- a) 测评指标：应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查安全事件报告和响应处置记录是否记录引发安全事件的系统弱点、不同安全事件发生的原因、处置过程、经验教训总结、补救措施等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.12.4 测评单元（L4-MMS1-42）

该测评单元包括以下要求：

- a) 测评指标：对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序；
- b) 测评对象：记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人其不同安全事件的报告流程；
 - 2) 应核查安全事件报告和处理程序文档是否根据不同安全事件制定不同的处理和报告程序，是否明确具体报告方式、报告内容、报告人等方面内容。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.13 应急预案管理

9.1.8.13.1 测评单元（L3-MMS1-43）

该测评单元包括以下要求：

- a) 测评指标：应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；
- b) 测评对象：管理制度类文档；
- c) 测评实施：应核查应急预案框架是否覆盖启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等方面；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.13.2 测评单元（L3-MMS1-44）

该测评单元包括以下要求：

- a) 测评指标：应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；
- b) 测评对象：管理制度类文档。
- c) 测评实施：应核查是否具有重要事件的应急预案（如针对机房、系统、网络等各个层面）；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.13.3 测评单元（L4-MMS1-45）

该测评单元包括以下要求：

- a) 测评指标：应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；
- b) 测评对象：运维负责人和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人是否定期对相关人员进行应急预案培训和演练；
 - 2) 应核查应急预案培训记录是否明确培训对象、培训内容、培训结果等；
 - 3) 应核查应急预案演练记录是否记录演练时间、主要操作内容、演练结果等。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.13.4 测评单元（L4-MMS1-46）

该测评单元包括以下要求：

- a) 测评指标：应定期对原有的应急预案重新评估，修订完善；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查应急预案修订记录是否明确修订时间、修订内容等；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.14 外包运维管理

9.1.8.14.1 测评单元（L4-MMS1-47）

该测评单元包括以下要求：

- a) 测评指标：应确保外包运维服务商的选择符合国家的有关规定；
- b) 测评对象：运维负责人；
- c) 测评实施包括以下内容：
 - 1) 应访谈运维负责人是否有外包运维服务情况；
 - 2) 应访谈运维负责人进行外包运维服务的服务单位是否符合国家有关规定。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.1.8.14.2 测评单元（L4-MMS1-48）

该测评单元包括以下要求：

- a) 测评指标：应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查外包运维服务协议是否明确约定外包运维的范围和工作内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.14.3 测评单元（L4-MMS1-49）

该测评单元包括以下要求：

- a) 测评指标：应确保选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查与外包运维服务商签订的协议中是否明确其具有等级保护要求的服务能力要求；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.1.8.14.4 测评单元（L4-MMS1-50）

该测评单元包括以下要求：

- a) 测评指标：应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查外包运维服务协议是否包含可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.2 云计算安全测评扩展要求

9.2.1 物理和环境安全

9.2.1.1 物理位置选择

9.2.1.1.1 测评单元（L4-PES2-01）

该测评单元包括以下要求：

- a) 测评指标：应确保云计算基础设施位于中国境内；
- b) 测评对象：机房管理员、办公场地、机房和平台建设方案；
- c) 测评实施包括以下内容：
 - 1) 应访谈机房管理员云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和数据的软硬件是否均位于中国境内；
 - 2) 应核查云平台建设方案是否明确云计算服务器、云管理平台、信息系统上重要信息的处理、存储、业务的运行需位于中国境内。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2 网络和通信安全

9.2.2.1 网络架构

9.2.2.1.1 测评单元 (L4-NCS2-01)

该测评单元包括以下要求：

- a) 测评指标：应确保云计算平台不承载高于其安全保护等级的业务应用系统；
- b) 测评对象：云计算平台和业务应用系统定级材料；
- c) 测评实施：应核查云计算平台和云计算平台承载的业务应用系统相关定级材料，查看云计算平台安全保护等级是否不低于其承载的业务应用系统；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

9.2.2.1.2 测评单元 (L4-NCS2-02)

该测评单元包括以下要求：

- a) 测评指标：应绘制与当前运行情况相符的虚拟化网络拓扑结构图，并能对虚拟化网络资源、网络拓扑进行实时更新；
- b) 测评对象：综合网管系统、云管理平台、网络拓扑图、网络设备和安全设备；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务商综合网管系统、云管理平台或云服务客户管理平台是否对虚拟化网络资源（如虚拟交换机、虚拟防火墙等）、虚拟网络拓扑进行实时更新；
 - 2) 应核查网络拓扑结构图是否与当前运行情况相符。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.1.3 测评单元 (L4-NCS2-03)

该测评单元包括以下要求：

- a) 测评指标：应实现不同云服务客户虚拟网络之间的隔离；
- b) 测评对象：网络资源隔离措施、综合网管系统和云管理平台；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户之间虚拟网络隔离措施；
 - 2) 应核查云服务客户之间虚拟网络资源隔离策略是否有效；
 - 3) 应测试不同云服务客户之间的网络隔离措施是否生效。

- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.1.4 测评单元 (L4-NCS2-04)

该测评单元包括以下要求：

- a) 测评指标：应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；
- b) 测评对象：防火墙、入侵检测系统和入侵保护系统等安全设备；
- c) 测评实施包括以下内容：
 - 1) 核查向云服务客户提供的通信传输、边界防护、入侵防范等安全机制是否有效；
 - 2) 核查虚拟防火墙、虚拟入侵保护系统等安全机制是否满足客户业务安全需求。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.1.5 测评单元 (L4-NCS2-05)

该测评单元包括以下要求：

- a) 测评指标：应具有根据云服务客户业务需求自主设置安全策略集的能力，包括定义访问路径、选择安全组件、配置安全策略；
- b) 测评对象：云管理平台、网络管理平台、网络设备和安全访问路径；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务商的云管理平台或网络设备是否支持云服务客户业务自定义安全策略集、安全访问路径、安全组件和安全策略；
 - 2) 应核查云服务客户的网络管理平台或网络设备是否已定义安全访问路径、安全策略和安全组件；
 - 3) 核查云服务商管理员进行远程管理时，管理终端与管理服务器之间是否建立了安全访问路径。
- d) 单元判定：如果 2) 或 1)、3) 为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.1.6 测评单元 (L4-NCS2-06)

该测评单元包括以下要求：

- a) 测评指标：应保证云计算平台管理流量与云服务客户业务流量分离；
- b) 测评对象：网络架构和云管理平台；
- c) 测评实施包括以下内容：
 - 1) 应核查网络架构和配置策略能否采用带外管理或策略配置等方式实现管理流量和业务流量分离；
 - 2) 应核查云平台管理流量与云服务客户业务流量是否分离，核查所采取的技术手段和流量分离手段；
 - 3) 应测试云计算平台管理流量与业务流量是否分离。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.1.7 测评单元 (L4-NCS2-07)

该测评单元包括以下要求：

- a) 测评指标：应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云平台选择第三方安全服务；
- b) 测评对象：系统管理员、相关接口和相关服务；
- c) 测评实施包括以下内容：
 - 1) 应核查接口设计文档或开放性服务技术文档是否符合开放性、安全性要求；
 - 2) 如果提供开放接口，应核查内部通信网络（虚拟网络）为第三方安全产品所提供的开放接口安全保障机制、接口配置或参数是否符合安全需求；
 - 3) 如果提供开放性安全产品、服务，应核查开放性安全产品及服务的服务内容和实现开放性安全服务所采用的技术手段、安全保障机制是否符合安全需求。
- d) 单元判定：如果 1)、2) 或 1)、3) 为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.1.8 测评单元（L4-NCS2-08）

该测评单元包括以下要求：

- a) 测评指标：应为四级业务应用系统划分独立的资源池；
- b) 测评对象：网络结构和云平台建设方案；
- c) 测评实施包括以下内容：
 - 1) 云平台建设方案中是否对承载四级业务系统的资源池做出独立划分设计；
 - 2) 网络结构中是否对四级业务系统划分独立的资源池。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.2 访问控制

9.2.2.2.1 测评单元（L4-NCS2-09）

该测评单元包括以下要求：

- a) 测评指标：应禁止云服务客户虚拟机访问宿主机；
- b) 测评对象：云管理平台和虚拟机监视器；
- c) 测评实施包括以下内容：
 - 1) 应核查云管理平台等能否检测到云服务客户虚拟机对宿主机的访问；
 - 2) 应测试虚拟机监视器和云管理平台，验证是否能够及时检测到云服务客户虚拟机访问宿主机资源等行为并进行报警，如利用虚机逃逸漏洞验证是否触发报警。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.2.2 测评单元（L4-NCS2-10）

该测评单元包括以下要求：

- a) 测评指标：应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；
- b) 测评对象：访问控制机制、网络边界设备和虚拟化网络边界设备；
- c) 测评实施包括以下内容：
 - 1) 应核查云平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略是否有效；

- 2) 应核查云平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等是否有效;
 - 3) 应核查不同云服务客户间访问控制规则和访问控制策略是否有效;
 - 4) 应核查云服务客户业务系统不同区域间访问控制规则和访问控制策略是否有效;
 - 5) 应测试虚拟化网络边界访问控制设备,验证是否可以正确拒绝违反访问控制规则的非法访问。
- d) 单元判定:如果 1)~5)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

9.2.2.2.3 测评单元 (L4-NCS2-11)

该测评单元包括以下要求:

- a) 测评指标:应保证当虚拟机迁移时,访问控制策略随其迁移;
- b) 测评对象:虚拟机、虚拟机迁移记录和相关配置;
- c) 测评实施包括以下内容:
 - 1) 应核查虚拟机迁移时访问控制策略随之迁移的措施或手段;
 - 2) 应核查虚拟机迁移记录及相关配置,查看虚拟机迁移后访问控制策略是否部署;
 - 3) 应测试虚拟机迁移,验证访问控制措施是否随其迁移。
- d) 单元判定:如果 1)~3)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

9.2.2.2.4 测评单元 (L4-NCS2-12)

该测评单元包括以下要求:

- a) 测评指标:应允许云服务客户设置不同虚拟机之间的访问控制策略;
- b) 测评对象:云服务商管理平台、云服务客户管理系统和虚拟化网络边界访问控制设备;
- c) 测评实施包括以下内容:
 - 1) 应核查云服务商的云管理平台等是否允许云服务客户设置不同虚拟机间访问控制策略;
 - 2) 应核查云服务商的云管理平台是否存在不同虚拟机间的访问控制管理模块,是否开启该访问控制功能;
 - 3) 应核查云服务客户管理系统,不同虚拟机间访问控制策略是否安全;
 - 4) 应测试虚拟化网络边界访问控制设备是否可以正确拒绝违反虚拟机间访问控制策略的非法访问。
- d) 单元判定:如果 1)、2)、4)或 3)、4)为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

9.2.2.2.5 测评单元 (L4-NCS2-13)

该测评单元包括以下要求:

- a) 测评指标:应在不同等级的网络区域边界部署访问控制机制,设置访问控制规则;
- b) 测评对象:网闸、防火墙、路由器和交换机等提供访问控制功能的设备;
- c) 测评实施包括以下内容:
 - 1) 应核查不同安全等级网络区域边界的访问控制规则和访问控制策略是否有效;
 - 2) 应测试不同安全等级的网络区域间进行非法访问时,是否可以正确拒绝该非法访问。
- d) 单元判定:如果 1)~2)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

9.2.2.3 入侵防范

9.2.2.3.1 测评单元（L4-NCS2-14）

该测评单元包括以下要求：

- a) 测评指标：应能检测到并告警后及时处理云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；
- b) 测评对象：网络入侵检测系统、入侵保护系统、国家认可的相关机制和入侵防范措施；
- c) 测评实施包括以下内容：
 - 1) 应核查是否有专门设备对网络入侵进行防范，核查网络入侵防范规则库的升级方式；
 - 2) 应核查网络入侵检测系统、入侵保护系统或机制，当采用网络入侵防范机制时所采取的机制是否已被测试是安全的（如第三方测试报告），核查入侵检测系统、入侵保护系统或机制的规则库是否为最新；
 - 3) 应测试网络入侵检测系统、入侵保护系统或机制，当采用网络入侵防范机制时所采取的机制是否已被测试是安全的（如第三方测试报告），验证入侵检测系统、入侵保护系统或机制对异常流量和未知威胁的监控策略是否有效（如模拟产生攻击动作，验证网络入侵检测系统、入侵保护系统的反应，是否能记录攻击类型、攻击时间、攻击流量）；
 - 4) 应核查系统是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能、报警功能；
 - 5) 应核查是否具有对 SQL 注入、跨站脚本等攻击进行检测发现的能力；
 - 6) 应具有对恶意虚拟机，如具有恶意行为、过分占用计算资源和带宽资源等的虚拟机，进行检测的能力；
 - 7) 应核查云管理平台等对云服务客户攻击的防范措施，核查对云服务客户的网络攻击行为的记录情况，记录应包括攻击类型、攻击时间、攻击流量等；
 - 8) 应测试网络入侵检测系统、入侵保护系统或机制，验证其云服务客户网络攻击报警报警策略是否有效（如模拟产生攻击动作，验证网络入侵检测系统、入侵保护系统是否能实时报警）；
 - 9) 应对云平台内部发起的恶意攻击或恶意对外连接的行为进行限制，核查是否对内部行为进行监控且保存相关日志记录；
 - 10) 应通过对外攻击发生器伪造对外攻击行为，核查云租的网络攻击的日志记录，确认是否正确记录到相应攻击行为，攻击行为日志记录是否包含攻击类型、攻击时间、攻击者 IP、攻击流量规模等；
 - 11) 应核查运行虚拟机监控器（VMM）和云管理平台软件的物理主机，核查其安全加固手段是否能够应对虚拟化共享带来的安全漏洞。
- d) 单元判定：如果 1) -11) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.3.2 测评单元（L4-NCS2-15）

该测评单元包括以下要求：

- a) 测评指标：应能检测到并告警后及时处理对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；
- b) 测评对象：网络入侵检测系统、入侵保护系统、国家认可的相关机制和入侵防范措施；
- c) 测评实施包括以下内容：
 - 1) 应核查是否有专门设备对虚拟网络节点的网络攻击行为进行防范，核查网络入侵防范规则库的升级方式；

- 2) 应核查网络入侵检测系统、入侵保护系统或机制，当对虚拟网络节点采用网络入侵防范机制时所采取的机制是否已被测试是安全的（如第三方测试报告），核查入侵检测系统、入侵保护系统或机制的规则库是否为最新；
- 3) 应测试网络入侵检测系统、入侵保护系统或机制，当对虚拟网络节点采用网络入侵防范机制时所采取的机制是否已被测试是安全的（如第三方测试报告），验证入侵检测系统、入侵保护系统或机制对异常流量和未知威胁的监控策略是否有效（如模拟产生攻击动作，验证网络入侵检测系统、入侵保护系统的反应，是否能记录攻击类型、攻击时间、攻击流量）。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.3.3 测评单元（L4-NCS2-16）

该测评单元包括以下要求：

- a) 测评指标：应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量，并进行告警；
- b) 测评对象：虚拟机、宿主机、入侵检测系统和入侵保护系统；
- c) 测评实施包括以下内容：
 - 1) 应核查系统是否具备虚拟机与宿主机之间、虚拟机与虚拟机之间的异常流量、大规模攻击流量、高级持续性攻击的检测功能和告警功能；
 - 2) 应核查网络入侵检测系统、入侵保护系统的告警策略和告警记录；
 - 3) 应测试网络入侵检测系统、入侵保护系统，验证其对异常流量和未知威胁的监控策略是否有效（如模拟产生攻击动作，验证网络入侵检测系统、入侵保护系统是否能记录攻击类型、攻击时间、攻击流量）。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.3.4 测评单元（L4-NCS2-17）

该测评单元包括以下要求：

- a) 测评指标：应向云服务客户提供互联网发布内容监测功能，便于云服务客户对其发布内容中的有害信息进行实时监测并告警后及时处理；
- b) 测评对象：安全服务、安全组件、监测信息和有害信息过滤规则；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务商安全服务是否可为云服务客户提供互联网发布内容监测功能；
 - 2) 应核查云服务客户能否对其发布到互联网的有害信息进行实时监测并告警后及时处理；
 - 3) 应核查云服务客户对其发布到互联网有害信息的实时监测情况、历史告警信息和告警处理记录；
 - 4) 应核查云服务客户设置的有害信息过滤规则，查看过滤规则是否可对常见有害信息进行过滤。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.4 安全审计

9.2.2.4.1 测评单元（L4-NCS2-18）

该测评单元包括以下要求：

- a) 测评指标：应对云服务商和云服务客户远程管理时执行特权命令进行审计，至少包括虚拟机删除、虚拟机重启；
- b) 测评对象：边界网络设备、网络虚拟化设备和相关审计数据；
- c) 测评实施包括以下内容：
 - 1) 应核查对云服务商和云服务客户远程管理时执行的远程特权命令后是否有相关审计记录；
 - 2) 当云服务商采用第三方运维时，应核查第三方运维方是否向云服务商提供审计数据，或云服务商是否可采取措施收集相关审计数据；
 - 3) 应核查边界网络设备、网络虚拟化设备远程执行特权命令的限制措施，核查是否对远程执行特权命令的行为进行安全审计，至少包括虚拟机删除、虚拟机重启；
 - 4) 应测试云服务商或云服务客户远程删除或重启虚拟机后，是否有产生相应审计记录。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.4.2 测评单元（L4-NCS2-19）

该测评单元包括以下要求：

- a) 测评指标：应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；
- b) 测评对象：审计数据收集系统、收集设备、云管理平台 and 审计数据；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务商审计数据收集系统或设备是否根据云服务商和云服务客户的职责划分，实现各自控制部分审计数据的收集；
 - 2) 如果云服务客户授权云服务商收集部分云服务客户控制的审计数据，应核查云服务商是否在不影响其他云服务客户安全的前提下将云服务客户审计数据提供给云服务客户；
 - 3) 应核查云服务商审计数据是否不包括云服务客户控制部分的审计数据。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.2.5 集中管控

9.2.2.5.1 测评单元（L4-NCS2-20）

该测评单元包括以下要求：

- a) 测评指标：应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测；
- b) 测评对象：云平台和监控信息汇集接口；
- c) 测评实施包括以下内容：
 - 1) 应核查云平台是否为虚拟化网络、虚拟机、虚拟化安全设备等运行状况监控信息的汇集提供了接口，并实现集中监控；
 - 2) 应核查虚拟化网络、虚拟机、虚拟化安全设备等监控信息汇集接口配置或参数，核查集中监控措施和记录。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3 设备和计算安全

9.2.3.1 身份鉴别

9.2.3.1.1 测评单元（L4-ECS2-01）

该测评单元包括以下要求：

- a) 测评指标：应在网络策略控制器和网络设备（或设备代理）之间建立通信时验证身份；
- b) 测评对象：网络管理员、网络策略控制器和网络设备（代理设备）；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络管理员是否在网络策略控制器和网络设备（或设备代理）之间建立通信时建立身份验证机制；
 - 2) 应核查网络策略控制器和网络设备（或设备代理）之间的身份验证机制；
 - 3) 应对网络策略控制器和网络设备（代理设备）进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）对网络设备进行渗透测试，验证网络设备防护能力是否符合要求，是否在网络策略控制器和网络设备（或设备代理）之间建立通信时建立身份验证机制。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.1.2 测评单元（L4-ECS2-02）

该测评单元包括以下要求：

- a) 测评指标：当进行远程管理时，管理终端和云计算平台边界设备之间应建立双向身份验证机制；
- b) 测评对象：管理终端和云计算平台；
- c) 测评实施包括以下内容：
 - 1) 应核查当进行远程管理时，是否建立双向身份验证机制；
 - 2) 应对管理终端和云计算平台进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）对网络设备进行渗透测试，验证网络设备防护能力是否符合要求，是否在管理终端和云计算平台之间建立双向身份验证机制。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.2 访问控制

9.2.3.2.1 测评单元（L4-ECS2-03）

该测评单元包括以下要求：

- a) 测评指标：应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；
- b) 测评对象：云平台、数据库、相关授权文档和管理文档；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户数据管理权限授权流程、授权方式、授权内容；
 - 2) 应核查云计算平台是否具有云服务客户数据的管理权限，如果具有，核查相关授权证明及数据管理权限保护措施；
 - 3) 应测试数据库系统，验证云服务商是否不能对云服务客户非授权数据进行管理。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.2.2 测评单元（L4-ECS2-04）

该测评单元包括以下要求：

- a) 测评指标：提供云计算平台管理用户权限分离机制，为网络管理员、系统管理员建立不同账户并分配相应的权限；
- b) 测评对象：云管理平台和相关文档；
- c) 测评实施包括以下内容：
 - 1) 应核查云平台运维管理员和云服务运营管理员的权限是否分离，网络管理员、系统管理员是否建立不同账户并分配相应的权限；
 - 2) 应核查云服务商的云管理平台是否提供云平台管理用户权限分离机制，是否能为网络管理、系统管理建立不同账户并分配相应的权限。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.3 安全审计

9.2.3.3.1 测评单元（L4-ECS2-05）

该测评单元包括以下要求：

- a) 测评指标：应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计；
- b) 测评对象：安全审计策略、审计设备和审计数据；
- c) 测评实施包括以下内容：
 - 1) 应核查安全审计配置是否能够保证云服务商对云服务客户系统和数据的操作（如增、删、改、查等操作）可被云服务客户审计；
 - 2) 应核查是否支持云服务客户部署第三方安全审计设备，保证云服务商对云服务客户系统和数据的操作可被租户审计；
 - 3) 应核查云服务商与云服务客户收集的审计数据，查看云服务商对云服务客户系统和数据的操作是否可被云服务客户审计。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.4 入侵防范

9.2.3.4.1 测评单元（L4-ECS2-06）

该测评单元包括以下要求：

- a) 测评指标：应能检测虚拟机之间的资源隔离失效，并进行告警；
- b) 测评对象：系统管理员、服务器、宿主机、虚拟机、操作系统、数据库系统、虚拟机监视器和云平台；
- c) 测评实施包括以下内容：
 - 1) 应核查服务器、宿主机及虚拟机，虚拟机监视器，云平台是否采取措施对不同虚拟机的 CPU、内存和磁盘资源进行隔离，是否实现不同云服务客户自有数据库之间的隔离；是否采取措施能够检测到虚拟机之间的资源隔离失效，并进行告警；
 - 2) 应访谈系统管理员是否采取措施对不同虚拟机资源进行了安全隔离，是否采取措施能够检测到虚拟机之间的资源隔离失效，并进行告警。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.4.2 测评单元（L4-ECS2-07）

该测评单元包括以下要求：

- a) 测评指标：应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；
- b) 测评对象：系统管理员、服务器、宿主机、虚拟机、操作系统、数据库系统、虚拟机监视器和云平台；
- c) 测评实施：应核查服务器、宿主机及虚拟机，操作系统，数据库系统，虚拟机监视器，云平台是否能够检测到非授权新建虚拟机或者重新启用虚拟机，并进行告警；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

9.2.3.4.3 测评单元（L4-ECS2-08）

该测评单元包括以下要求：

- a) 测评指标：应能够检测恶意代码感染及在虚拟机间蔓延的情况，并告警后及时处理；
- b) 测评对象：服务器、宿主机、虚拟机、终端、虚拟机监视器和云平台；
- c) 测评实施包括以下内容：
 - 1) 应核查服务器、宿主机、虚拟机、终端、虚拟机监视器、云平台是否建立恶意代码传播路径追踪机制，是否可以检测查看恶意代码的感染情况，并告警后及时处理。
 - 2) 应核查服务器、宿主机、虚拟机、终端，虚拟机监视器，云平台是否能够检测恶意代码感染及在虚拟机间蔓延的情况，是否能够检测出虚拟机的恶意行为，并告警后及时处理。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.5 资源控制

9.2.3.5.1 测评单元（L4-ECS2-09）

该测评单元包括以下要求：

- a) 测评指标：应屏蔽虚拟资源故障，某个虚拟机宕机后不影响虚拟机监视器及其他虚拟机；
- b) 测评对象：资源控制相关平台和云平台；
- c) 测评实施包括以下内容：
 - 1) 应核查资源控制相关平台所采取的屏蔽虚拟资源故障措施、相关虚拟机故障记录，核查是否不存在虚拟机崩溃后影响虚拟机监视器及其他虚拟机的历史记录；
 - 2) 应核查云平台所采取的屏蔽虚拟资源故障的技术手段是否能在某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.5.2 测评单元（L4-ECS2-10）

该测评单元包括以下要求：

- a) 测评指标：应对物理资源和虚拟资源按照策略做统一管理调度与分配；
- b) 测评对象：运营管理平台、资源调度平台和云管理平台；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户的运营管理平台或资源调度平台的资源调度策略、资源调度分配情况；

- 2) 应核查云服务商云管理平台所提供策略能否对物理资源和虚拟资源做统一管理调度与分配。
- d) 单元判定：如果 1)-2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.5.3 测评单元 (L4-ECS2-11)

该测评单元包括以下要求：

- a) 测评指标：应确保云计算平台具有虚拟机内存隔离措施；
- b) 测评对象：云管理平台和虚拟机监视器；
- c) 测评实施包括以下内容：
 - 1) 应核查云管理平台和虚拟机监视器的计算资源分配情况、资源分配的审计记录或告警记录是否不存在内存资源过量占用警告；
 - 2) 应核查云计算平台和虚拟机监视器的虚拟机内存隔离措施或机制。
- d) 单元判定：如果 1)-2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.5.4 测评单元 (L4-ECS2-12)

该测评单元包括以下要求：

- a) 测评指标：应确保云服务客户的虚拟机使用独占的内存空间；
- b) 测评对象：云管理平台和虚拟机监视器；
- c) 测评实施包括以下内容：
 - 1) 应核查内存空间分配策略和内存空间分配情况、内存隔离相关审计记录或告警记录是否不存在内存资源过量占用警告，核查是否为云服务客户业务应用系统的虚拟机分配可独占内存空间；
 - 2) 应核查云服务客户虚拟机内存隔离措施或机制是否有效。
- d) 单元判定：如果 1)-2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.5.5 测评单元 (L4-ECS2-13)

该测评单元包括以下要求：

- a) 测评指标：应对虚拟机的网络接口的带宽进行设置，并进行监测；
- b) 测评对象：云管理平台或其他安全组件；
- c) 测评实施包括以下内容：
 - 1) 应核查云管理平台或其他安全组件是否能对虚拟机网络接口带宽进行设置，是否能对其进行监控；
 - 2) 应核查云管理平台上虚拟机的网络接口带宽的配置及参数、带宽监控记录。
- d) 单元判定：如果 1)-2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.6 镜像和快照保护

9.2.3.6.1 测评单元 (L4-ECS2-14)

该测评单元包括以下要求：

- a) 测评指标：应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
- b) 测评对象：云管理平台、虚拟机监视器和虚拟机镜像文件；
- c) 测评实施包括以下内容：
 - 1) 应核查虚拟机监视器是否有对镜像文件定期进行有效性验证的记录；
 - 2) 应核查虚拟机监视器，云管理平台是否提供有效的虚拟机镜像和快照文件管理机制，虚拟机是否能够及时被备份和快照，以及是否准确地恢复到所需还原点；
 - 3) 应核查虚拟机监视器，云管理平台是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。
- d) 单元判定：如果 1)–3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.6.2 测评单元（L4-ECS2-15）

该测评单元包括以下要求：

- a) 测评指标：应针对重要业务系统提供加固的操作系统镜像；
- b) 测评对象：云管理平台、虚拟机监视器和虚拟机镜像文件；
- c) 测评实施：应核查虚拟机监视器，云管理平台是否对生成的虚拟机镜像进行必要的加固措施，如关闭不必要的端口、服务及进行安全加固配置；
- d) 单元判定：如果以上测评实施内容均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.3.6.3 测评单元（L4-ECS2-16）

该测评单元包括以下要求：

- a) 测评指标：应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；
- b) 测评对象：云管理平台、虚拟机监视器和虚拟机镜像文件；
- c) 测评实施：应核查虚拟机监视器，云管理平台是否对虚拟机镜像或快照中的敏感资源，通过加密、访问控制、权限控制等技术手段进行保护，防止可能存在的针对快照的非法访问；
- d) 单元判定：如果以上测评实施内容均为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

9.2.4 应用和数据安全

9.2.4.1 数据完整性

9.2.4.1.1 测评单元（L4-ADS2-01）

该测评单元包括以下要求：

- a) 测评指标：应使用校验码或密码技术确保虚拟机迁移过程中，重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；
- b) 测评对象：虚拟机；
- c) 测评实施包括以下内容：
 - 1) 应核查虚拟资源迁移过程中采用的数据完整性保障措施及恢复措施；
 - 2) 应核查在虚拟资源迁移过程中，是否采取校验码或密码技术等措施保证虚拟资源数据及重要数据的完整性，并在检测到完整性受到破坏时是否采取必要的恢复措施。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.4.2 数据保密性

9.2.4.2.1 测评单元 (L4-ADS2-02)

该测评单元包括以下要求：

- a) 测评指标：应使用密码技术确保虚拟机迁移过程中，重要数据的保密性，防止在迁移过程中的重要数据泄露；
- b) 测评对象：系统管理数据（如镜像文件、快照）、鉴别信息和重要业务数据（如用户隐私数据）；
- c) 测评实施包括以下内容：
 - 1) 应核查虚拟机迁移过程中重要数据的保密措施是否能够有效防止迁移过程中重要数据的泄露；
 - 2) 应核查是否采取加密或其他保护措施实现系统管理数据（如镜像文件、快照），鉴别信息和重要业务数据（如用户隐私数据）来保证虚拟机迁移过程中重要数据的保密性，防止迁移过程中重要数据的泄露；
 - 3) 应核查是否使用密码技术确保虚拟机迁移过程中，重要数据的保密性。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.4.2.2 测评单元 (L4-ADS2-03)

该测评单元包括以下要求：

- a) 测评指标：应支持云服务客户部署密钥管理解决方案，确保云服务客户自行实现数据的加解密过程；
- b) 测评对象：密钥管理解决方案；
- c) 测评实施包括以下内容：
 - 1) 当云服务客户已部署密钥管理解决方案，应核查密钥管理解决方案是否能确保云服务客户自行实现数据的加解密过程；
 - 2) 应核查云服务商支持云服务客户部署密钥管理解决方案所采取的技术手段或管理措施是否能确保云服务客户自行实现数据的加解密过程。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.4.3 数据备份恢复

9.2.4.3.1 测评单元 (L4-ADS2-04)

该测评单元包括以下要求：

- a) 测评指标：应提供查询云服务客户数据及备份存储位置的方式；
- b) 测评对象：云管理平台、云平台和相关技术文档；
- c) 测评实施包括以下内容：
 - 1) 应核查云管理平台或云平台为云服务客户提供数据及备份存储位置的查询记录；
 - 2) 应核查云服务商是否为云服务客户提供数据及备份存储位置查询的接口或其他技术、管理手段。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.4.3.2 测评单元 (L4-ADS2-05)

该测评单元包括以下要求：

- a) 测评指标：云服务客户应在本地保存其业务数据的备份；
- b) 测评对象：虚拟机、虚拟机监视器和云平台；
- c) 测评实施包括以下内容：应核查是否提供备份措施保证云服务客户可以在本地保存其业务数据；
- d) 单元判定：如果以上测评实施内容均为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

9.2.4.3.3 测评单元 (L4-ADS2-06)

该测评单元包括以下要求：

- a) 测评指标：应保证不同云服务客户的审计数据隔离存放；
- b) 测评对象：云服务客户审计数据；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户是否不能访问其他云服务客户审计数据；
 - 2) 应核查是否采取云服务客户审计数据隔离存放措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.4.3.4 测评单元 (L4-ADS2-07)

该测评单元包括以下要求：

- a) 测评指标：应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程；
- b) 测评对象：相关技术措施和手段；
- c) 测评实施包括以下内容：
 - 1) 应核查相关技术手段是否能保障云服务客户将业务系统及数据迁移到其他云计算平台和本地系统；
 - 2) 应核查云服务商是否提供措施、手段或人员协助云服务客户完成迁移过程。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.4.3.5 测评单元 (L4-ADS2-08)

该测评单元包括以下要求：

- a) 测评指标：云服务商的云存储服务应确保云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；
- b) 测评对象：云存储、相关技术措施和手段；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户数据副本存储方式，核查是否存在若干个可用的副本；
 - 2) 应核查各副本内容保持一致的技术措施或手段是否能保障云服务客户将业务系统及数据迁移到其他云计算平台和本地系统；
 - 3) 应核查云服务商是否提供措施、手段或人员协助云服务客户完成迁移过程。

- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.4.4 剩余信息保护

9.2.4.4.1 测评单元 (L4-ADS2-09)

该测评单元包括以下要求：

- a) 测评指标：应保证虚拟机所使用的内存和存储空间回收时得到完全清除；
- b) 测评对象：系统管理员、虚拟机、虚拟机监视器系统、云管理平台系统、操作系统技术开发手册或产品检测报告、数据库系统技术开发手册和产品检测报告；
- c) 测评实施包括以下内容：
 - 1) 应核查资源抽象层用户的鉴别信息存储空间在回收时的数据清除策略；
 - 2) 应核查系统和数据库系统技术开发手册或产品检测报告，查看用户的鉴别信息存储空间回收时是否得到完全清除；
 - 3) 应核查操作系统和数据库系统技术开发手册或产品检测报告，查看文件、目录和数据库记录等资源所在的存储空间回收时是否得到完全清除；
 - 4) 应核查虚拟机监视器和云管理平台内的文件、目录、数据库记录和虚拟资源等所在的存储空间回收时是否得到完全清除；
 - 5) 应核查虚拟机的内存和存储空间回收时，是否得到完全清除；
 - 6) 应核查在迁移或删除虚拟机后，数据以及备份数据（如镜像文件、快照文件等）是否已清理。
- d) 单元判定：如果 1) -6) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.4.4.2 测评单元 (L4-ADS2-10)

该测评单元包括以下要求：

- a) 测评指标：云服务客户删除业务应用数据时，云计算平台应确保云存储中所有副本被删除；
- b) 测评对象：云存储和云计算平台；
- c) 测评实施包括以下内容：
 - 1) 应核查云平台中云服务客户业务应用数据备份方式和备份管理方式，当云服务客户删除业务应用数据时，核查是否支持所有副本删除；
 - 2) 应核查云计算平台，当云服务客户删除业务应用数据时，云存储中所有副本是否被删除。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.4.5 个人信息保护

9.2.4.5.1 测评单元 (L4-ADS2-11)

该测评单元包括以下要求：

- a) 测评指标：应确保云服务客户账户信息、鉴别信息、系统信息存储于中国境内；
- b) 测评对象：数据库服务器、数据存储设备和管理文档记录；
- c) 测评实施包括以下内容：
 - 1) 应核查云服务客户账户信息、鉴别信息、系统信息所在的服务器及数据存储设备是否存储于中国境内；

- 2) 应核查相关管理文档或记录,核查云服务客户账户信息、鉴别信息、系统信息及其备份是否存储于中国境内。
- d) 单元判定:如果 1)-2)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

9.2.5 安全建设管理

9.2.5.1 云服务商选择

9.2.5.1.1 测评单元 (L4-CMS2-01)

该测评单元包括以下要求:

- a) 测评指标:应选择安全合规的云服务商,其所提供的云平台应为其所承载的业务应用系统提供相应等级的安全保护能力;
- b) 测评对象:系统建设负责人、安全责任合同书、保密协议和服务合同;
- c) 测评实施包括以下内容:
 - 1) 应访谈系统建设负责人是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云平台及云服务商;
 - 2) 应核查云服务商提供的相关服务合同是否明确其云平台具有与所承载的业务应用系统相应或高于的安全保护能力。
- d) 单元判定:如果 1)-2)均为肯定,则符合本单元测评指标要求,否则不符合或部分符合本单元测评指标要求。

9.2.5.1.2 测评单元 (L4-CMS2-02)

该测评单元包括以下要求:

- a) 测评指标:应在服务水平协议中规定云服务的各项服务内容和具体技术指标;
- b) 测评对象:服务水平协议;
- c) 测评实施包括以下内容:
 - 1) 应核查服务水平协议是否规定了云服务的各项服务内容和具体指标、服务期限、双方签字或盖章等;
- d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

9.2.5.1.3 测评单元 (L4-CMS2-03)

该测评单元包括以下要求:

- a) 测评指标:应在服务水平协议中规定云服务商的权限与责任,包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等;
- b) 测评对象:服务水平协议;
- c) 测评实施:应核查服务水平协议中是否规范了安全服务商和云服务供应商的权限与责任,包括管理范围、职责划分、访问授权、隐私保护、行为准则等;
- d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

9.2.5.1.4 测评单元 (L4-CMS2-04)

该测评单元包括以下要求:

- a) 测评指标：应在服务水平协议中规定服务合约到期时，完整地返还云服务客户信息，并承诺相关信息在云计算平台上清除；
- b) 测评对象：服务水平协议；
- c) 测评实施包括以下内容：
 - 1) 应核查服务水平协议是否明确服务合约到期时，云服务商完整地返还云服务客户信息，并承诺相关信息在云平台上清除；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

9.2.5.1.5 测评单元（L4-CMS2-05）

该测评单元包括以下要求：

- a) 测评指标：应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据和业务系统的相关重要信息；
- b) 测评对象：安全责任合同书、保密协议和服务合同；
- c) 测评实施：应核查安全责任合同书、保密协议或服务合同是否包含对云服务商不得泄露云服务客户数据和业务系统的相关重要信息的要求；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

9.2.5.1.6 测评单元（L4-CMS2-06）

该测评单元包括以下要求：

- a) 测评指标：应对可能接触到云服务客户数据的员工进行背景调查，并签署保密协议；
- b) 测评对象：系统建设负责人、调查文件或调查报告、保密协议；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统建设负责人是否与云服务商可接触到云服务客户数据的员工签订保密协议，并进行背景调查；
 - 2) 应核查员工保密协议是否明确相关保密义务；
 - 3) 应核查背景调查报告是否明确人员相关背景调查情况。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.5.2 供应链管理

9.2.5.2.1 测评单元（L4-CMS2-07）

该测评单元包括以下要求：

- a) 测评指标：应确保供应商的选择符合国家有关规定；
- b) 测评对象：系统建设负责人；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统建设负责人云服务商的选择是否符合国家的有关规定；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

9.2.5.2.2 测评单元（L4-CMS2-08）

该测评单元包括以下要求：

- a) 测评指标：应确保供应链安全事件信息或威胁信息能够及时传达到云服务客户；
- b) 测评对象：系统建设负责人、供应链安全事件或威胁报告；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统建设负责人云服务商供应商是否及时传达安全事件或威胁信息；
 - 2) 应核查供应链安全事件或威胁报告是否明确相关事件信息或威胁信息。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.5.2.3 测评单元（L4-CMS2-09）

该测评单元包括以下要求：

- a) 测评指标：应保证供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取有关措施对风险进行控制；
- b) 测评对象：供应商重要变更记录、安全风险评估报告和风险预案；
- c) 测评实施：应核查安全风险评估报告和风险预案，确认对每次供应商的重要变更都进行评估与风险预案设计；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

9.2.6 安全运维管理

9.2.6.1 云计算环境管理

9.2.6.1.1 测评单元（L4-MMS2-01）

该测评单元包括以下要求：

- a) 测评指标：云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定；
- b) 测评对象：运维设备、运维地点、运维记录和相关管理文档；
- c) 测评实施包括以下内容：
 - 1) 应核查运维地点是否位于中国境内，是否不存在从境外对境内云计算平台实施远程运维的设备、地点和相关内容；
 - 2) 应核查云计算平台远程运维记录中境外对境内云计算平台实施运维操作是否遵循国家相关规定。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.6.1.2 测评单元（L4-MMS2-02）

该测评单元包括以下要求：

- a) 测评指标：云计算平台运维过程产生的配置数据、日志信息等存储于中国境内，如需出境应遵循国家相关规定；
- b) 测评对象：云计算平台运行管理设计文档和管理文档；
- c) 测评实施包括以下内容：
 - 1) 应核查云计算平台运维过程产生的配置数据、日志信息等是否存储于中国境内；
 - 2) 对于有出境需求的配置数据和日志信息，应核查数据出境是否遵循国家相关规定。

- d) 单元判定：如果 1) 或 2) 为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.3 移动互联安全测评扩展要求

9.3.1 物理和环境安全

9.3.1.1 无线接入点的物理位置

9.3.1.1.1 测评单元（L4-PES3-01）

该测评单元包括以下要求：

- a) 测评指标：应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰；
- b) 测评对象：无线接入设备；
- c) 测评实施包括以下内容：
 - 1) 应核查物理位置与无线信号的覆盖范围；
 - 2) 应测试无线信号的覆盖范围并测试在一定范围内是否可以进行电磁干扰。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.3.2 网络和通信安全

9.3.2.1 边界防护

9.3.2.1.1 测评单元（L4-NCS3-01）

该测评单元包括以下要求：

- a) 测评指标：应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备；
- b) 测评对象：无线接入网关设备；
- c) 测评实施：应核查有线网络与无线网络边界之间是否部署无线接入网关设备；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.2.2 访问控制

9.3.2.2.1 测评单元（L4-NCS3-02）

该测评单元包括以下要求：

- a) 测评指标：无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证；
- b) 测评对象：无线接入设备；
- c) 测评实施：应核查是否开启接入认证功能，是否采用认证服务器或国家密码管理机构批准的密码模块进行认证；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.2.3 入侵防范

9.3.2.3.1 测评单元（L4-NCS3-03）

该测评单元包括以下要求：

- a) 测评指标：应能够检测、记录、定位非授权无线接入设备；
- b) 测评对象：入侵防范设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否能够检测、记录、定位非授权无线接入设备；
 - 2) 应测试是否能够检测、记录、定位非授权无线接入设备。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.3.2.3.2 测评单元（L4-NCS3-04）

该测评单元包括以下要求：

- a) 测评指标：应能够对非授权移动终端接入的行为进行检测、记录、定位并阻断；
- b) 测评对象：入侵防范设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否能够检测、记录、定位并阻断非授权移动终端接入；
 - 2) 应测试是否能够检测、记录、定位并阻断非授权移动终端接入。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.3.2.3.3 测评单元（L4-NCS3-05）

该测评单元包括以下要求：

- a) 测评指标：应具备对针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位；
- b) 测评对象：入侵防范设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否能够对网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位；
 - 2) 应核查规则库版本，查看其规则库是否及时更新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.3.2.3.4 测评单元（L4-NCS3-06）

该测评单元包括以下要求：

- a) 测评指标：应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；
- b) 测评对象：入侵防范设备；
- c) 测评实施：应核查是否能够检测无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.2.3.5 测评单元（L4-NCS3-07）

该测评单元包括以下要求：

- a) 测评指标：应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等；
- b) 测评对象：无线接入设备和无线接入网关设备；

- c) 测评实施：应核查是否关闭了 SSID 广播、WEP 认证等存在风险的功能；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.2.3.6 测评单元（L4-NCS3-08）

该测评单元包括以下要求：

- a) 测评指标：应禁止多个 AP 使用同一个鉴别密钥；
- b) 测评对象：无线接入设备；
- c) 测评实施：应核查是否分别使用了不同的鉴别密钥；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.3 设备和计算安全

9.3.3.1 移动终端管控

9.3.3.1.1 测评单元（L4-ECS3-01）

该测评单元包括以下要求：

- a) 测评指标：应保证移动终端安装、注册并运行终端管理客户端软件；
- b) 测评对象：移动终端和移动终端管理系统；
- c) 测评实施：应核查移动终端管理系统，查看移动终端客户端软件的安装、注册与管理策略；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.3.1.2 测评单元（L4-ECS3-02）

该测评单元包括以下要求：

- a) 测评指标：移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等；
- b) 测评对象：移动终端和移动终端管理系统；
- c) 测评实施包括以下内容：
 - 1) 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等安全策略；
 - 2) 应测试是否能够对移动终端进行远程锁定和远程擦除等。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.3.3.2 移动应用管控

9.3.3.2.1 测评单元（L4-ECS3-03）

该测评单元包括以下要求：

- a) 测评指标：应具有选择应用软件安装、运行的功能；
- b) 测评对象：移动终端管理客户端；
- c) 测评实施：应核查是否具有选择应用软件安装、运行的功能；

- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.3.2.2 测评单元（L4-ECS3-04）

该测评单元包括以下要求：

- a) 测评指标：应具有软件白名单功能，应能根据白名单控制应用软件安装、运行；
- b) 测评对象：移动终端管理客户端；
- c) 测评实施包括以下内容：
 - 1) 应核查是否具有软件白名单功能；
 - 2) 应测试使用白名单控制应用软件安装、运行。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.3.3.2.3 测评单元（L4-ECS3-05）

该测评单元包括以下要求：

- a) 测评指标：应具有应用软件权限控制功能，应能控制应用软件对移动终端中资源访问；
- b) 测评对象：移动终端管理客户端；
- c) 测评实施包括以下内容：
 - 1) 应核查是否具有应用软件权限控制功能；
 - 2) 应测试是否可以对移动终端中资源的访问进行限制。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.3.3.2.4 测评单元（L4-ECS3-06）

该测评单元包括以下要求：

- a) 测评指标：应只允许系统管理者指定证书签名的应用软件安装和运行；
- b) 测评对象：移动终端管理客户端；
- c) 测评实施：应核查允许使用的签名证书，且证书是否由系统管理者指定；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.3.2.5 测评单元（L4-ECS3-07）

该测评单元包括以下要求：

- a) 测评指标：应具有接受移动终端管理服务端推送的移动应用软件管理策略，并根据该策略对软件实施管控的能力；
- b) 测评对象：移动终端管理客户端；
- c) 测评实施：应核查是否具有接受移动终端管理服务端远程管控的能力；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.3.3 资源控制

9.3.3.3.1 测评单元（L4-ECS3-08）

该测评单元包括以下要求：

- a) 测评指标：应保证移动终端只用于处理指定业务；
- b) 测评对象：移动终端；
- c) 测评实施：应核查是否为专用终端，仅处理访问指定业务；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.3.3.2 测评单元（L4-ECS3-09）

该测评单元包括以下要求：

- a) 测评指标：应限制用户或进程对移动终端系统资源的最大使用限度，防止移动终端被提权；
- b) 测评对象：移动终端；
- c) 测评实施：应核查是否可以对用户或进程等可访问资源进行限定，是否可以防止移动终端被提权；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.4 安全建设管理

9.3.4.1 移动应用软件采购

9.3.4.1.1 测评单元（L4-CMS3-01）

该测评单元包括以下要求：

- a) 测评指标：应保证移动终端安装、运行的应用软件来自系统管理者指定证书签名或指定分发渠道；
- b) 测评对象：安全管理员；
- c) 测评实施：应访谈安全管理员，移动应用软件是否采用系统管理者指定的证书签名或使用指定的分发渠道；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.4.1.2 测评单元（L4-CMS3-02）

该测评单元包括以下要求：

- a) 测评指标：应保证移动终端安装、运行的移动应用软件由经系统管理者指定的开发者开发；
- b) 测评对象：安全管理员；
- c) 测评实施：应访谈安全管理员，移动应用软件是否由经系统管理者指定的开发者开发；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.4.2 移动应用软件开发

9.3.4.2.1 测评单元（L4-CMS3-01）

该测评单元包括以下要求：

- a) 测评指标：应要求对移动业务应用软件开发进行资格审查；
- b) 测评对象：系统建设负责人；

- c) 测评实施：应访谈系统建设负责人，是否对开发者进行资格审查；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.4.2.2 测评单元（L4-CMS3-02）

该测评单元包括以下要求：

- a) 测评指标：应确保开发移动业务应用程序的签名证书合法性；
- b) 测评对象：软件的签名证书；
- c) 测评实施：应核查开发移动业务应用程序的签名证书是否具有合法性；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.5 安全运维管理

9.3.5.1 配置管理

9.3.5.1.1 测评单元（L4-MMS3-01）

该测评单元包括以下要求：

- a) 测评指标：应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别；
- b) 测评对象：记录表单类文档；
- c) 测评实施：应核查记录表单类文档，是否建立无线接入设备和合法移动终端配置库，并通过配置库识别非法设备；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.4 物联网安全测评扩展要求

9.4.1 物理和环境安全

9.4.1.1 感知节点设备物理防护

9.4.1.1.1 测评单元（L4-PES4-01）

该测评单元包括以下要求：

- a) 测评指标：感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；
- b) 测评对象：感知节点设备所处物理环境和设计或验收文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈物理安全负责人现有感知节点设备的环境条件是否具有防挤压、防强振动等防物理破坏的能力；
 - 2) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备所处物理环境具有防挤压、防强振动等能力的说明，是否与实际情况一致；
 - 3) 应核查感知节点设备所处物理环境是否采取了防挤压、防强振动等的防护措施。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.1.1.2 测评单元（L4-PES4-02）

该测评单元包括以下要求：

- a) 测评指标：感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）；
- b) 测评对象：感知节点设备所处物理环境和设计或验收文档；
- c) 测评实施包括以下内容：
 - 1) 应核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备在工作状态所处物理环境的说明，是否与实际情况一致；
 - 2) 应核查感知节点设备在工作状态所处物理环境是否能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.1.1.3 测评单元（L4-PES4-03）

该测评单元包括以下要求：

- a) 测评指标：感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等；
- b) 测评对象：感知节点设备所处物理环境和设计或验收文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈物理安全负责人现有感知节点设备的环境条件是否对感知节点设备的正常工作造成影响，是否采取了防强干扰、防阻挡屏蔽等措施；
 - 2) 应核查感知节点设备所处物理环境的设计或验收文档，是否具有感知节点设备所处物理环境防强干扰、防阻挡屏蔽等能力的说明，是否与实际情况一致；
 - 3) 应核查感知节点设备所处物理环境是否采取了防强干扰、防阻挡屏蔽等防护措施。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.1.1.4 测评单元（L4-PES4-04）

该测评单元包括以下要求：

- a) 测评指标：关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久的，稳定的电力供应能力）；
- b) 测评对象：关键感知节点设备的供电设备（关键网关节点设备的供电设备）和设计或验收文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈物理安全负责人现有关键感知节点设备（关键网关节点设备）是否设置了可供长时间工作的电力供应措施（持久的、稳定的电力供应措施），供电时间是否满足设备的电力供应需求；
 - 2) 应核查关键感知节点设备（关键网关节点设备）电力供应设计或验收文档是否标明电力供应要求，其中是否明确保障关键感知节点设备长时间工作的电力供应措施（关键网关节点设备持久的、稳定的电力供应措施）；
 - 3) 应核查是否具有相关电力供应措施的运行维护记录，是否与电力供应设计一致。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.2 网络和通信安全

9.4.2.1 入侵防范

9.4.2.1.1 测评单元（L4-NCS4-01）

该测评单元包括以下要求：

- a) 测评指标：应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为；
- b) 测评对象：感知节点设备和设计文档；
- c) 测评实施包括以下内容：
 - 1) 应核查感知层安全设计文档，是否有对感知节点通信目标地址的控制措施说明；
 - 2) 应核查感知节点设备，是否配置了对感知节点通信目标地址的控制措施，相关参数配置是否符合设计要求；
 - 3) 应对感知节点设备进行渗透测试，测试是否能够限制感知节点设备对违反访问控制策略的通信目标地址进行访问或攻击。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.2.1.2 测评单元（L4-NCS4-02）

该测评单元包括以下要求：

- a) 测评指标：应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为；
- b) 测评对象：网关节点设备和设计文档；
- c) 测评实施包括以下内容：
 - 1) 应核查感知层安全设计文档，是否有对网关节点通信目标地址的控制措施说明；
 - 2) 应核查网关节点设备，是否配置了对网关节点通信目标地址的控制措施，相关参数配置是否符合设计要求；
 - 3) 应对感知节点设备进行渗透测试，测试是否能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.2.2 接入控制

9.4.2.2.1 测评单元（L4-NCS4-03）

该测评单元包括以下要求：

- a) 测评指标：应确保只有授权的感知节点可以接入；
- b) 测评对象：感知节点设备和设计文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术、身份鉴别技术等，具体措施有哪些；
 - 2) 应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述；
 - 3) 应对边界和感知层网络进行渗透测试，测试是否不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3 设备和计算安全

9.4.3.1 感知节点设备安全

9.4.3.1.1 测评单元（L4-ECS4-01）

该测评单元包括以下要求：

- a) 测评指标：应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更；
- b) 测评对象：感知节点设备；
- c) 测评实施包括以下内容：
 - 1) 应核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更；
 - 2) 应测试通过试图接入和控制传感网访问未授权的资源，验证感知节点设备的访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3.1.2 测评单元（L4-ECS4-02）

该测评单元包括以下要求：

- a) 测评指标：应具有对连接的网关节点设备（包括读卡器）设备进行身份标识和鉴别的能力；
- b) 测评对象：网关节点设备（包括读卡器）；
- c) 测评实施包括以下内容：
 - 1) 应核查是否对连接的网关节点设备（包括读卡器）设备进行身份标识与鉴别，是否配置了符合安全策略的参数；
 - 2) 应进行渗透测试，验证是否不存在绕过身份标识与鉴别功能的方法。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3.1.3 测评单元（L4-ECS4-03）

该测评单元包括以下要求：

- a) 测评指标：应具有对连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力；
- b) 测评对象：其他感知节点设备（包括路由节点）；
- c) 测评实施包括以下内容：
 - 1) 应核查是否对连接的其他感知节点设备（包括路由节点）设备进行身份标识与鉴别，是否配置了符合安全策略的参数；
 - 2) 应进行渗透测试，验证是否不存在绕过身份标识与鉴别功能的方法。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3.2 网关节点设备安全

9.4.3.2.1 测评单元（L4-ECS4-04）

该测评单元包括以下要求：

- a) 测评指标：应设置最大并发连接数；
- b) 测评对象：网关节点设备；

- c) 测评实施：应核查网关节点设备是否配置了最大并发连接数参数；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3.2.2 测评单元（L4-ECS4-05）

该测评单元包括以下要求：

- a) 测评指标：应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力；
- b) 测评对象：网关节点设备；
- c) 测评实施包括以下内容：
 - 1) 应核查网关节点设备是否能够对连接设备（包括终端节点、路由节点、数据处理中心）进行标识并配置了鉴别功能；
 - 2) 应进行渗透测试，验证是否不存在绕过身份标识与鉴别功能的方法。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3.2.3 测评单元（L4-ECS4-06）

该测评单元包括以下要求：

- a) 测评指标：应具备过滤非法节点和伪造节点所发送的数据的能力；
- b) 测评对象：网关节点设备；
- c) 测评实施包括以下内容：
 - 1) 应核查网关节点设备是否配置了过滤非法节点和伪造节点发送的数据的功能；
 - 2) 应测试网关节点设备，是否能够过滤非法节点和伪造节点发送的数据。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3.2.4 测评单元（L4-ECS4-07）

该测评单元包括以下要求：

- a) 测评指标：授权用户应能够在设备使用过程中对密钥进行在线更新；
- b) 测评对象：感知节点设备；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员有哪些感知节点设备需要采用密钥进行通信，是否对设备的关键密钥进行在线更新；
 - 2) 应核查感知节点设备是否对其密钥进行在线更新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3.2.5 测评单元（L4-ECS4-08）

该测评单元包括以下要求：

- a) 测评指标：授权用户应能够在设备使用过程中对关键配置参数进行在线更新；
- b) 测评对象：感知节点设备；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员感知节点设备是否支持对其关键配置参数进行在线更新；

2) 应核查感知节点设备在线更新方式是否有效。

- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.4 应用和数据安全

9.4.4.1 抗数据重放

9.4.4.1.1 测评单元 (L4-ADS4-01)

该测评单元包括以下要求：

- a) 测评指标：应能够鉴别数据的新鲜性，避免历史数据的重放攻击；
- b) 测评对象：感知节点设备；
- c) 测评实施包括以下内容：
 - 1) 应核查感知节点设备鉴别数据新鲜性的措施，是否能够避免历史数据重放；
 - 2) 应将感知节点设备历史数据进行重放测试，验证其保护措施是否生效。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.4.1.2 测评单元 (L4-ADS4-02)

该测评单元包括以下要求：

- a) 测评指标：应能够鉴别历史数据的非法修改，避免数据的修改重放攻击；
- b) 测评对象：感知节点设备；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员针对感知节点设备历史数据的保护措施，具体措施有哪些，是否具有对历史数据被非法修改的检测措施，检测措施有哪些；
 - 2) 应核查感知层是否配备检测感知节点设备历史数据被非法篡改的措施，在检测到被修改时是否能采取必要的恢复措施；
 - 3) 应测试检测措施的有效性，是否能够避免数据的修改重放攻击。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.4.2 数据融合处理

9.4.4.2.1 测评单元 (L4-ADS4-03)

该测评单元包括以下要求：

- a) 测评指标：应对来自传感网的数据进行数据融合处理，使不同类型的数据可以在同一个平台被使用；
- b) 测评对象：物联网应用系统；
- c) 测评实施包括以下内容：
 - 1) 应访谈应用系统管理员来自传感网的数据的类型和数据格式等；
 - 2) 应核查是否提供对来自传感网的数据进行数据融合处理的功能；
 - 3) 应测试数据融合处理功能是否能够处理不同类型的数据。
- d) 单元判定：如果 2) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.4.2.2 测评单元（L4-ADS4-04）

该测评单元包括以下要求：

- a) 测评指标：应对不同数据之间的依赖关系和制约关系等进行智能处理，如一类数据达到某个门限时可以影响对另一类数据采集终端的管理指令；
- b) 测评对象：物联网应用系统；
- c) 测评实施包括以下内容：
 - 1) 应访谈应用系统管理员对不同数据之间的依赖关系和制约关系等方面的处理方式；
 - 2) 应核查是否能够智能处理不同数据之间的依赖关系和制约关系。
- d) 单元判定：如果 2) 为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.5 安全运维管理

9.4.5.1 感知节点管理

9.4.5.1.1 测评单元（L4-MMS4-01）

该测评单元包括以下要求：

- a) 测评指标：应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；
- b) 测评对象：维护记录；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统运维负责人是否有专门的人员对感知节点设备、网关节点设备进行定期维护，由何部门或何人负责，维护周期多长；
 - 2) 应核查感知节点设备、网关节点设备部署环境维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.5.1.2 测评单元（L4-MMS4-02）

该测评单元包括以下要求：

- a) 测评指标：应记录感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息），对网关设备进行现场维护（除尘、充电、修理等）；
- b) 测评对象：维护记录；
- c) 测评实施：应核查感知节点设备、网关节点设备部署环境维护记录是否包括了感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息）核查、对网关设备进行现场维护（除尘、充电、修理等）等方面内容；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.5.1.3 测评单元（L4-MMS4-03）

该测评单元包括以下要求：

- a) 测评指标：应对感知节点和网关节点设备部署环境的评估方法作出明确规定；
- b) 测评对象：感知节点和网关节点设备部署环境的评估说明文档；

- c) 测评实施包括以下内容：
 - 1) 应访谈系统运维负责人是否明确规定需对感知节点和网关节点设备部署环境进行评估；
 - 2) 应核查感知节点和网关节点设备部署环境的评估说明文档内容是否包含可操作的评估方法。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.5.1.4 测评单元 (L4-MMS4-04)

该测评单元包括以下要求：

- a) 测评指标：应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；
- b) 测评对象：感知节点和网关节点设备安全管理文档；
- c) 测评实施：
 - 1) 应访谈系统运维负责人是否明确规定需对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程进行全程管理；
 - 2) 应核查感知节点和网关节点设备安全管理文档是否覆盖感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等方面。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.5.1.5 测评单元 (L4-MMS4-05)

该测评单元包括以下要求：

- a) 测评指标：应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等；
- b) 测评对象：感知节点设备、网关节点设备部署环境的管理制度；
- c) 测评实施：
 - 1) 应核查感知节点设备、网关节点设备部署环境管理文档是否包括负责核查和维护的人员调离工作岗位立即交还相关核查工具和核查维护记录等方面内容；
 - 2) 应核查是否具有感知节点设备、网关节点设备部署环境的相关保密性管理记录。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5 工业控制系统安全测评扩展要求

9.5.1 物理和环境安全

9.5.1.1 室外控制设备物理防护

9.5.1.1.1 测评单元 (L4-PES5-01)

该测评单元包括以下要求：

- a) 测评指标：室外控制设备应放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；控制设备应安装在金属或其它绝缘板上(非木质板)，并紧固于箱体或装置中；
- b) 测评对象：室外控制设备；

- c) 测评实施包括以下内容：
 - 1) 应核查是否放置于采用铁板或其他防火绝缘材料制作，具有透风、散热、防盗、防雨、防火能力的箱体或装置中；
 - 2) 应核查是否安装在金属或其它绝缘板上(非木质板)，并紧固于箱体或装置中。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.1.1.2 测评单元 (L4-PES5-02)

该测评单元包括以下要求：

- a) 测评指标：室外控制设备放置应远离强电磁干扰、热源和应远离极端天气环境等，如无法避免，在遇到极端天气时应及时做好应急处置及检修确保设备正常运行；
- b) 测评对象：室外控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查是否远离极端天气环境；
 - 2) 应核查是否有极端天气时的应急处置及检修维护记录；
 - 3) 应核查位置放置是否远离强电磁干扰和热源。
- d) 单元判定：如果 1) -3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.2 网络和通信安全

9.5.2.1 网络架构

9.5.2.1.1 测评单元 (L4-NCS5-01)

该测评单元包括以下要求：

- a) 测评指标：工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用符合国家或行业规定的专用产品实现单向安全隔离；
- b) 测评对象：网闸、防火墙和单向安全隔离装置等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查工业控制系统的网络是否部署单向隔离设备；
 - 2) 应核查在网络边界处是否采用了有效的单向隔离策略实施访问控制；
 - 3) 应核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离强度相同的措施；
 - 4) 应核查所使用的专用产品是否符合国家规定，如有行业特殊规定的是否符合行业规定。
- d) 单元判定：如果 1) -4) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.2.1.2 测评单元 (L4-NCS5-02)

该测评单元包括以下要求：

- a) 测评指标：工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；
- b) 测评对象：路由器、交换机和防火墙等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查工业控制系统内部不同的子系统类型，是否按照安全等级和安全防护强度等业务特点划分了不同的安全域；

- 2) 应核查各安全域之间交换机和防火墙是否配置了有效的访问控制策略。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.2.1.3 测评单元 (L4-NCS5-03)

该测评单元包括以下要求：

- a) 测评指标：涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其它数据网及外部公共信息网的安全隔离；
- b) 测评对象：路由器和交换机等提供网络通信功能的设备；
- c) 测评实施：应核查工业控制系统关键区域的传输数据要求，涉及实时传输数据与控制要求的，核查是否采用独立的网络和设备组网实现关键部位安全防护；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.2.2 通信传输

9.5.2.2.1 测评单元 (L4-NCS5-04)

该测评单元包括以下要求：

- a) 测评指标：在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输；
- b) 测评对象：加密认证设备、路由器、交换机和防火墙等提供访问控制功能的设备；
- c) 测评实施：应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术手段实现身份认证、访问控制和数据加密传输；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.2.3 访问控制

9.5.2.3.1 测评单元 (L4-NCS5-05)

该测评单元包括以下要求：

- a) 测评指标：工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务；
- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备；
- c) 测评实施包括以下内容：
 - 1) 应核查在工业控制系统与企业其他系统之间的网络边界是否部署访问控制设备，是否配置访问控制策略；
 - 2) 应核查设备安全策略，是否禁止 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越边界。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.2.3.2 测评单元 (L4-NCS5-06)

该测评单元包括以下要求：

- a) 测评指标：应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警；

- b) 测评对象：网闸、防火墙、路由器和交换机等提供访问控制功能的设备，监控预警设备；
- c) 测评实施包括以下内容：
 - 1) 应核查设备是否可以在策略失效的时候进行告警；
 - 2) 应核查是否部署监控预警系统或相关模块，在边界防护机制失效时可及时告警。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.2.4 拨号使用控制

9.5.2.4.1 测评单元 (L4-NCS5-07)

该测评单元包括以下要求：

- a) 测评指标：工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量；并采取用户身份鉴别和访问控制等措施；
- b) 测评对象：拨号服务类设备；
- c) 测评实施包括以下内容：
 - 1) 应核查工业控制系统是否确需使用拨号服务；
 - 2) 应核查拨号设备是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用账户/口令等身份鉴别方式，是否采用控制账户权限等访问控制措施。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.2.4.2 测评单元 (L4-NCS5-08)

该测评单元包括以下要求：

- a) 测评指标：拨号服务器和客户端均应使用经安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施；
- b) 测评对象：拨号服务类设备；
- c) 测评实施：应核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.2.4.3 测评单元 (L4-NCS5-09)

该测评单元包括以下要求：

- a) 测评指标：涉及实时控制和数据传输的工业控制系统禁止使用拨号访问服务；
- b) 测评对象：拨号服务类设备；
- c) 测评实施：应核查涉及实时控制和数据传输的工业控制系统内是否禁止使用拨号访问服务；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.2.5 无线使用控制

9.5.2.5.1 测评单元 (L4-NCS5-10)

该测评单元包括以下要求：

- a) 测评指标：应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；

- b) 测评对象：无线通信网络及设备；
- c) 测评实施包括以下内容：
 - 1) 应核查无线通信的用户在登录时是否采用了身份鉴别措施；
 - 2) 应核查无线通信的用户列表，核查用户身份标识是否具有唯一性。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.2.5.2 测评单元（L4-NCS5-11）

该测评单元包括以下要求：

- a) 测评指标：应对所有参与无线通信的用户（人员、软件进程或者设备）进行授权以及执行使用进行限制；
- b) 测评对象：无线通信网络及设备；
- c) 测评实施：应核查无线通信过程中是否对用户进行授权，核查具体权限是否合理；核查未授权的使用是否可以被发现及告警；
- d) 单元判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.2.5.3 测评单元（L4-NCS5-12）

该测评单元包括以下要求：

- a) 测评指标：应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护；
- b) 测评对象：无线通信网络及设备；
- c) 测评实施：应核查无线通信传输中是否采用加密措施保证传输报文的机密性；
- d) 单元判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.2.5.4 测评单元（L4-NCS5-13）

该测评单元包括以下要求：

- a) 测评指标：对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统行为；
- b) 测评对象：无线通信网络及设备、监测设备；
- c) 测评实施：应核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备应及时发出告警并可以对试图接入的无线设备进行屏蔽；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.3 设备和计算安全

9.5.3.1 控制设备安全

9.5.3.1.1 测评单元（L4-ECS5-01）

该测评单元包括以下要求：

- a) 测评指标：控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等设备和计算方面的安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；

- b) 测评对象：控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；
 - 2) 如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。
- d) 单元判定：如果 2) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.3.1.2 测评单元（L4-ECS5-02）

该测评单元包括以下要求：

- a) 测评指标：应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；
- b) 测评对象：控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查测试环境或测试报告，核查是否有测试评估记录；
 - 2) 应核查控制设备版本、补丁及固件是否经过充分测试后进行了更新。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.3.1.3 测评单元（L4-ECS5-03）

该测评单元包括以下要求：

- a) 测评指标：应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口等，确需保留的必须通过相关的技术措施实施严格的监控管理；
- b) 测评对象：控制设备；
- c) 测评实施包括以下内容：
 - 1) 应核查控制设备是否关闭或拆除设备的软盘驱动、光盘驱动、USB 接口、串行口等；
 - 2) 应核查保留的软盘驱动、光盘驱动、USB 接口、串行口等是否通过相关的措施实施严格的监控管理。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.3.1.4 测评单元（L4-ECS5-04）

该测评单元包括以下要求：

- a) 测评指标：应使用专用设备和专用软件对控制设备进行更新；
- b) 测评对象：控制设备；
- c) 测评实施：应核查更新控制设备时是否为专用设备和专用软件；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.3.1.5 测评单元（L4-ECS5-05）

该测评单元包括以下要求：

- a) 测评指标：应保证控制设备在上线前经过安全性检测，确保控制设备固件中不存在恶意代码程序；

- b) 测评对象：控制设备；
- c) 测评实施：应核查控制设备在上线前的检测报告，明确控制设备固件中是否不存在恶意代码程序；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.4 安全建设管理

9.5.4.1 产品采购和使用

9.5.4.1.1 测评单元（L4-CMS5-01）

该测评单元包括以下要求：

- a) 测评指标：工业控制系统重要设备及专用信息安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用；
- b) 测评对象：安全管理员和检测报告类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员系统使用的工业控制系统重要设备及专用信息安全产品是否通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测；
 - 2) 应核查工业控制系统是否有通过国家及行业监管部门认可的专业机构出具的安全性及电磁兼容性检测的检测报告。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.4.2 外包软件开发

9.5.4.2.1 测评单元（L4-CMS5-02）

该测评单元包括以下要求：

- a) 测评指标：应在外包开发合同中包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款；
- b) 测评对象：外包合同；
- c) 测评实施：应核查外包开发合同中是否包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.5 安全运维管理

9.5.5.1 漏洞和风险管理

9.5.5.1.1 测评单元（L4-MMS5-01）

该测评单元包括以下要求：

- a) 测评指标：应采取必要的措施识别安全漏洞和隐患，并根据风险分析的后果，对发现的安全漏洞和隐患在确保安全生产的情况下及时进行修补；或评估可能的影响后采取必要的补救措施，补救措施宜在系统维护期间开展；
- b) 测评对象：安全管理员、管理制度类文档和记录表单类文档；

- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否采取必要的措施识别安全漏洞隐患，并根据风险分析的后果，对发现的安全漏洞和隐患在确保安全生产的情况下及时进行修补；
 - 2) 应核查是否有文档描述了存在的漏洞、严重级别、原因分析和改进意见等方面；
 - 3) 应核查是否有维护期间设备检修记录，查阅相关修补说明。
- d) 单元判定：如果 1)～3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.5.1.2 测评单元 (L4-MMS5-02)

该测评单元包括以下要求：

- a) 测评指标：应按照工业控制系统类别，建立控制设备漏洞台账或漏洞库，通过扫描机制或情报共享机制定期更新；通过漏洞台账或漏洞库，建立漏洞测试验证机制，定期对不影响生产环境的高危漏洞进行修补；对不能修复的漏洞，应建立补偿措施，弥补漏洞对工业控制系统带来的风险；
- b) 测评对象：安全管理员、控制设备、漏洞台账和漏洞库系统；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否建设了漏洞台账或漏洞库；
 - 2) 应核查漏洞台账或漏洞库内容是否更新；
 - 3) 应核查是否对漏洞有测试验证机制；
 - 4) 应核查是否对控制设备做过漏洞修复，提供相关变更文档；
 - 5) 应核查存在高危漏洞的控制设备是否采用了相关弥补措施。
- d) 单元判定：如果 1)～5) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.5.2 恶意代码防范管理

9.5.5.2.1 测评单元 (L4-MMS5-03)

该测评单元包括以下要求：

- a) 测评指标：在更新恶意代码库、木马库以及规则库前，应首先在测试环境中测试通过，对隔离区域恶意代码更新应有专人负责，更新操作应离线进行，并保存更新记录；
- b) 测评对象：安全管理员、管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈系统管理员是否在更新恶意代码库、木马库以及规则库前在实验环境进行测试，对隔离区域恶意代码更新是否有专人负责，更新操作是否离线进行，是否保存更新记录；
 - 2) 应核查恶意代码防范管理制度中是否对恶意代码库升级测试及更新等流程提出相关要求；
 - 3) 应核查恶意代码库升级测试及更新记录是否与制度要求相符。
- d) 单元判定：如果 1)～3) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.5.5.2.2 测评单元 (L4-MMS5-04)

该测评单元包括以下要求：

- a) 测评指标：工业控制系统重要软硬件系统、设备及专用信息安全产品应采用符合国家及行业相关要求的产品及服务；

- b) 测评对象：安全管理员和检测报告类文档；
- c) 测评实施：应访谈安全管理员系统使用的工业控制系统重要软硬件系统、设备及专用信息安全产品是否为国家及行业监管部门认可的产品及服务；
- d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.5.5.3 安全事件处置

9.5.5.3.1 测评单元（L4-MMS5-05）

该测评单元包括以下要求：

- a) 测评指标：应建立工业控制系统联合防护和应急机制，负责处置跨单位工业控制系统安全事件；
- b) 测评对象：安全管理员、管理制度类文档和记录表单类文档；
- c) 测评实施包括以下内容：
 - 1) 应访谈安全管理员是否建立跨单位处置工业控制系统安全事件流程；
 - 2) 应核查跨单位安全事件报告和处置管理制度，核查是否含有工业控制系统联合防护和应急的相关内容。
- d) 单元判定：如果 1) -2) 均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

10 第五级测评要求

略。

11 整体测评

11.1 概述

国标GB/T 22239-20XX中的要求项，是为了对抗相应等级的威胁或具备相应等级的恢复能力而设计的，但由于安全措施的实现方式多种多样，安全技术也在不断发展，等级保护对象的运行使用单位所采用的安全措施和技术并不一定和GB/T 22239-20XX的要求项完全一致。因此，需要从等级保护对象整体上是否能够对抗相应等级威胁的角度，对单项测评中的不符合项和部分符合项进行综合分析，分析这些不符合项或部分符合项是否会影响到等级保护对象整体安全保护能力的缺失。等级保护对象的整体测评就是在单项测评的基础上，评价等级保护对象的整体安全保护能力有没有缺失，是否能够对抗相应等级的安全威胁。

等级保护对象整体测评应从安全控制点、安全控制点间和层面间等方面进行测评和综合安全分析，从而给出等级测评结论。整体测评包括安全控制点测评、安全控制点间测评和层面间测评。

安全控制点测评是指对单个控制点中所有要求项的符合程度进行分析和判定。

安全控制点间安全测评是指对同一区域同一层面内的两个或者两个以上不同安全控制点间的关联进行测评分析，其目的是确定这些关联对等级保护对象整体安全保护能力的影响。

层面间安全测评是指对同一区域内的两个或者两个以上不同层面安全控制点间的关联进行测评分析，其目的是确定这些关联对等级保护对象整体安全保护能力的影响。

11.2 安全控制点测评

在单项测评完成后,如果该安全控制点下的所有要求项为符合,则该安全控制点符合,否则为不符合或部分符合。

11.3 安全控制点间测评

在单项测评完成后,如果等级保护对象的某个安全控制点中的要求项存在不符合或部分符合,应进行安全控制点间测评,应分析在同一层面内,是否存在其他安全控制点对该安全控制点具有补充作用(如物理访问控制和防盗窃、身份鉴别和访问控制等)。同时,分析是否存在其他的安全措施或技术与该要求项具有相似的安全功能。

根据测评分析结果,综合判断该安全控制点所对应的系统安全保护能力是否缺失,如果经过综合分析单项测评中的不符合项或部分符合项不造成系统整体安全保护能力的缺失,则该安全控制点的测评结论应调整为符合。

11.4 层面间测评

在单项测评完成后,如果等级保护对象的某个安全控制点中的要求项存在不符合或部分符合,应进行层面间安全测评,重点分析其他层面上功能相同或相似的安全控制点是否对该安全控制点存在补充作用(如应用和数据层加密与网络和通信层加密、设备和计算层与应用和数据层上的身份鉴别等),以及技术与管理上各层面的关联关系(如设备和计算安全与安全运维管理、应用和数据安全与安全运维管理等)。

根据测评分析结果,综合判断该安全控制点所对应的系统安全保护能力是否缺失,如果经过综合分析单项测评中的不符合项或部分符合项不造成系统整体安全保护能力的缺失,则该安全控制点的测评结论应调整为符合。

12 测评结论

12.1 各层面的测评结论

通过汇总安全控制点的测评结果,等级测评报告可以给出等级保护对象在安全技术和安全管理各个层面的等级测评结论。

在安全技术四个层面的等级测评结论中,通常物理和环境安全测评结论应重点给出等级保护对象在防范各种自然灾害和人为物理破坏方面安全控制措施的落实情况;网络和通信安全测评结论应重点给出等级保护对象在网络结构安全、通信传输、边界保护、访问控制、入侵防范、恶意代码防范、安全审计和集中管控等方面安全控制措施的落实情况;设备和计算安全测评结论应重点给出身份鉴别、访问控制、安全审计入侵防范、恶意代码防范和资源控制等方面安全控制措施的落实情况;应用和数据安全测评结论应重点给出身份鉴别、访问控制、安全审计、软件容错、资源控制、数据完整性、数据保密性、数据备份恢复、剩余信息保护和个人隐私保护等方面的安全控制措施的落实情况。

在安全管理四个方面的等级测评结论中,通常安全策略和管理制度应重点给出安全策略及管理制度体系的完备性和制修订的及时性等方面的测评结论;安全管理机构和人员应重点给出机构、岗位设置、人员配备、人员录用、离岗和培训等方面的测评结论;安全建设管理可重点给出系统定级与备案、安全方案设计、产品采购与使用、系统的测试验收和交付等方面的测评结论;安全运维管理可重点给出设备维护管理、网络与系统安全管理、漏洞和风险管理、恶意代码防范管理、安全事件处置以及应急预案管理等方面的测评结论。

不同等级等级保护对象在不同层面上会有不同的关注点,应反映到相应层面的等级测评结论中。

12.2 风险分析和评价

等级测评报告中应对整体测评之后单项测评结果中的不符合项或部分符合项进行风险分析和评价。

采用风险分析的方法对单项测评结果中存在的不符合项或部分符合项,分析所产生的安全问题被威胁利用的可能性,判断其被威胁利用后对业务信息安全和系统服务安全造成影响的程度,综合评价这些不符合项或部分符合项对定级对象造成的安全风险。

12.3 等级测评结论

等级测评报告应给出等级保护对象的等级测评结论,确认等级保护对象达到相应等级保护要求的程度。

应结合各层面的测评结论和对单项测评结果的风险分析给出等级测评结论:

- a) 符合:定级对象中未发现安全问题,等级测评结果中所有测评项的单项测评结果中部分符合和不符合项的统计结果全为0,综合得分为100分。
- b) 基本符合:定级对象中存在安全问题,部分符合和不符合项的统计结果不全为0,但存在的安全问题不会导致定级对象面临高等级安全风险,且综合得分不低于阈值。
- c) 不符合:定级对象中存在安全问题,部分符合项和不符合项的统计结果不全为0,而且存在的安全问题会导致定级对象面临高等级安全风险,或者综合得分低于阈值。

附录 A

（资料性附录）

测评力度

A.1 概述

测评力度是在等级测评过程中实施测评工作的力度，体现为测评工作的实际投入程度，具体由测评的广度和深度来反映。测评广度越大，测评实施的范围越大，测评实施包含的测评对象就越多。测评深度越深，越需要在细节上展开，测评就越严格，因此就越需要更多的工作投入。投入越多，测评力度就越强，测评效果就越有保证。

测评方法是测评人员依据测评内容选取的、实施特定测评操作的具体方法，涉及访谈、核查和测试等三种基本测评方法。三种基本测评方法的测评力度可以通过其测评的深度和广度来描述：

- 访谈深度：分别为简要、充分、较全面和全面等四种。简要访谈只包含通用和高级的问题；充分访谈包含通用和高级的问题以及一些较为详细的问题；较全面访谈包含通用和高级的问题以及一些有难度和探索性的问题；全面访谈包含通用和高级的问题以及较多有难度和探索性的问题。
- 访谈广度：体现在访谈人员的构成和数量上。访谈覆盖不同类型的人员和同一类人的数量多少，体现出访谈的广度不同。
- 核查深度：分别为简要、充分、较全面和全面等四种。简要核查主要是对功能性的文档、机制和活动，使用简要的评审、观察或核查以及核查列表和其他相似手段的简短测评；充分核查有详细的分析、观察和研究，除了功能性的文档、机制和活动外，还适当需要一些总体或概要设计信息；较全面核查有详细、彻底分析、观察和研究，除了功能性的文档、机制和活动外，还需要总体/概要和一些详细设计以及实现上的相关信息；全面核查有详细、彻底分析、观察和研究，除了功能性的文档、机制和活动外，还需要总体/概要和详细设计以及实现上的相关信息。
- 核查广度：核查的广度体现在核查对象的种类（文档、机制等）和数量上。核查覆盖不同类型的对象和同一类对象的数量多少，体现出对象的广度不同。
- 测试深度：测试的深度体现在执行的测试类型上，包括功能测试、性能测试和渗透测试。功能测试和性能测试只涉及机制的功能规范、高级设计和操作规程；渗透测试涉及机制的所有可用文档，并试图智取进入等级保护对象。
- 测试广度：测试的广度体现在被测试的机制种类和数量上。测试覆盖不同类型的机制以及同一类型机制的数量多少，体现出对象的广度不同。

A.2 等级测评力度

为了检验不同级别的等级保护对象是否具有相应等级的安全保护能力，是否满足相应等级的保护要求，需要实施与其安全保护等级相适应的测评，付出相应的工作投入，达到应有的测评力度。测评的广度和深度落实到访谈、核查和测试三种不同的测评方法上，能体现出测评实施过程中访谈、核查和测试的投入程度的不同。第一级到第四级等级保护对象的测评力度反映在访谈、核查和测试等三种基本测评方法的测评广度和深度上，落实在不同单项测评中具体的测评实施上。

表A. 1从测评对象数量和种类以及测评深度等方面详细分析了不同测评方法的测评力度在不同级别的等级保护对象安全测评中的具体体现。

表A.1 不同级别的等级保护对象的测评力度要求

测评 力度	测评 方法	第一级	第二级	第三级	第四级
广度	访谈	测评对象在种类和数量上抽样,种类和数量都较少	测评对象在种类和数量上抽样,种类和数量都较多	测评对象在数量上抽样,在种类上基本覆盖	测评对象在数量上抽样,在种类上全部覆盖
	核查				
	测试				
深度	访谈	简要	充分	较全面	全面
	核查				
	测试	功能测试	功能测试	功能测试和测试验证	功能测试和测试验证

从表A. 1可以看到，对不同级别的等级保护对象进行等级测评时，选择的测评对象的种类和数量是不同的，随着等级保护对象安全保护等级的增高，抽查的测评对象的种类和数量也随之增加。

对不同级别的等级保护对象进行等级测评时，实际抽查测评对象的种类和数量，应当达到表A. 1的要求，以满足相应等级的测评力度要求。在具体测评对象选择工作过程中，可参照遵循以下原则：

- a) 完整性原则，选择的设备及安全措施等应能满足相应等级的测评力度要求；
- b) 重要性原则，应抽查重要的网络设备、安全设备、服务器、数据库和应用软件等；
- c) 安全性原则，应抽查对外暴露的网络边界设备；
- d) 共享性原则，应抽查共享设备和数据交换平台（设备）；
- e) 代表性原则，抽查应尽量覆盖各种设备类型、操作系统类型、数据库系统类型和应用系统的类型。

附 录 B
(规范性附录)
测评单元编号说明

B.1 测评单元编码规则

测评单元编号为三组数据，格式为XX-XXXX-XX，各组含义和编码规则如下：

第1组由两位组成，第1位为字母L，第2位为数字，其中数字1为第一级，2为第二级，3为第三级，4为第四级，5为第五级。

第2组由4位组成，前3位为字母，第4位为数字。字母代表层面：PES为物理和环境安全，NCS为网络和通信安全，ECS为设备和计算安全，ADS为应用和数据安全，PSS为安全策略和管理制度，ORS为安全管理机构和人员，CMS为安全建设管理，MMS为安全运维管理。数字代表标准分册：1为安全测评通用要求部分，2为云计算安全测评扩展要求部分，3为移动互联安全测评扩展要求部分，4为物联网安全测评扩展要求部分，5为工业控制系统安全测评扩展要求部分。

第3组由2位数字组成，按层面对基本要求中的要求项进行顺序编号。

示例：测评单元编号为L1-PES1-01，代表源自安全测评通用要求部分的第一级物理和环境安全类的第1个指标。

B.2 专用缩略语

下列专用缩略语适用于本标准。

OS	总体安全 (Overall Security)
ADS	应用和数据安全 (Application and Data Security)
CMS	安全建设管理 (Construction Management Security)
ECS	设备和计算安全 (Equipment and Computing Security)
MMS	安全运维管理 (Maintenance Management Security)
NCS	网络和通信安全 (Network and Communication Security)
ORS	安全管理机构和人员 (Organization and Resource Security)
PES	物理和环境安全为 (Physical and Environment Security)
PSS	安全策略和管理制度 (Policy and System Security)

附 录 C
(资料性附录)
设计要求测评验证表

为便于测评实施人员进行快速查询本标准条款与《信息安全技术 网络安全等级保护设计要求》条款的对应关系，本附录进行索引对应。针对大数据等级保护对象的测评实施将另行制定。

C.1 通用安全设计要求测评验证表

C.1.1 第一级

适用范围	功能要求	设计要求	测评要求
5.3.1 安全计算环境设计技术要求	5.3.1.1 通用安全计算环境设计技术要求	a) 用户身份鉴别 应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份；在每次用户登录系统时，采用口令鉴别机制进行用户身份鉴别，并对口令数据进行保护。	测评单元（L1-ECS1-01） 应核查用户在登录时是否采用了身份鉴别措施；应核查用户列表，核查用户身份标识是否具有唯一性；应核查用户配置信息或访谈系统管理员，核查是否不存在空口令用户；应核查用户鉴别信息是否具有复杂度要求并定期更换。 测评单元（L1-ADS1-17） 应核查系统设计文档，重要管理数据、重要业务数据在传输过程中是否采用了校验码技术或密码技术保证完整性；应测试在传输过程中对重要管理数据、重要业务数据进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。
		b) 自主访问控制 应在安全策略控制范围内，使用用户/用户组对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户/用户组。访问控制主体的粒度为用户/用户组级，客体的粒度为文件或数	测评单元（L1-ECS1-03） 应访谈网络管理员、安全管理员、系统管理员或核查用户账户和权限设置情况；应核查是否已禁用或限制匿名、默认账户的访问权限。 测评单元（L1-ADS1-03） 应核查是否提供访问控制功能；应核查是否

		数据库表级。访问操作包括对客体的创建、读、写、修改和删除等。	有管理用户负责对系统用户进行账户分配和权限管理。
		c) 用户数据完整性保护 可采用常规校验机制, 检验存储的用户数据的完整性, 以发现其完整性是否被破坏。	测评单元 (L1-ADS1-17) 应核查系统设计文档, 重要管理数据、重要业务数据在传输过程中是否采用了校验码技术或密码技术保证完整性; 应测试在传输过程中对重要管理数据、重要业务数据进行篡改, 查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。
		d) 恶意代码防范 应安装防恶意代码软件或配置具有相应安全功能的操作系统, 并定期进行升级和更新, 以防范和清除恶意代码。	— —
		e) 程序可信执行保护 可基于可信根对计算节点的 BIOS、引导程序、操作系统内核等进行可信验证, 并在检测到其可信性受到破坏后进行报警。	— —
5.3.2 安全区域边界设计技术要求	5.3.2.1 通用安全区域边界设计技术要求	a) 区域边界包过滤 可根据区域边界安全控制策略, 通过检查数据包的源地址、目的地址、传输层协议和请求的服务等, 确定是否允许该数据包通过该区域边界。	测评单元 (L1-NCS1-05) 应核查在网络边界或区域之间是否部署访问控制设备, 是否启用访问控制策略; 应核查设备的最后一条访问控制策略是否为禁止所有网络通信。
		b) 区域边界恶意代码防范 可在安全区域边界设置防恶意代码软件, 并定期进行升级和更新, 以防止恶意代码入侵。	— —
5.3.3 安全通信网络设计技术要求	5.3.3.1 通用安全通信网络设计技	a) 通信网络数据传输完整性保护 通信网络数据传输完整性保护。可采用常规校验机制, 检验通信网络	测评单元 (L4-NCS1-07) 应核查是否在数据传输过程中使用密码技术来保证其完整性; 应测试验证密码技术设备

	术要求	数据传输的完整性，并能发现其完整性被破坏。	或组件是否保证通信过程中数据的完整性。

C.1.2 第二级

适用范围	功能要求	设计要求	测评要求
6.3.1 安全计算环境设计技术要求	6.3.3.1 通用安全计算环境设计技术要求	a) 用户身份鉴别 应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录系统时，采用受控的口令或具有相应安全强度的其他机制进行用户身份鉴别，并使用密码技术对鉴别数据进行保密性和完整性保护。	测评单元（L2-ECS1-01） 应核查用户在登录时是否采用了身份鉴别措施； 应核查用户列表，核查用户身份标识是否具有唯一性；应核查用户配置信息或访谈系统管理员，核查是否不存在空口令用户；应核查用户鉴别信息是否具有复杂度要求并定期更换。 测评单元（L2-ADS1-17） 应核查系统设计文档，重要管理数据、重要业务数据在传输过程中是否采用了校验码技术或密码技术保证完整性；应测试在传输过程中对重要管理数据、重要业务数据进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。
		b) 自主访问控制 应在安全策略控制范围内，使用用户对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户。访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。访问操作包括对客体的创建、读、写、修改和删除等。	测评单元（L2-ECS1-04） 应访谈网络管理员、安全管理员、系统管理员或核查用户账户和权限设置情况；应核查是否已禁用或限制匿名、默认账户的访问权限。 测评单元（L2-ADS1-05） 应核查是否提供访问控制功能；应核查是否有管理用户负责对系统用户进行账户分配和权限管理。
		c) 系统安全审计 应提供安全审计机制，记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和	测评单元（L2-NCS1-12） 应核查设备是否开启了日志记录或安全审计功能；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件

		结果等内容。该机制应提供审计记录查询、分类和存储保护，并可由安全管理中心管理。	进行了审计。 测评单元（L2-NCS1-13） 应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。 测评单元（L2-NCS1-14） 应核查是否采取了技术措施能够对审计记录进行保护；应核查审计记录的备份机制和备份策略是否合理。
		d) 用户数据完整性保护 可采用常规校验机制，检验存储的用户数据的完整性，以发现其完整性是否被破坏。	测评单元（L2-ADS1-17） 应核查系统设计文档，重要管理数据、重要业务数据在传输过程中是否采用了校验码技术或密码技术保证完整性；应测试在传输过程中对重要管理数据、重要业务数据进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。
		e) 用户数据保密性保护 可采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的进行用户数据进行保密性保护。	— —
		f) 客体安全重用 应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。	测评单元（L2-ADS1-20） 应核查相关配置信息或访谈应用系统管理员，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。
		g) 恶意代码防范 应安装防恶意代码软件或配置具有相应安全功能的操作系统，并定期进行升级和更新，以防范和清除	测评单元（L2-ECS1-16） 应核查防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库。

		恶意代码。	
		h) 程序可信执行保护 可基于可信根对计算节点的 BIOS、引导程序、操作系统内核、应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。	— —
6.3.2 安全区域边界设计技术要求	6.3.2.1 通用安全区域边界设计技术要求	a) 区域边界包过滤 应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议和请求的服务等，确定是否允许该数据包通过该区域边界。	测评单元 (L2-NCS1-07) 应核查在网络边界或区域之间是否部署访问控制设备，是否启用访问控制策略；应核查设备的最后一条访问控制策略是否为禁止所有网络通信。
		b) 区域边界安全审计 应在安全区域边界设置审计机制，并由安全管理中心统一管理。	测评单元 (L2-NCS1-12) 应核查设备是否开启了日志记录或安全审计功能；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行了审计。 测评单元 (L2-NCS1-13) 应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。
		c) 区域边界恶意代码防范 可在安全区域边界设置防恶意代码网关，由安全管理中心管理。	测评单元 (L2-NCS1-11) 应核查相关系统或设备是否能够检测到以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；应核查相关系统或设备的规则库版本是否已经更新到最新版本；应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点。应测试相关系统或设备验证其安全策略是否有效
		d) 区域边界完整性保护 应在区域边界设置探测器，探测非	测评单元 (L2-NCS1-06) 应核查在网络边界处是否部署访问控制设备；应

		法外联等行为，并及时报告安全管理中心。	核查设备配置信息是否指定端口进行跨越边界的网络通信，该端口配置并启用了安全策略；应采用其他技术手段（如非法无线网络设备定位检查、核查设备配置信息等）核查是否不存在其他未受控端口进行跨越边界的网络通信。
6.3.3 安全通信网络设计技术要求	6.3.3.1 通用安全通信网络设计技术要求	a) 通信网络安全审计 应在安全通信网络设置审计机制，由安全管理中心管理。	测评单元（L2-NCS1-12） 应核查设备是否开启了日志记录或安全审计功能；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行了审计。 测评单元（L2-NCS1-13） 应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。
		b) 通信网络数据传输完整性保护 可采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护。	测评单元（L2-ADS1-17） 应核查系统设计文档，重要管理数据、重要业务数据在传输过程中是否采用了校验码技术或密码技术保证完整性；应测试在传输过程中对重要管理数据、重要业务数据进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。
		c) 通信网络数据传输保密性保护 采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。	—
6.3.4 安全管理中心设计技术要求	6.3.4.1 系统管理	可通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、可信基准库、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复以及恶意代码防范等。 应对系统管理员进行身份鉴别，只	测评单元（L2-MMS1-10） 应核查网络和系统安全管理文档是否明确要求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）。 测评单元（L2-MMS1-11） 应访谈运维负责人是否指定专门的部门或人员

		允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。	进行账户管理；应核查相关审批记录或流程是否对申请账户、建立账户、删除账户等进行控制。 测评单元（L2-MMS1-12） 应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略，账户管理（用户责任、义务、风险、权限审批、权限分配、账户注销等），配置文件的生成、备份，变更审批、符合性核查等，授权访问，最小服务，升级与打补丁，审计日志，登录设备和系统的口令更新周期等方面。 测评单元（L2-ADS1-08） 应核查是否提供并启用了安全审计功能；应核查审计范围是否覆盖到每个用户；应核查并测试是否对重要的用户行为和重要安全事件进行审计。
	6.4.3.2 审计管理	可通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。	测评单元（L2-ORS1-03） 应访谈信息安全主管是否配备了系统管理员、网络管理员和安全管理员；应核查人员配备文档是否有各岗位人员配备情况。 测评单元（L2-MMS1-10） 应核查网络和系统安全管理文档是否明确要求对网络 and 系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）。 测评单元（L2-ADS1-08） 应核查是否提供并启用了安全审计功能；应核查审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行审计。

C.1.3 第三级

适用范围	功能要求	设计要求	测评要求
7.3.1 安全计算环境设计技	7.3.3.1 通用安全计算	a) 用户身份鉴别 应支持用户标识和用户鉴别。在对	测评单元（L3-ECS1-01） 应核查用户在登录时是否采用了身份鉴别措施； 应核查用户列表，核查用户身份标识是否具有唯

术要求	环境设计技术要求	每一个用户注册到系统时,采用用户名和用户标识符标识用户身份,并确保在系统整个生存周期用户标识的唯一性;在每次用户登录系统时,采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别,并对鉴别数据进行保密性和完整性保护。	一性;应核查用户配置信息或访谈系统管理员,核查是否不存在空口令用户;应核查用户鉴别信息是否具有复杂度要求并定期更换。 测评单元(L3-ECS1-04) 应核查系统是否采用两种或两种以上组合的鉴别技术对用户身份进行鉴别,其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现; 测评单元(L3-ADS1-26) 应核查设计文档,是否采用校验码技术或密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性;应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性;应测试在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改,查看是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。
		b) 自主访问控制 应在安全策略控制范围内,使用户对其创建的客体具有相应的访问操作权限,并能将这些权限的部分或全部授予其他用户。自主访问控制主体的粒度为用户级,客体的粒度为文件或数据库表级和(或)记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。	测评单元(L3-ECS1-05) 应访谈网络管理员、安全管理员、系统管理员或核查用户账户和权限设置情况;应核查是否已禁用或限制匿名、默认账户的访问权限。 测评单元(L3-ADS1-10) 应核查是否由授权主体负责配置访问控制策略;应核查授权主体是否依据安全策略配置了主体对客体的访问规则;应测试是否不存在可越权访问情形。 测评单元(L3-ADS1-11) 应核查并测试访问控制策略的控制粒度是否达到主体为用户级,客体为文件、数据库表、记录或字段级。
		c) 标记与强制访问控制	测评单元(L3-ADS1-12)

		在对安全管理员进行身份鉴别和权限控制的基础上,应由安全管理员通过特定操作界面对主、客体进行安全标记;应按安全标记和强制访问控制规则,对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级,客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息,并实施相同的强制访问控制规则。	应核查是否依据安全策略对敏感信息资源设置了安全标记;应测试依据安全标记是否实现主体对客体的强制访问控制功能。
	d) 系统安全审计	应记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护;确保对特定安全事件进行报警;确保审计记录不被破坏或非授权访问。应为安全管理中心提供接口;对不能由系统独立处理的安全事件,提供由授权主体调用的接口。	测评单元 (L3-NCS1-23) 应核查设备是否开启了日志记录或安全审计功能;应核查是否部署了综合安全审计系统或类似功能的系统平台;应核查安全审计范围是否覆盖到每个用户;应核查是否对重要的用户行为和重要安全事件进行了审计。 测评单元 (L3-NCS1-24) 应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。 测评单元 (L3-NCS1-25) 应核查是否采取了技术措施对审计记录进行保护;应核查审计记录的备份机制和备份策略是否合理。 测评单元 (L3-NCS1-34) 应核查是否部署了相关系统平台能够对各类安全事件进行分析并通过声光等方式实时报警;应核查安全事件的监测范围是否能够覆盖网络所有关键路径。
	e) 用户数据完整性保护	应采用密码等技术支持的完整性	测评单元 (L3-ADS1-25) 应核查系统设计文档,鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和

		校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。	重要个人信息等在传输过程中是否采用了校验码技术或密码技术保证完整性；应测试在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。 测评单元（L3-ADS1-26） 应核查设计文档，是否采用校验码技术或密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；应测试在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。
	f) 用户数据保密性保护	应采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保护。	测评单元（L3-ADS1-27） 应核查系统设计文档，鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性；应通过嗅探等方式抓取传输过程中的数据包，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。 测评单元（L3-ADS1-28） 应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性；应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性。
	g) 客体安全重用	应采用具有安全客体复用功能的	测评单元（L3-ADS1-32） 应核查相关配置信息或访谈应用系统管理员，用

		系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。	户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。 测评单元（L3-ADS1-33） 应核查相关配置信息或访谈应用系统管理员，敏感数据所在的存储空间被释放或重新分配给其他用户前是否得到完全清除。
		h) 程序可信执行保护 可基于可信根对计算节点的BIOS、引导程序、操作系统内核、应用程序等进行可信验证，并在应用程序的关键执行环节对系统调用、中断、关键内存区域等进行可信验证，并在检测到其完整性受到破坏时采取措施恢复。	测评单元（L3-ECS1-23） 应核查防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库，或核查是否采用可信计算技术建立从系统到应用的信任链；应访谈系统管理员，核查是否有保护重要系统程序或文件完整性的措施；当检测到程序或文件受到破坏后，核查是否具备恢复的措施。
		i) 网络可信连接保护 应采用具有网络可信连接保护功能的系统软件或具有相应功能的信息技术产品，在设备连接网络时，对源和目标进行平台身份鉴别、平台完整性校验、数据传输的保密性和完整性保护等。	—
		j) 配置可信核查 应将系统的安全配置信息形成基准库，实时监控或定期检查配置信息的修改行为，及时修复和基准库中内容不符的配置信息。	测评单元（L3-ADS1-26） 应核查设计文档，是否采用校验码技术或密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；应测试在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。

7.3.2 安全区域边界设计技术要求	7.3.2.1 通用安全区域边界设计技术要求	a) 区域边界访问控制 应在安全区域边界设置自主和强制访问控制机制，应对源及目标计算节点的身份、地址、端口和应用协议等进行可信验证，对进出安全区域边界的数据信息进行控制，阻止非授权访问。	测评单元（L3-NCS1-12） 应核查在网络边界或区域之间是否部署访问控制设备，是否启用访问控制策略；应核查设备的最后一条访问控制策略是否为禁止所有网络通信。
		b) 区域边界包过滤 应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出该区域边界。	测评单元（L3-NCS1-12） 应核查在网络边界或区域之间是否部署访问控制设备，是否启用访问控制策略；应核查设备的最后一条访问控制策略是否为禁止所有网络通信。
		c) 区域边界安全审计 应在安全区域边界设置审计机制，由安全管理中心集中管理，并对确认的违规行为及时报警。	测评单元（L3-NCS1-23） 应核查设备是否开启了日志记录或安全审计功能；应核查是否部署了综合安全审计系统或类似功能的系统平台；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行了审计。 测评单元（L3-NCS1-24） 应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。
		d) 区域边界完整性保护 应在区域边界设置探测器，例如外接探测软件，探测非法外联和入侵行为，并及时报告安全管理中心。	测评单元（L3-NCS1-09） 应核查是否采用技术措施防止非授权设备接入内部网络并进行有效阻断；应核查所有路由器和交换机等相关设备闲置端口是否均已关闭。 测评单元（L3-NCS1-10） 应核查是否采用技术措施防止内部用户非法外联行为。
		a) 通信网络安全审计	测评单元（L3-NCS1-23）

信网络设计技术要求	用安全通信网络设计技术要求	应在安全通信网络设置审计机制，由安全管理中心集中管理，并对确认的违规行为进行报警。	应核查设备是否开启了日志记录或安全审计功能；应核查是否部署了综合安全审计系统或类似功能的系统平台；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行了审计。 测评单元（L3-NCS1-24） 应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。
		b) 通信网络数据传输完整性保护 应采用由密码技术支持的完整性校验机制，以实现通信网络数据传输完整性保护，并在发现完整性被破坏时进行恢复。	测评单元（L3-NCS1-06） 应核查是否在数据传输过程中使用校验码技术或密码技术来保证其完整性；应测试验证密码技术设备或组件是否保证通信过程中数据的完整性。
		c) 通信网络数据传输保密性保护 应采用由密码技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。	测评单元（L3-NCS1-07） 应核查是否在通信过程中采取保密措施，具体采用哪些技术措施；应测试验证在通信过程中是否对敏感信息字段或整个报文进行加密。
		d) 通信网络可信接入保护 可采用由可信根支持的可信网络连接机制，通过对连接到通信网络的设备进行可信验证，确保接入通信网络的设备真实可信，防止设备的非法接入。	测评单元（L3-NCS1-09） 应核查是否采用技术措施防止非授权设备接入内部网络并进行有效阻断；应核查所有路由器和交换机等相关设备闲置端口是否均已关闭。
7.3.4 安全管理中心设计技术要求	7.3.4.1 系统管理	可通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、可信基准库、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操	测评单元（L3-MMS1-15） 应核查网络和系统安全管理文档是否明确要求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）。 测评单元（L3-MMS1-16） 应访谈运维负责人是否指定专门的部门或人员进行账户管理；应核查相关审批记录或流程是否对申请账户、建立账户、删除账户等进行控制。

		作进行审计。	测评单元（L3-MMS1-17） 应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略，账户管理（用户责任、义务、风险、权限审批、权限分配、账户注销等），配置文件的生成、备份，变更审批、符合性检查等，授权访问，最小服务，升级与打补丁，审计日志，登录设备和系统的口令更新周期等方面。 测评单元（L3-ADS1-13） 应核查是否提供并启用了安全审计功能；应核查审计范围是否覆盖到每个用户；应核查并测试是否对重要的用户行为和重要安全事件进行审计。
	7.3.4.2 安全管理	应通过安全管理员对系统中的主体、客体进行统一标记，对主体进行授权，配置可信验证策略。 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并进行审计。	测评单元（L3-ORS1-04） 应访谈信息安全主管是否配备系统管理员、网络管理员和安全管理员；应核查人员配备文档是否明确各岗位人员配备情况。 测评单元（L3-ORS1-05） 应核查人员配备文档是否配备了专职安全管理员。 测评单元（L3-MMS1-17） 应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略，账户管理（用户责任、义务、风险、权限审批、权限分配、账户注销等），配置文件的生成、备份，变更审批、符合性检查等，授权访问，最小服务，升级与打补丁，审计日志，登录设备和系统的口令更新周期等方面。 测评单元（L3-ADS1-13） 应核查是否提供并启用了安全审计功能；应核查审计范围是否覆盖到每个用户；应核查并测试是否对重要的用户行为和重要安全事件进行审计。
	7.3.4.3 审计管理	应通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时	测评单元（L3-ORS1-04） 应访谈信息安全主管是否配备系统管理员、网络管理员和安全管理员；应核查人员配备文档是否明确各岗位人员配备情况。

		间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行及时处理。 应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。	测评单元（L3-MMS1-15） 应核查网络和系统安全管理文档是否明确要求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）。 测评单元（L3-ADS1-13） 应核查是否提供并启用了安全审计功能；应核查审计范围是否覆盖到每个用户；应核查并测试是否对重要的用户行为和重要安全事件进行审计。

C.1.4 第四级

适用范围	功能要求	设计要求	测评要求
8.3.1 安全计算环境设计技术要求	8.3.3.1 通用安全计算环境设计技术要求	a) 用户身份鉴别 应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录和重新连接系统时，采用受安全管理中心控制的口令、基于生物特征的数据、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，且其中一种鉴别技术产生的鉴别数据是不可替代的，并对鉴别数据进行保密性和完整性保护。	测评单元（L4-ECS1-01） 应核查用户在登录时是否采用了身份鉴别措施；应核查用户列表，查看用户身份标识是否具有唯一性。应核查用户配置或访谈系统管理员，查看是否存在空口令用户；应核查用户鉴别信息是否具有复杂度要求并定期更换。 测评单元（L4-ECS1-04） 应核查系统是否采用两种或两种以上组合的鉴别技术对用户身份进行鉴别，其中一种鉴别技术至少应使用密码技术或生物技术来实现； 测评单元（L4-ADS1-26） 应核查系统设计文档，鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了密码技术保证完整性；应测试在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。

		b) 自主访问控制 应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和（或）记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。	测评单元（L4-ECS1-05） 应测试网络管理员、安全管理员、系统管理员或核查用户账户和权限设置情况；应核查是否已禁用或限制匿名、默认账户的访问权限。 测评单元（L4-ADS1-11） 应核查是否由授权主体负责配置访问控制策略；应核查授权主体是否依据安全策略配置了主体对客体的访问规则；应测试非授权主体是否不能配置访问控制策略；应测试是否不存在可越权访问情形。 测评单元（L4-ADS1-12） 应核查并测试访问控制策略的控制粒度是否达到主体为用户级，客体为文件、数据库表、记录或字段级。
		c) 标记与强制访问控制 在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记，将强制访问控制扩展到所有主体与客体；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。	测评单元（L4-ADS1-13） 应核查是否依据安全策略对所有主体和客体设置了安全标记；应测试是否依据安全标记和强制访问控制规则确定主体对客体的访问。
		d) 系统安全审计 应记录系统相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；能对特定安全事件进行报警，终止违例进程等；确保审计记录不被破坏或非授权访问以及防止审计记录丢失等。应为安全管理中心	测评单元（L4-NCS1-25） 应核查设备是否开启了日志记录或安全审计功能；应核查是否部署了综合安全审计系统或类似功能的系统平台；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行了审计。 测评单元（L4-NCS1-26） 应核查审计记录信息是否包括事件的日期和时间、

		提供接口；对不能由系统独立处理的安全事件，提供由授权主体调用的接口。	用户、事件类型、事件是否成功及其他与审计相关的信息。 测评单元（L4-NCS1-27） 应核查是否采取了技术措施能够对审计记录进行保护；应核查审计记录的备份机制和备份策略是否合理。 测评单元（L4-NCS1-35） 应核查是否部署了相关系统平台能够对各类安全事件进行分析并通过声光等方式实时报警；应核查安全事件的监测范围是否能够覆盖网络所有关键路径。
		e) 用户数据完整性保护 应采用密码等技术支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。	测评单元（L4-ADS1-26） 应核查系统设计文档，鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了密码技术保证完整性；应测试在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。 测评单元（L4-ADS1-27） 应核查设计文档，是否采用了密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；应测试在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。
		f) 用户数据保密性保护	测评单元（L4-ADS1-29）

		采用密码等技术支持的保密性保护机制，对在安全计算环境中的用户数据进行保密性保护。	应核查系统设计文档，重鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性；应通过嗅探等方式抓取传输过程中的数据包，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。 测评单元（L4-ADS1-30） 应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性；应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性。
		g) 客体安全重用应 采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。	测评单元（L4-ADS1-35） 应核查相关配置信息或访谈应用系统管理员，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。 测评单元（L4-ADS1-36） 应核查相关配置信息或访谈应用系统管理员，敏感数据所在的存储空间被释放或重新分配给其他用户前是否得到完全清除。
		h) 程序可信执行保护 可基于可信计算技术对计算节点的BIOS、引导程序、操作系统内核、应用程序等进行可信验证，并在应用程序的所有执行环节对系统调用、中断、关键内存区域等进行可信验证，并在检测到其完整性受到破坏时采取措施恢复。	测评单元（L4-ECS1-23） 应核查是否采用基准库比对或其他可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证；应核查是否有保护重要系统程序或文件完整性的措施；当检测到程序或文件受到破坏后，核查是否具备恢复的措施。
		i) 网络可信连接保护 应采用具有网络可信连接保护功能的系统软件或具有相应功能的信息技术产品，在设备连接网络时，对源和目标进行平台身份鉴别、平台完整性校验、数据传输的保密性和完整性保护等。	测评单元（L4-NCS1-15） 应核查是否采用可信验证机制对接入到网络中的设备进行可信验证；应测试验证是否能够对连接到内部网络的设备进行可信验证。
		j) 配置可信核查	测评单元（L4-ADS1-27）

		应将系统的安全配置信息形成基准库，实时监控或定期检查配置信息的修改行为，及时修复和基准库中内容不符的配置信息。	应核查设计文档，是否采用了密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；应测试在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。
8.3.2 安全区域边界设计技术要求	8.3.2.1 通用安全区域边界设计技术要求	a) 区域边界访问控制 应在安全区域边界设置自主和强制访问控制机制，应对源及目标计算节点的身份、地址、端口和应用协议等进行可信验证，对进出安全区域边界的数据信息进行控制，阻止非授权访问。	测评单元（L4-NCS1-16） 应核查在网络边界或区域之间是否部署访问控制设备，是否启用访问控制策略；应核查设备的最后一条访问控制策略是否为禁止所有网络通信。
		b) 区域边界包过滤 应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出受保护的区域边界。	测评单元（L4-NCS1-16） 应核查在网络边界或区域之间是否部署访问控制设备，是否启用访问控制策略；应核查设备的最后一条访问控制策略是否为禁止所有网络通信。
		c) 区域边界安全审计 应在安全区域边界设置审计机制，通过安全管理中心集中管理，对确认的违规行为及时报警并做出相应处置。	测评单元（L4-NCS1-25） 应核查设备是否开启了日志记录或安全审计功能；应核查是否部署了综合安全审计系统或类似功能的系统平台；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行了审计。 测评单元（L4-NCS1-26） 应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

		d) 区域边界完整性保护 应在区域边界设置探测器, 例如外接探测软件, 探测非法外联和入侵行为, 并及时报告安全管理中心。	测评单元 (L4-NCS1-12) 应核查是否采用技术措施防止非授权设备接入内部网络, 并进行有效阻断; 应核查所有路由器和交换机等相关设备闲置端口是否均已关闭; 测评单元 (L4-NCS1-13) 应核查是否采用技术措施防止内部用户非法外联行为。
8.3.3 安全通信网络设计技术要求	8.3.3.1 通用安全通信网络设计技术要求	a) 通信网络安全审计 应在安全通信网络设置审计机制, 由安全管理中心集中管理, 并对确认的违规行为进行报警, 且做出相应处置。	测评单元 (L4-NCS1-25) 应核查设备是否开启了日志记录或安全审计功能; 应核查是否部署了综合安全审计系统或类似功能的系统平台; 应核查安全审计范围是否覆盖到每个用户; 应核查是否对重要的用户行为和重要安全事件进行了审计。 测评单元 (L4-NCS1-26) 应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。
		b) 通信网络数据传输完整性保护 应采用由密码等技术支持的完整性校验机制, 以实现通信网络数据传输完整性保护, 并在发现完整性被破坏时进行恢复。	测评单元 (L4-NCS1-07) 应核查是否在数据传输过程中使用密码技术来保证其完整性; 应测试验证密码技术设备或组件是否保证通信过程中数据的完整性。
		c) 通信网络数据传输保密性保护 采用由密码等技术支持的保密性保护机制, 以实现通信网络数据传输保密性保护。	测评单元 (L4-NCS1-08) 应核查是否在通信过程中采取保密措施, 具体采用哪些技术措施; 应测试验证在通信过程中是否对敏感信息字段或整个报文进行加密。
		d) 通信网络可信接入保护 可采用由可信根支持的可信网络连接机制, 通过对连接到通信网络的设备进行可信验证, 确保接入通信网络的设备真实可信, 防止设备的非法接入。	测评单元 (L4-NCS1-12) 应核查是否采用技术措施防止非授权设备接入内部网络, 并进行有效阻断; 应核查所有路由器和交换机等相关设备闲置端口是否均已关闭。
8.3.4 安全管	8.3.4.1 系	可通过系统管理员对系统的资源和运行进行配置、控制和管理, 包括用户身份、	测评单元 (L4-MMS1-16) 应核查网络和系统安全管理文档, 查看是否明确要

理中心设计技术要求	统管理	可信基准库、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。	求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）。 测评单元（L4-MMS1-17） 应访谈运维负责人是否指定专门的部门或人员进行账户管理；应核查相关审批记录或流程是否对申请账户、建立账户、删除账户等进行控制。 测评单元（L4-MMS1-18） 应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略，账户管理（用户责任、义务、风险、权限审批、权限分配、账户注销等），配置文件的生成、备份，变更审批、符合性核查等，授权访问，最小服务，升级与打补丁，审计日志，登录设备和系统的口令更新周期等方面。 测评单元（L4-ADS1-14） 应核查是否提供并启用了安全审计功能；应核查审计范围是否覆盖到每个用户；应核查并测试是否对重要的用户行为和重要安全事件进行审计。
	8.3.4.2 安全管理	应通过安全管理员对系统中的主体、客体进行统一标记，对主体进行授权，配置可信验证策略，并确保标记、授权和安全策略的数据完整性。 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并进行审计。	测评单元（L4-ORS1-04） 应访谈信息安全主管是否配备系统管理员、网络管理员和安全管理员；应核查人员配备文档是否明确各岗位人员配备情况。 测评单元（L4-ORS1-05） 应核查人员配备文档是否明确配备了专职安全管理员。 测评单元（L4-MMS1-18） 应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略，账户管理（用户责任、义务、风险、权限审批、权限分配、账户注销等），配置文件的生成、备份，变更审批、符合性核查等，授权访问，最小服务，升级与打补丁，审计日志，登录设备和系统的口令更新周期等方面。 测评单元（L4-ADS1-14）

			应核查是否提供并启用了安全审计功能；应核查审计范围是否覆盖到每个用户；应核查并测试是否对重要的用户行为和重要安全事件进行审计。
	8.3.4.3 审计管理	应通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行及时处理。 应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。	测评单元（L4-ORS1-04） 应访谈信息安全主管是否配备系统管理员、网络管理员和安全管理员；应核查人员配备文档是否明确各岗位人员配备情况。 测评单元（L4-MMS1-16） 应核查网络和系统安全管理文档，查看是否明确要求对网络和系统管理员用户进行分类，并定义各个角色的责任和权限（比如：划分不同的管理角色，系统管理权限与安全审计权限分离等）。 测评单元（L4-ADS1-14） 应核查是否提供并启用了安全审计功能；应核查审计范围是否覆盖到每个用户；应核查并测试是否对重要的用户行为和重要安全事件进行审计。
8.3.5 系统安全保护环境结构化设计技术要求	8.3.5.1 安全保护部件结构化设计技术要求	第四级系统安全保护环境各安全保护部件的设计应基于形式化的安全策略模型。安全保护部件应划分为关键安全保护部件和非关键安全保护部件，防止违背安全策略致使敏感信息从关键安全保护部件流向非关键安全保护部件。关键安全保护部件应划分功能层次，明确定义功能层次间的调用接口，确保接口之间的信息安全交换。	— —
	8.3.5.2 安全保护部件互联结构化设计技术要求	第四级系统各安全保护部件之间互联的接口功能及其调用关系应明确定义；各安全保护部件之间互联时，需要通过可信验证机制相互验证对方的可信性，确保安全保护部件间的可信连接。	— —
	8.3.5.3 重要参数结构	应对第四级系统安全保护环境设计实现的与安全策略相关的重要参数的数据结	— —

	化设计技术要求	构给出明确定义，包括参数的类型、使用描述以及功能说明等，并用可信验证机制确保数据不被篡改。	

C.2 云安全设计要求测评验证表

C.2.1 第一级

适用范围	功能要求	设计要求	测评要求
5.3.1 安全计算环境设计技术要求	5.3.1.2 云安全计算环境设计技术要求	a) 数据备份与恢复 应采取冗余架构或分布式架构设计；应支持数据多副本存储方式；应支持通用接口确保云服务客户可以将业务系统及数据迁移到其他云计算平台和本地系统，保证可移植性。	测评单元（L1-ADS1-08） 应核查是否按照备份策略进行本地备份；应核查备份策略设置是否合理、配置是否正确；应核查备份结果是否与备份策略一致；应核查近期恢复测试记录，查看是否能够进行正常的的数据恢复。 测评单元（L1-ADS2-02） 应核查云管理平台或云平台为云服务客户提供数据及备份存储位置的查询记录；应核查云服务商是否为云服务客户提供数据及备份存储位置查询的接口或其他技术、管理手段。
		b) 虚拟化安全 应实现虚拟机之间的 CPU、内存和存储空间安全隔离；应限制虚拟机对宿主机物理资源的直接访问；应支持不同云服务客户虚拟化网络之间安全隔离。	测评单元（L1-NCS2-04） 应核查云平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略是否有效；应核查云平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等是否有效；应核查不同云服务客户间访问控制规则和访问控制策略是否有效；应核查云服务客户业务系统不同区域间访问控制规则和访问控制策略是否有效。
		c) 恶意代码防范 物理机和宿主机应安装经过安全加固的操作系统或进行主机恶意代码防范；虚拟机应安装经过安全加固的操作系统或	测评单元（L1-ECS1-08） 应核查防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库。

		进行主机恶意代码防范；应支持对 Web 应用恶意代码检测和防护的能力。	
5.3.2 安全区域边界设计技术要求	5.3.2.2 云安全区域边界设计技术要求	a) 区域边界结构 安全应保证虚拟机只能接收到目的地址包括自己地址的报文或业务需求的广播报文，同时限制广播攻击。	测评单元（L1-NCS2-02） 应核查是否采用 VLAN、SDN 等技术手段隔离虚拟网络中不同租户的数据传输，保证云服务客户不能接收到目的地址中不包括自己的非广播数据包；应采用抓包等方式测试虚拟机是否只能接收到目的地址中仅包括自己地址的报文或业务需求的广播报文；应测试不同网段的虚拟机进行广播时，是否只能接收到目的地址中包括自己地址的报文或业务需求的广播报文。
		b) 区域边界访问控制 应保证当虚拟机迁移时，访问控制策略随其迁移；应允许云服务客户设置不同虚拟机之间的访问控制策略；应建立租户私有网络实现不同租户之间的安全隔离。	测评单元（L1-NCS2-05） 应核查虚拟机迁移时访问控制策略随之迁移的措施或手段；应核查虚拟机迁移记录及相关配置，查看虚拟机迁移后访问控制策略是否部署。 测评单元（L1-NCS2-04） 应核查云平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略是否有效；应核查云平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等是否有效；应核查不同云服务客户间访问控制规则和访问控制策略是否有效；应核查云服务客户业务系统不同区域间访问控制规则和访问控制策略是否有效。
5.3.3 安全通信网络设计技术要求	5.3.3.2 云安全通信网络设计技术要求	a) 通信网络传输保密性 应支持云服务客户远程通信数据保密性保护。	测评单元（L1-NCS1-03）应核查是否在数据传输过程中使用校验码技术来保护其完整性。

C.2.2 第二级

适用范围	功能要求	设计要求	测评要求

6.3.1 安全 计算环境设 计技术要求	6.3.1.2 云 安全计算环 境设计技术 要求	a) 用户身份鉴别 应支持注册到云计算服务的云服务客 户建立主子账号,并采用用户名和用户 标识符标识主子账号用户身份。	测评单元 (L4-ECS2-02) 应核查当进行远程管理时,是否建立双向身份验 证机制;应对管理终端和云计算平台进行渗透测 试,通过使用各种渗透测试技术(如口令猜解等) 对网络设备进行渗透测试,验证网络设备防护能 力是否符合要求,是否在管理终端和云计算平台 之间建立双向身份验证机制。
		b) 用户账户保护 应支持建立云服务客户账户体系,实现 主体与对虚拟机、云数据库、云网络、 云存储等客体的访问授权。	测评单元 (L2-ECS2-02) 应核查云服务客户数据管理权限授权流程、授权 方式、授权内容;应核查云计算平台是否具有云 服务客户数据的管理权限,如果具有,核查相关 授权证明及数据管理权限保护措施。
		c) 审计记录保护 应支持租户收集和查看与本租户资源 相关的审计信息,保证云服务商对云服 务客户系统和数据的访问操作可被租 户审计。	测评单元 (L2-ECS2-03) 应核查安全审计配置是否能够保证云服务商对云 服务客户系统和数据的操作(如增、删、改、查 等操作)可被云服务客户审计;应核查是否支持 云服务客户部署第三方安全审计设备,保证云服 务商对云服务客户系统和数据的操作可被租户审 计;应核查云服务商与云服务客户收集的审计数 据,查看云服务商对云服务客户系统和数据的操 作是否可被云服务客户审计。
		d) 数据备份与恢复 应采取冗余架构或分布式架构设计;应 支持数据多副本存储方式;应支持通用 接口确保云服务客户可以将业务系统 及数据迁移到其他云计算平台和本地 系统,保证可移植性。	测评单元 (L2-ADS2-02) 应核查云管理平台或云平台为云服务客户提供数 据及备份存储位置的查询记录;应核查云服务商 是否为云服务客户提供数据及备份存储位置查询 的接口或其他技术、管理手段。 测评单元 (L2-ADS2-03) 应访谈系统管理员是否采取措施使云服务客户可 以在本地保存其业务数据的备份;应核查是否提 供备份措施保证云服务客户可以在本地保存其业 务数据。
		e) 虚拟化安全 应实现虚拟机之间的 CPU、内存和存储	测评单元 (L2-ECS2-07) 应核查云管理平台和虚拟机监视器的计算资源分

		空间安全隔离；应限制虚拟机对宿主机物理资源的直接访问；应支持不同云服务客户虚拟化网络之间安全隔离。	配情况、资源分配的审计记录或告警记录是否存在内存资源过量占用警告；应核查云计算平台和虚拟机监视器的虚拟机内存隔离措施或机制。 测评单元（L2-ECS2-04） 应核查云管理平台等能否检测虚拟机对宿主机的异常访问。
		f) 恶意代码防范 物理机和宿主机应安装经过安全加固的操作系统或进行主机恶意代码防范；虚拟机应安装经过安全加固的操作系统或进行主机恶意代码防范；应支持对Web 应用恶意代码检测和防护的能力。	测评单元（L2-ECS1-16） 应核查防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库。
		g) 镜像和快照安全 应支持镜像和快照提供对虚拟机镜像和快照文件的完整性保护；防止虚拟机镜像、快照中可能存在的敏感资源被非授权访问；针对重要业务系统提供加固的操作系统镜像或支持对操作系统镜像进行自加固。	测评单元（L2-ECS2-08） 应核查虚拟机监视器是否有对镜像文件定期进行有效性验证的记录；应核查虚拟机监视器，云管理平台是否提供有效的虚拟机镜像和快照文件管理机制，虚拟机是否能够及时被备份和快照，以及是否准确地恢复到所需还原点；应核查虚拟机监视器，云管理平台是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。 测评单元（L2-ECS2-09） 应核查虚拟机监视器，云管理平台是否对生成的虚拟机镜像进行必要的加固措施，如关闭不必要的端口、服务及进行安全加固配置。
6.3.2 安全区域边界设计技术要求	6.3.2.2 云安全区域边界设计技术要求	a) 区域边界结构安全 应保证虚拟机只能接收到目的地址包括自己地址的报文或业务需求的广播报文，同时限制广播攻击。	测评单元（L2-NCS2-02） 应核查是否采用 VLAN、SDN 等技术手段隔离虚拟网络中不同租户的数据传输，保证云服务客户不能接收到目的地址中不包括自己的非广播数据包；应采用抓包等方式测试虚拟机是否只能接收到目的地址中仅包括自己地址的报文或业务需求的广播报文；应测试不同网段的虚拟机进行广播时，是否只能接收到目的地址中包括自己地址的

			报文或业务需求的广播报文。
		b) 区域边界访问控制 应保证当虚拟机迁移时，访问控制策略随其迁移；应允许云服务客户设置不同虚拟机之间的访问控制策略；应建立租户私有网络实现不同租户之间的安全隔离。	测评单元（L2-NCS2-07） 应核查云平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略是否有效；应核查云平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等是否有效；应核查不同云服务客户间访问控制规则和访问控制策略是否有效；应核查云服务客户业务系统不同区域间访问控制规则和访问控制策略是否有效。 测评单元（L2-NCS2-08） 应核查虚拟机迁移时访问控制策略随之迁移的措施或手段；应核查虚拟机迁移记录及相关配置，查看虚拟机迁移后访问控制策略是否部署。
		a) 通信网络传输保密性 应支持云服务客户远程通信数据保密性保护；	测评单元（L2-NCS2-05） 核查防火墙、入侵检测系统等设备，是否能为客户提供虚拟化的安全机制；核查虚拟防火墙、虚拟入侵保护系统等安全机制是否满足客户业务安全需求。 测评单元（L2-NCS1-05） 应访谈安全管理员是否在数据传输过程中使用校验码技术来保护其完整性；
6.3.3 安全通信网络设计技术要求	6.3.3.2 云安全通信网络设计技术要求	b) 通信网络安全审计 应支持租户收集和查看与本租户资源相关的审计信息；应保证云服务商对云服务客户通信网络的访问操作可被租户审计。	测评单元（L2-NCS2-13） 应核查对云服务商和云服务客户远程管理时执行的远程特权命令后是否有相关审计记录；当云服务商采用第三方运维时，应核查第三方运维方是否向云服务商提供审计数据，或云服务商是否可采取措施收集相关审计数据；应核查边界网络设备、网络虚拟化设备远程执行特权命令的限制措施，核查是否对远程执行特权命令的行为进行安全审计，至少包括虚拟机删除、虚拟机重启；应测试云服务商或云服务客户远程删除或重启虚拟机后，是否有产生相应审计记录。

6.3.4 安全管理中心设计技术要求	6.3.4.1 系统管理	在进行云计算平台安全设计时，安全管理应提供查询云服务客户数据及备份存储位置的方式。	测评单元（L2-ADS2-02） 应核查云管理平台或云平台为云服务客户提供数据及备份存储位置的查询记录；应核查云服务商是否为云服务客户提供数据及备份存储位置查询的接口或其他技术、管理手段。
	6.3.4.2 审计管理	在进行云计算平台安全设计时，云计算平台应对云服务器、云数据库、云存储等云服务的创建、删除等操作行为进行审计。	测评单元（L2-ECS2-03） 应核查安全审计配置是否能够保证云服务商对云服务客户系统和数据的操作（如增、删、改、查等操作）可被云服务客户审计；应核查是否支持云服务客户部署第三方安全审计设备，保证云服务商对云服务客户系统和数据的操作可被租户审计；应核查云服务商与云服务客户收集的审计数据，查看云服务商对云服务客户系统和数据的操作是否可被云服务客户审计。

C.2.3 第三级

适用范围	功能要求	设计要求	测评要求
7.3.1 安全计算环境设计技术要求	7.3.1.2 云安全计算环境设计技术要求	a) 用户身份鉴别 应支持注册到云计算服务的云服务客户建立主子账号，并采用用户名和用户标识符标识主子账号用户身份。	测评单元（L4-ECS2-02） 应核查当进行远程管理时，是否建立双向身份验证机制；应对管理终端和云计算平台进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）对网络设备进行渗透测试，验证网络设备防护能力是否符合要求，是否在管理终端和云计算平台之间建立双向身份验证机制。
		b) 用户账户保护 应支持建立云服务客户账户体系，实现主体与对虚拟机、云数据库、云网络、云存储等客体的访问授权。	测评单元（L3-ECS2-03） 应核查云服务客户数据管理权限授权流程、授权方式、授权内容；应核查云计算平台是否具有云服务客户数据的管理权限，如果具有，核查相关授权证明及数据管理权限保护措施；应测试数据库系统，验证云服务商是否不能对云服务客户非授权数据进行管理。
		c) 审计记录保护 应支持租户收集和查看与本租户资源相	测评单元（L3-ECS2-05） 应核查安全审计配置是否能够保证云服务商对云

		关的审计信息，保证云服务商对云服务客户系统和数据的访问操作可被租户审计。	服务客户系统和数据的操作（如增、删、改、查等操作）可被云服务客户审计；应核查是否支持云服务客户部署第三方安全审计设备，保证云服务商对云服务客户系统和数据的操作可被租户审计；应核查云服务商与云服务客户收集的审计数据，查看云服务商对云服务客户系统和数据的操作是否可被云服务客户审计。
		d) 数据保密性保护 应提供重要业务数据加密服务，加密密钥由租户自行管理；应提供加密服务，保证虚拟机在迁移过程中重要数据的保密性。	测评单元（ L3-ADS1-28） 应核查系统设计文档，重鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性；应通过嗅探等方式抓取传输过程中的数据包，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。 测评单元（ L3-ADS1-29） 应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性；应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性。 测评单元（ L3-ADS2-03） 当云服务客户已部署密钥管理解决方案，应核查密钥管理解决方案是否能确保云服务客户自行实现数据的加解密过程；应核查云服务商支持云服务客户部署密钥管理解决方案所采取的技术手段或管理措施是否能确保云服务客户自行实现数据的加解密过程。 测评单元（ L3-ADS2-02） 应核查虚拟机迁移过程中重要数据的保密措施是否能够有效防止迁移过程中重要数据的泄露；应核查是否采取加密或其他保护措施实现系统管理数据（如镜像文件、快照），鉴别信息和重要业务数据（如用户隐私数据）来保证虚拟机迁移过程中

			重要数据的保密性，防止迁移过程中重要数据的泄露；应核查是否使用密码技术确保虚拟机迁移过程中，重要数据的保密性。
		e) 数据备份与恢复 应采取冗余架构或分布式架构设计；应支持数据多副本存储方式；应支持通用接口确保云服务客户可以将业务系统及数据迁移到其他云计算平台和本地系统，保证可移植性。	测评单元（L3-ADS1-32） 应核查重要数据处理系统（包括边界交换机、边界防火墙、核心路由器、应用服务器和数据库服务器等）是否采用热冗余方式部署。 测评单元（L3-ADS2-08） 应核查云服务客户数据副本存储方式，核查是否存在若干个可用的副本；应核查各副本内容保持一致的技术措施或手段是否能保障云服务客户将业务系统及数据迁移到其他云计算平台和本地系统；应核查云服务商是否提供措施、手段或人员协助云服务客户完成迁移过程。 测评单元（L3-ADS2-07） 应访谈系统管理员采取了哪些技术手段保证云服务客户能够将业务系统及数据迁移到其他云计算平台和本地系统，是否协助云服务客户完成迁移过程；应核查相关技术手段是否能保障云服务客户将业务系统及数据迁移到其他云计算平台和本地系统；应核查云服务商是否提供措施、手段或人员协助云服务客户完成迁移过程。
		f) 虚拟化安全 应实现虚拟机之间的 CPU、内存和存储空间安全隔离，能检测到非授权管理虚拟机等情况，并进行告警；应限制虚拟机对宿主机物理资源的直接访问，应能对异常访问进行告警；应支持不同云服务客户虚拟化网络之间安全隔离；应监控物理机、宿主机、虚拟机的运行状态，并提供接口供安全管理中心集中监控。	测评单元（L3-ECS2-12） 应核查云管理平台和虚拟机监视器的计算资源分配情况、资源分配的审计记录或告警记录是否存在内存资源过量占用警告；应核查云计算平台和虚拟机监视器的虚拟机内存隔离措施或机制。 测评单元（L3-ECS2-07） 应核查服务器、宿主机及虚拟机，虚拟机监视器，云平台是否采取措施对不同虚拟机的 CPU、内存和磁盘资源进行隔离，是否实现不同云服务客户自有数据库之间的隔离；是否采取措施能够检测到虚拟机之间的资源隔离失效，并进行告警；应访

			谈系统管理员是否采取措施对不同虚拟机资源进行了安全隔离，是否采取措施能够检测到虚拟机之间的资源隔离失效，并进行告警。 测评单元（L3-NCS2-04） 应核查云服务客户之间虚拟网络隔离措施；应核查云服务客户之间虚拟网络资源隔离策略是否有效；应测试不同云服务客户之间的网络隔离措施是否生效。 测评单元（L3-NCS2-05） 核查向云服务客户提供的通信传输、边界防护、入侵防范等安全机制是否有效；核查虚拟防火墙、虚拟入侵保护系统等安全机制是否满足客户业务安全需求。
		g) 入侵防范 应支持对云服务客户进行行为监控，对云服务客户发起的恶意攻击或恶意对外连接进行检测和告警。	测评单元（L3-ECS1-22） 应访谈并核查入侵检测的措施，访谈是否部署了入侵检测工具；应核查重要节点的入侵行为记录和报警情况。 测评单元（L3-ECS2-08） 应核查服务器、宿主机及虚拟机，操作系统，数据库系统，虚拟机监视器，云平台是否能够检测到非授权新建虚拟机或者重新启用虚拟机，并进行告警。 测评单元（L3-NCS2-15） 应核查是否有专门设备对网络入侵进行防范，核查网络入侵防范规则库的升级方式；应核查网络入侵检测系统、入侵保护系统或机制，当采用网络入侵防范机制时所采取的机制是否已被测试是安全的（如第三方测试报告），核查入侵检测系统、入侵保护系统或机制的规则库是否为最新；应测试网络入侵检测系统、入侵保护系统或机制，当采用网络入侵防范机制时所采取的机制是否已被测试是安全的（如第三方测试报告），验证入侵检测系统、入侵保护系统或机制对异常流量和未知

		威胁的监控策略是否有效（如模拟产生攻击动作，验证网络入侵检测系统、入侵保护系统的反应，是否能记录攻击类型、攻击时间、攻击流量）；应核查系统是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能、报警功能和清洗处置功能；应核查是否具有对 SQL 注入、跨站脚本等攻击进行检测发现并阻断的能力；应具有对恶意虚拟机，如具有恶意行为、过分占用计算资源和带宽资源等的虚拟机，进行检测的能力；应核查云管理平台等对云服务客户攻击的防范措施，核查对云服务客户的网络攻击行为的记录情况，记录应包括攻击类型、攻击时间、攻击流量等；应测试网络入侵检测系统、入侵保护系统或机制，验证其云服务客户网络攻击报警报警策略是否有效（如模拟产生攻击动作，验证网络入侵检测系统、入侵保护系统是否能实时报警）；应对云平台内部发起的恶意攻击或恶意对外连接的行为进行限制，核查是否对内部行为进行监控且保存相关日志记录；应通过对外攻击发生器伪造对外攻击行为，核查云租的网络攻击的日志记录，确认是否正确记录到相应攻击行为，攻击行为日志记录是否包含攻击类型、攻击时间、攻击者 IP、攻击流量规模等；应核查运行虚拟机监控器（VMM）和云管理平台软件的物理主机，核查其安全加固手段是否能够应对虚拟化共享带来的安全漏洞。	威胁的监控策略是否有效（如模拟产生攻击动作，验证网络入侵检测系统、入侵保护系统的反应，是否能记录攻击类型、攻击时间、攻击流量）；应核查系统是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能、报警功能和清洗处置功能；应核查是否具有对 SQL 注入、跨站脚本等攻击进行检测发现并阻断的能力；应具有对恶意虚拟机，如具有恶意行为、过分占用计算资源和带宽资源等的虚拟机，进行检测的能力；应核查云管理平台等对云服务客户攻击的防范措施，核查对云服务客户的网络攻击行为的记录情况，记录应包括攻击类型、攻击时间、攻击流量等；应测试网络入侵检测系统、入侵保护系统或机制，验证其云服务客户网络攻击报警报警策略是否有效（如模拟产生攻击动作，验证网络入侵检测系统、入侵保护系统是否能实时报警）；应对云平台内部发起的恶意攻击或恶意对外连接的行为进行限制，核查是否对内部行为进行监控且保存相关日志记录；应通过对外攻击发生器伪造对外攻击行为，核查云租的网络攻击的日志记录，确认是否正确记录到相应攻击行为，攻击行为日志记录是否包含攻击类型、攻击时间、攻击者 IP、攻击流量规模等；应核查运行虚拟机监控器（VMM）和云管理平台软件的物理主机，核查其安全加固手段是否能够应对虚拟化共享带来的安全漏洞。
		h) 恶意代码防范 物理机和宿主机应安装经过安全加固的操作系统或进行主机恶意代码防范；虚拟机应安装经过安全加固的操作系统或进行主机恶意代码防范；应支持对 Web 应用恶意代码检测和防护的能力。	测评单元（L3-ECS1-23） 应核查防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库，或核查是否采用可信计算技术建立从系统到应用的信任链；应访谈系统管理员，核查是否有保护重要系统程序或文件完整性的措施；应当检测到程序或文件受到破坏后，是否具备恢复的措施。 测评单元（L3-ECS2-09）

			应核查服务器、宿主机、虚拟机、终端、虚拟机监视器、云平台是否建立恶意代码传播路径追踪机制，是否可以检测查看恶意代码的感染情况，并提出告警。应核查服务器、宿主机、虚拟机、终端，虚拟机监视器，云平台是否能够检测恶意代码感染及在虚拟机间蔓延的情况，是否能够检测出虚拟机的恶意行为，并提出告警。
		i) 镜像和快照安全 应支持镜像和快照提供对虚拟机镜像和快照文件的完整性保护；防止虚拟机镜像、快照中可能存在的敏感资源被非授权访问；针对重要业务系统提供加固的操作系统镜像或支持对操作系统镜像进行自加固。	测评单元（L3-ECS2-15） 应核查虚拟机监视器是否有对镜像文件定期进行有效性验证的记录；应核查虚拟机监视器，云管理平台是否提供有效的虚拟机镜像和快照文件管理机制，虚拟机是否能够及时被备份和快照，以及是否准确地恢复到所需还原点；应核查虚拟机监视器，云管理平台是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。 测评单元（L3-ECS2-16） 应核查虚拟机监视器，云管理平台是否对生成的虚拟机镜像进行必要的加固措施，如关闭不必要的端口、服务及进行安全加固配置。 测评单元（L3-ECS2-17） 应核查虚拟机监视器，云管理平台是否对虚拟机镜像或快照中的敏感资源，通过加密、访问控制、权限控制等技术手段进行保护，防止可能存在的针对快照的非法访问。
7.3.2 安全区域边界设计技术要求	7.3.2.2 云安全区域边界设计技术要求	a) 区域边界结构安全 应保证虚拟机只能接收到目的地址包括自己地址的报文或业务需求的广播报文，同时限制广播攻击；应实现不同租户间虚拟网络资源之间的隔离，并避免网络资源过量占用；应保证云计算平台管理流量与云服务客户业务流量分离；	测评单元（L3-NCS2-02） 应核查是否采用 VLAN、SDN 等技术手段隔离虚拟网络中不同租户的数据传输，保证云服务客户不能接收到目的地址中不包括自己的非广播数据包；应采用抓包等方式测试虚拟机是否只能接收到目的地址中仅包括自己地址的报文或业务需求的广播报文；应测试不同网段的虚拟机进行广播时，是否只能接收到目的地址中包括自己地址的

		应能够识别、监控虚拟机之间、虚拟机与物理机之间的网络流量；提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云平台选择第三方安全服务。	报文或业务需求的广播报文；应核查是否具备限制广播攻击的措施防止不同云服务客户间的虚拟机地址欺骗。 测评单元（L3-NCS2-04） 应核查云服务客户之间虚拟网络隔离措施；应核查云服务客户之间虚拟网络资源隔离策略是否有效；应测试不同云服务客户之间的网络隔离措施是否生效。
		b) 区域边界访问控制 应保证当虚拟机迁移时，访问控制策略随其迁移；应允许云服务客户设置不同虚拟机之间的访问控制策略；应建立租户私有网络实现不同租户之间的安全隔离。	测评单元（L3-NCS2-11） 应核查云平台和云服务客户业务系统虚拟化网络边界访问控制规则和访问控制策略是否有效；应核查云平台的网络边界设备或虚拟化网络边界设备安全保障机制、访问控制规则和访问控制策略等是否有效；应核查不同云服务客户间访问控制规则和访问控制策略是否有效；应核查云服务客户业务系统不同区域间访问控制规则和访问控制策略是否有效；应测试虚拟化网络边界访问控制设备，验证是否可以正确拒绝违反访问控制规则的非法访问。 测评单元（L3-NCS2-13） 应核查云服务商的云管理平台等是否允许云服务客户设置不同虚拟机间访问控制策略；应核查云服务商的云管理平台是否存在不同虚拟机间的访问控制管理模块，是否开启该访问控制功能；应核查云服务客户管理系统，不同虚拟机间访问控制策略是否安全；应测试虚拟化网络边界访问控制设备是否可以正确拒绝违反虚拟机间访问控制策略的非法访问。
		c) 区域边界入侵防范 当虚拟机迁移时，入侵防范机制可应用于新的边界处；应将区域边界入侵防范机制纳入安全管理中心统一管理。	测评单元（L3-NCS2-15） 应核查是否有专门设备对网络入侵进行防范，核查网络入侵防范规则库的升级方式；应核查网络入侵检测系统、入侵保护系统或机制，当采用网络入侵防范机制时所采取的机制是否已被测试是

			安全的（如第三方测试报告），核查入侵检测系统、入侵保护系统或机制的规则库是否为最新；应测试网络入侵检测系统、入侵保护系统或机制，当采用网络入侵防范机制时所采取的机制是否已被测试是安全的（如第三方测试报告），验证入侵检测系统、入侵保护系统或机制对异常流量和未知威胁的监控策略是否有效（如模拟产生攻击动作，验证网络入侵检测系统、入侵保护系统的反应，是否能记录攻击类型、攻击时间、攻击流量）；应核查系统是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能、报警功能和清洗处置功能；应核查是否具有对 SQL 注入、跨站脚本等攻击进行检测发现并阻断的能力；应具有对恶意虚拟机，如具有恶意行为、过分占用计算资源和带宽资源等的虚拟机，进行检测的能力；应核查云管理平台等对云服务客户攻击的防范措施，核查对云服务客户的网络攻击行为的记录情况，记录应包括攻击类型、攻击时间、攻击流量等；应测试网络入侵检测系统、入侵保护系统或机制，验证其云服务客户网络攻击报警报警策略是否有效（如模拟产生攻击动作，验证网络入侵检测系统、入侵保护系统是否能实时报警）；应对云平台内部发起的恶意攻击或恶意对外连接的行为进行限制，核查是否对内部行为进行监控且保存相关日志记录；应通过对外攻击发生器伪造对外攻击行为，核查云租的网络攻击的日志记录，确认是否正确记录到相应攻击行为，攻击行为日志记录是否包含攻击类型、攻击时间、攻击者 IP、攻击流量规模等；应核查运行虚拟机监控器（VMM）和云管理平台软件的物理主机，核查其安全加固手段是否能够应对虚拟化共享带来的安全漏洞。
		d) 区域边界审计要求	测评单元（L3-NCS2-19） 应核查对云服务商和云服务客户远程管理时执行

		根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据；根据云服务商和云服务客户的职责划分，实现各自控制部分的集中审计；当发生虚拟机迁移或虚拟资源变更时，安全审计机制可应用于新的边界处；为安全审计数据的汇集提供接口，并可供第三方审计。	的远程特权命令后是否有相关审计记录；当云服务商采用第三方运维时，应核查第三方运维方是否向云服务商提供审计数据，或云服务商是否可采取措施收集相关审计数据；应核查边界网络设备、网络虚拟化设备远程执行特权命令的限制措施，核查是否对远程执行特权命令的行为进行安全审计，至少包括虚拟机删除、虚拟机重启；应测试云服务商或云服务客户远程删除或重启虚拟机后，是否有产生相应审计记录。 测评单元（L3-NCS2-20） 应核查云服务商审计数据收集系统或设备是否根据云服务商和云服务客户的职责划分，实现各自控制部分审计数据的收集；如果云服务客户授权云服务商收集部分云服务客户控制的审计数据，应核查云服务商是否在不影响其他云服务客户安全的前提下将云服务客户审计数据提供给云服务客户；应核查云服务商审计数据是否不包括云服务客户控制部分的审计数据。
7.3.3 安全通信网络设计技术要求	7.3.3.2 云安全通信网络设计技术要求	a) 通信网络传输保密性 应支持云服务客户远程通信数据保密性保护；	测评单元（L3-NCS1-07） 应核查是否在通信过程中采取保密措施，具体采用哪些技术措施；应测试验证在通信过程中是否对敏感信息字段或整个报文进行加密。
		b) 通信网络可信接入保护 应禁止通过互联网直接访问云计算平台物理网络；应提供开放接口，允许接入可信的第三方安全产品。	测评单元（L3-NCS2-09） 应核查接口设计文档或开放性服务技术文档是否符合开放性、安全性要求；如果提供开放接口，应核查内部通信网络（虚拟网络）为第三方安全产品所提供的开放接口安全保障机制、接口配置或参数是否符合安全需求；如果提供开放性安全产品、服务，应核查开放性安全产品及服务的服务内容和实现开放性安全服务所采用的技术手段、安全保障机制是否符合安全需求。

		c) 通信网络安全审计 应支持租户收集和查看与本租户资源相关的审计信息；应保证云服务商对云服务客户通信网络的访问操作可被租户审计。	测评单元（L3-NCS2-19） 应核查对云服务商和云服务客户远程管理时执行的远程特权命令后是否有相关审计记录；当云服务商采用第三方运维时，应核查第三方运维方是否向云服务商提供审计数据，或云服务商是否可采取措施收集相关审计数据；应核查边界网络设备、网络虚拟化设备远程执行特权命令的限制措施，核查是否对远程执行特权命令的行为进行安全审计，至少包括虚拟机删除、虚拟机重启；应测试云服务商或云服务客户远程删除或重启虚拟机后，是否有产生相应审计记录。 测评单元（L3-NCS2-20） 应核查云服务商审计数据收集系统或设备是否根据云服务商和云服务客户的职责划分，实现各自控制部分审计数据的收集；如果云服务客户授权云服务商收集部分云服务客户控制的审计数据，应核查云服务商是否在不影响其他云服务客户安全的前提下将云服务客户审计数据提供给云服务客户；应核查云服务商审计数据是否不包括云服务客户控制部分的审计数据。
7.3.4 安全管理中心设计技术要求	7.3.4.1 系统管理	在进行云计算平台安全设计时，安全管理应提供查询云服务客户数据及备份存储位置的方式；云计算平台的运维应在中国境内，禁止从境外对境内云计算平台的运维。	测评单元（L3-ADS2-04） 应核查云管理平台或云平台为云服务客户提供数据及备份存储位置的查询记录；应核查云服务商是否为云服务客户提供数据及备份存储位置查询的接口或其他技术、管理手段。 测评单元（L3-MMS2-01） 应核查运维地点是否位于中国境内，是否不存在从境外对境内云计算平台实施远程运维的设备、地点和相关内容；应核查云计算平台远程运维记录中境外对境内云计算平台实施运维操作是否遵循国家相关规定。 测评单元（L3-MMS2-02） 应核查云计算平台运维过程产生的配置数据、日志信息等是否存储于中国境内；对于有出境需求

			的配置数据和日志信息，应核查数据出境是否遵循国家相关规定。
	7.3.4.2 安全管理	在进行云计算平台安全设计时，安全管理应具有对攻击行为回溯分析以及对网络安全事件进行预测和预警的能力；应具有对网络安全态势进行感知、预测和预判的能力。	测评单元（L3-CMS2-08） 应访谈云服务商安全主管是否供应商的重要变更是否及时传达到云服务客户，并且对带来的安全风险进行评估，并采取有关措施对风险进行控制；应核查系统，确认供应链安全事件信息或威胁信息是否能够及时传达到云服务客户。 测评单元（L3-CMS2-09） 应核查安全风险评估报告和风险预案，确认对每次供应商的重要变更都进行评估与风险预案设计。
	7.3.4.3 审计管理	在进行云计算平台安全设计时，云计算平台应对云服务器、云数据库、云存储等云服务的创建、删除等操作行为进行审计；应通过运维审计系统对管理员的运维行为进行安全审计；应通过租户隔离机制，确保审计数据隔离的有效性。	测评单元（L3-ECS2-05） 应核查安全审计配置是否能够保证云服务商对云服务客户系统和数据的操作（如增、删、改、查等操作）可被云服务客户审计；应核查是否支持云服务客户部署第三方安全审计设备，保证云服务商对云服务客户系统和数据的操作可被租户审计；应核查云服务商与云服务客户收集的审计数据，查看云服务商对云服务客户系统和数据的操作是否可被云服务客户审计。 测评单元（L3-ADS2-06） 应核查云服务客户是否不能访问其他云服务客户审计数据；应核查是否采取云服务客户审计数据隔离存放措施。

C.2.4 第四级

适用范围	功能要求	设计要求	测评要求
8.3.1 安全计算环境设计技术	8.3.1.2 云安全计算环境设计技术	a) 用户身份鉴别 应支持注册到云计算服务的云服务客户建立主子账户，并采用用户名和用户标识符标识主子账户用户身份；当进行远	测评单元（L4-ECS2-02） 应核查当进行远程管理时，是否建立双向身份验证机制；应对管理终端和云计算平台进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）

术要求	要求	程管理时，管理终端和云计算平台边界设备之间应建立双向身份验证机制。	对网络设备进行渗透测试，验证网络设备防护能力是否符合要求，是否在管理终端和云计算平台之间建立双向身份验证机制。
	b) 用户账户保护	应支持建立云服务客户账户体系，实现主体与对虚拟机、云数据库、云网络、云存储等客体的访问授权。	测评单元（L4-ECS2-03） 应核查云服务客户数据管理权限授权流程、授权方式、授权内容；应核查云计算平台是否具有云服务客户数据的管理权限，如果具有，核查相关授权证明及数据管理权限保护措施；应测试数据库系统，验证云服务商是否不能对云服务客户非授权数据进行管理；
	c) 审计记录保护	应支持租户收集和查看与本租户资源相关的审计信息，保证云服务商对云服务客户系统和数据的访问操作可被租户审计。	测评单元（L4-ECS2-05） 应核查安全审计配置是否能够保证云服务商对云服务客户系统和数据的操作（如增、删、改、查等操作）可被云服务客户审计；应核查是否支持云服务客户部署第三方安全审计设备，保证云服务商对云服务客户系统和数据的操作可被租户审计；应核查云服务商与云服务客户收集的审计数据，查看云服务商对云服务客户系统和数据的操作是否可被云服务客户审计。
	d) 数据保密性保护	应提供重要业务数据加密服务，加密密钥由租户自行管理；应提供加密服务，保证虚拟机在迁移过程中重要数据的保密性。	测评单元（L4-ADS1-30） 应核查系统设计文档，重鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性；应通过嗅探等方式抓取传输过程中的数据包，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。 测评单元（L4-ADS1-30） 应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性；应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性。 测评单元（L4-ADS2-03）

		当云服务客户已部署密钥管理解决方案，应核查密钥管理解决方案是否能确保云服务客户自行实现数据的加解密过程；应核查云服务商支持云服务客户部署密钥管理解决方案所采取的技术手段或管理措施是否能确保云服务客户自行实现数据的加解密过程； 测评单元（ L4-ADS2-02） 应核查虚拟机迁移过程中重要数据的保密措施是否能有效防止迁移过程中重要数据的泄露；应核查是否采取加密或其他保护措施实现系统管理数据（如镜像文件、快照），鉴别信息和重要业务数据（如用户隐私数据）来保证虚拟机迁移过程中重要数据的保密性，防止迁移过程中重要数据的泄露；应核查是否使用密码技术确保虚拟机迁移过程中，重要数据的保密性。	
		e) 数据备份与恢复 应采取冗余架构或分布式架构设计；应支持数据多副本存储方式；应支持通用接口确保云服务客户可以将业务系统及数据迁移到其他云计算平台和本地系统，保证可移植性。	测评单元（ L4-ADS1-34） 应核查重要数据处理系统（包括边界交换机、边界防火墙、核心路由器、应用服务器和数据库服务器等）是否采用热冗余方式部署。 测评单元（ L4-ADS2-08） 应核查云服务客户数据副本存储方式，核查是否存在若干个可用的副本；应核查各副本内容保持一致的技术措施或手段是否能保障云服务客户将业务系统及数据迁移到其他云计算平台和本地系统；应核查云服务商是否提供措施、手段或人员协助云服务客户完成迁移过程。 测评单元（L4-ADS2-07） 应访谈系统管理员采取了哪些技术手段保证云服务客户能够将业务系统及数据迁移到其他云计算平台和本地系统，是否协助云服务客户完成迁移过程；应核查相关技术手段是否能保障云服务客户将业务系统及数据迁移到其他云计算平台和本地系统；应核查云服务商是否提供措施、手段或

			人员协助云服务客户完成迁移过程。
		f) 虚拟化安全 应实现虚拟机之间的 CPU、内存和存储空间安全隔离，能检测到非授权管理虚拟机等情况，并进行告警；应限制虚拟机对宿主机物理资源的直接访问，应能对异常访问进行告警；应支持不同云服务客户虚拟化网络之间安全隔离；应监控物理机、宿主机、虚拟机的运行状态，并提供接口供安全管理中心集中监控。	测评单元（L4-ECS2-12） 应核查云管理平台和虚拟机监视器的计算资源分配情况、资源分配的审计记录或告警记录是否不存在内存资源过量占用警告；应核查云计算平台和虚拟机监视器的虚拟机内存隔离措施或机制。 测评单元（L4-ECS2-07） 应核查服务器、宿主机及虚拟机，虚拟机监视器，云平台是否采取措施对不同虚拟机的 CPU、内存和磁盘资源进行隔离，是否实现不同云服务客户自有数据库之间的隔离；是否采取措施能够检测到虚拟机之间的资源隔离失效，并进行告警；应访谈系统管理员是否采取措施对不同虚拟机资源进行了安全隔离，是否采取措施能够检测到虚拟机之间的资源隔离失效，并进行告警。
		g) 入侵防范 应支持对云服务客户进行行为监控，对云服务客户发起的恶意攻击或恶意对外连接进行检测和告警。	测评单元（L4-ECS1-22） 应访谈并核查入侵检测的措施，访谈是否部署了入侵检测工具；应核查重要节点的入侵行为记录和报警情况。 测评单元（L4-ECS2-08） 应核查服务器、宿主机及虚拟机，操作系统，数据库系统，虚拟机监视器，云平台是否能够检测到非授权新建虚拟机或者重新启用虚拟机，并进行告警。
		h) 恶意代码防范 物理机和宿主机应安装经过安全加固的操作系统或进行主机恶意代码防范；虚拟机应安装经过安全加固的操作系统或进行主机恶意代码防范；应支持对 Web 应用恶意代码检测和防护的能力。	测评单元（L4-ECS1-23） 应核查是否采用基准库比对或其他可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证；应核查是否有保护重要系统程序或文件完整性的措施；当检测到程序或文件受到破坏后，核查是否具备恢复的措施。 测评单元（L4-ECS2-09） 应核查服务器、宿主机、虚拟机、终端、虚拟机监视器、云平台是否建立恶意代码传播路径追踪

			机制，是否可以检测查看恶意代码的感染情况，并告警后及时处理；应核查服务器、宿主机、虚拟机、终端，虚拟机监视器，云平台是否能够检测恶意代码感染及在虚拟机间蔓延的情况，是否能够检测出虚拟机的恶意行为，并告警后及时处理。
		i) 镜像和快照安全 应支持镜像和快照提供对虚拟机镜像和快照文件的完整性保护；防止虚拟机镜像、快照中可能存在的敏感资源被非授权访问；针对重要业务系统提供加固的操作系统镜像或支持对操作系统镜像进行自加固。	测评单元（L4-ECS2-15） 应核查虚拟机监视器是否有对镜像文件定期进行有效性验证的记录；应核查虚拟机监视器，云管理平台是否提供有效的虚拟机镜像和快照文件管理机制，虚拟机是否能够及时被备份和快照，以及是否准确地恢复到所需还原点；应核查虚拟机监视器，云管理平台是否对快照功能生成的镜像或快照文件进行完整性校验，是否具有严格的校验记录机制，防止虚拟机镜像或快照被恶意篡改。 测评单元（L4-ECS2-17） 应核查虚拟机监视器，云管理平台是否对虚拟机镜像或快照中的敏感资源，通过加密、访问控制、权限控制等技术手段进行保护，防止可能存在的针对快照的非法访问。 测评单元（L4-ECS2-17） 应核查虚拟机监视器，云管理平台是否对生成的虚拟机镜像进行必要的加固措施，如关闭不必要的端口、服务及进行安全加固配置。
		j) 数据备份与恢复 应建立异地灾难备份中心，提供业务应用的实时切换。	测评单元（L4-ADS1-35） 应核查是否建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备；应核查是否提供业务应用的实时切换功能。
8.3.2 安全区域边界设计技术要求	8.3.2.2 云安全区域边界设计技术要求	a) 区域边界结构安全 应保证虚拟机只能接收到目的地址中包括自己地址的报文或业务需求的广播报文，同时限制广播攻击；应实现不同租户间虚拟网络资源之间的隔离，并避免	测评单元（L4-NCS2-02） 应核查是否采用 VLAN、SDN 等技术手段隔离虚拟网络中不同租户的数据传输，保证云服务客户不能接收到目的地址中不包括自己的非广播数据包；应采用抓包等方式测试虚拟机是否只能接收

		网络资源过量占用；应保证云计算平台管理流量与云服务客户业务流量分离；保证信息系统的外部通信接口经授权后方可传输数据；应确保云计算平台具有独立的资源池；应能够识别、监控虚拟机之间、虚拟机；物理机之间的网络流量；提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云平台选择第三方安全服务；应确保云服务客户的四级业务应用系统具有独立的资源池。	到目的地址中仅包括自己地址的报文或业务需求的广播报文；应测试不同网段的虚拟机进行广播时，是否只能接收到目的地址中包括自己地址的报文或业务需求的广播报文；应核查是否具备限制广播攻击的措施防止不同云服务客户间的虚拟机地址欺骗。 测评单元（L4-NCS2-04） 应核查云服务客户之间虚拟网络隔离措施；应核查云服务客户之间虚拟网络资源隔离策略是否有效；应测试不同云服务客户之间的网络隔离措施是否生效。 测评单元（L4-NCS2-07） 应核查网络架构和配置策略能否采用带外管理或策略配置等方式实现管理流量和业务流量分离；应核查云平台管理流量与云服务客户业务流量是否分离，核查所采取的技术手段和流量分离手段；应测试云计算平台管理流量与业务流量是否分离。 测评单元（L4-NCS2-08） 应核查同一宿主机内虚拟机之间、虚拟机与物理机之间流量是否能被识别、监控，并在发现异常流量时提供报警；应核查不同宿主机的虚拟机之间、虚拟机与物理机之间流量是否能被识别、监控，并在发现异常流量时提供报警。 测评单元（L4-NCS2-09） 应核查接口设计文档或开放性服务技术文档是否符合开放性、安全性要求；如果提供开放接口，应核查内部通信网络（虚拟网络）为第三方安全产品所提供的开放接口安全保障机制、接口配置或参数是否符合安全需求；如果提供开放性安全产品、服务，应核查开放性安全产品及服务的服务内容和实现开放性安全服务所采用的技术手段、安全保障机制是否符合安全需求；

			测评单元（L4-NCS2-10） 应核查云平台建设方案中是否对承载四级业务系统的资源池做出独立划分设计；应核查网络结构中是否对四级业务系统划分独立的资源池。
		b) 区域边界访问控制 应保证当虚拟机迁移时，访问控制策略随其迁移；应允许云服务客户设置不同虚拟机之间的访问控制策略；应建立租户私有网络实现不同租户之间的安全隔离；应在网络边界处部署监控机制，对进出网络的流量实施有效监控。	测评单元（L4-NCS2-13） 应核查虚拟机迁移时访问控制策略随之迁移的措施或手段；应核查虚拟机迁移记录及相关配置，查看虚拟机迁移后访问控制策略是否部署；应测试虚拟机迁移，验证访问控制措施是否随其迁移。 测评单元（L4-NCS2-14） 应核查云服务商的云管理平台等是否允许云服务客户设置不同虚拟机间访问控制策略；应核查云服务商的云管理平台是否存在不同虚拟机间的访问控制管理模块，是否开启该访问控制功能；应核查云服务客户管理系统，不同虚拟机间访问控制策略是否安全；应测试虚拟化网络边界访问控制设备是否可以正确拒绝违反虚拟机间访问控制策略的非法访问； 测评单元（L4-NCS2-04） 应核查云服务客户之间虚拟网络隔离措施；应核查云服务客户之间虚拟网络资源隔离策略是否有效；应测试不同云服务客户之间的网络隔离措施是否生效。
		c) 区域边界入侵防范 当虚拟机迁移时，入侵防范机制可应用于新的边界处；应将区域边界入侵防范机制纳入安全管理中心统一管理；应在关键区域边界处部署相应形态的文件级代码检测或文件运行行为检测的安全系统，对恶意代码进行检测和清除。	测评单元（L4-NCS2-13） 应核查虚拟机迁移时访问控制策略随之迁移的措施或手段；应核查虚拟机迁移记录及相关配置，查看虚拟机迁移后访问控制策略是否部署；应测试虚拟机迁移，验证访问控制措施是否随其迁移。 测评单元（L4-NCS2-16） 应核查是否有专用设备对网络入侵进行防范，核查网络入侵防范规则库的升级方式；应核查网络入侵检测系统、入侵保护系统或机制，当采用网络入侵防范机制时所采取的机制是否已被测试是

			安全的（如第三方测试报告），核查入侵检测系统、入侵保护系统或机制的规则库是否为最新；应测试网络入侵检测系统、入侵保护系统或机制，当采用网络入侵防范机制时所采取的机制是否已被测试是安全的（如第三方测试报告），验证入侵检测系统、入侵保护系统或机制对异常流量和未知威胁的监控策略是否有效（如模拟产生攻击动作，验证网络入侵检测系统、入侵保护系统的反应，是否能记录攻击类型、攻击时间、攻击流量）；应核查系统是否具备异常流量、大规模攻击流量、高级持续性攻击的检测功能、报警功能；应核查是否具有对 SQL 注入、跨站脚本等攻击进行检测发现的能力；应具有对恶意虚拟机，如具有恶意行为、过分占用计算资源和带宽资源等的虚拟机，进行检测的能力；应核查云管理平台等对云服务客户攻击的防范措施，核查对云服务客户的网络攻击行为的记录情况，记录应包括攻击类型、攻击时间、攻击流量等；应测试网络入侵检测系统、入侵保护系统或机制，验证其云服务客户网络攻击报警策略是否有效（如模拟产生攻击动作，验证网络入侵检测系统、入侵保护系统是否能实时报警）；应对云平台内部发起的恶意攻击或恶意对外连接的行为进行限制，核查是否对内部行为进行监控且保存相关日志记录；应通过对外攻击发生器伪造对外攻击行为，核查云租的网络攻击的日志记录，确认是否正确记录到相应攻击行为，攻击行为日志记录是否包含攻击类型、攻击时间、攻击者 IP、攻击流量规模等；应核查运行虚拟机监控器（VMM）和云管理平台软件的物理主机，核查其安全加固手段是否能够应对虚拟化共享带来的安全漏洞。
		d) 区域边界审计要求 根据云服务商和云服务客户的职责划	测评单元（L4-NCS2-21） 应核查云服务商审计数据收集系统或设备是否根

		分，收集各自控制部分的审计数据；根据云服务商和云服务客户的职责划分，实现各自控制部分的集中审计；当发生虚拟机迁移或虚拟资源变更时，安全审计机制可应用于新的边界处；为安全审计数据的汇集提供接口，并可供第三方审计；确认的违规行为及时报警并做出相应处置。	据云服务商和云服务客户的职责划分，实现各自控制部分审计数据的收集；如果云服务客户授权云服务商收集部分云服务客户控制的审计数据，应核查云服务商是否在不影响其他云服务客户安全的前提下将云服务客户审计数据提供给云服务客户；应核查云服务商审计数据是否不包括云服务客户控制部分的审计数据； 测评单元（L4-NCS2-13） 应核查虚拟机迁移时访问控制策略随之迁移的措施或手段；应核查虚拟机迁移记录及相关配置，查看虚拟机迁移后访问控制策略是否部署；应测试虚拟机迁移，验证访问控制措施是否随其迁移。 测评单元（L4-NCS2-09） 应核查接口设计文档或开放性服务技术文档是否符合开放性、安全性要求；如果提供开放接口，应核查内部通信网络（虚拟网络）为第三方安全产品所提供的开放接口安全保障机制、接口配置或参数是否符合安全需求；如果提供开放性安全产品、服务，应核查开放性安全产品及服务的服务内容和实现开放性安全服务所采用的技术手段、安全保障机制是否符合安全需求。
8.3.3 安全通信网络设计技术要求	8.3.3.2 云安全通信网络设计技术要求	a) 通信网络传输保密性 应支持云服务客户远程通信数据保密性保护；应支持使用硬件加密设备对重要通信过程进行密码运算和密钥管理。	测评单元（L4-NCS1-08） 应核查是否在通信过程中采取保密措施，具体采用哪些技术措施；应测试验证在通信过程中是否对敏感信息字段或整个报文进行加密。 测评单元（L4-NCS1-10） 应核查是否基于密码模块产生密钥并进行密码运算；应核查相关证书或证明材料，确认采用的密码算法是否符合国家有关部门的要求。
		b) 通信网络可信接入保护 应禁止通过互联网直接访问云计算平台物理网络；应提供开放接口，允许接入可信的第三方安全产品；应确保外部通	测评单元（L4-NCS1-15） 应核查是否采用可信验证机制对接入到网络中的设备进行可信验证；应测试验证是否能够对连接到内部网络的设备进行可信验证。

		信接口经授权后方可传输数据。	
		c) 通信网络安全审计 应支持租户收集和查看与本租户资源相关的审计信息；应保证云服务商对云服务客户通信网络的访问操作可被租户审计；应通过安全管理中心集中管理，并对确认的违规行为进行报警，且做出相应处置。	测评单元（L4-NCS1-21） 应核查云服务商审计数据收集系统或设备是否根据云服务商和云服务客户的职责划分，实现各自控制部分审计数据的收集；如果云服务客户授权云服务商收集部分云服务客户控制的审计数据，应核查云服务商是否在不影响其他云服务客户安全的前提下将云服务客户审计数据提供给云服务客户；应核查云服务商审计数据是否不包括云服务客户控制部分的审计数据。
8.3.4 安全管理中心设计技术要求	8.3.4.1 系统管理	在进行云计算平台安全设计时，安全管理应提供查询云服务客户数据及备份存储位置的方式；云计算平台的运维应在中国境内，禁止从境外对境内云计算平台的运维。	测评单元（L4-ADS2-04） 应核查云管理平台或云平台为云服务客户提供数据及备份存储位置的查询记录；应核查云服务商是否为云服务客户提供数据及备份存储位置查询的接口或其他技术、管理手段。 测评单元（L4-MMS2-01） 应核查运维地点是否位于中国境内，是否不存在从境外对境内云计算平台实施远程运维的设备、地点和相关内容；应核查云计算平台远程运维记录中境外对境内云计算平台实施运维操作是否遵循国家相关规定。 测评单元（L4-MMS2-02） 应核查云计算平台运维过程产生的配置数据、日志信息等是否存储于中国境内；对于有出境需求的配置数据和日志信息，应核查数据出境是否遵循国家相关规定。
	8.3.4.2 安全管理	在进行云计算平台安全设计时，安全管理应具有对攻击行为回溯分析以及对网络安全事件进行预测和预警的能力；应具有对网络安全态势进行感知、预测和预判的能力。	测评单元（L4-CMS2-08） 应访谈云服务商安全主管是否供应商的重要变更是否及时传达到云服务客户，并且对带来的安全风险进行评估，并采取有关措施对风险进行控制；应核查系统，确认供应链安全事件信息或威胁信息是否能够及时传达到云服务客户。 测评单元（L4-CMS2-09） 应核查安全风险评估报告和风险预案，确认对每

			次供应商的重要变更都进行评估与风险预案设计。
	8.3.4.3 审计管理	在进行云计算平台安全设计时，云计算平台应对云服务器、云数据库、云存储等云服务的创建、删除等操作行为进行审计；应通过运维审计系统对管理员的运维行为进行安全审计；应通过租户隔离机制，确保审计数据隔离的有效性。	测评单元（L4-ECS2-05） 应核查安全审计配置是否能够保证云服务商对云服务客户系统和数据的操作（如增、删、改、查等操作）可被云服务客户审计；应核查是否支持云服务客户部署第三方安全审计设备，保证云服务商对云服务客户系统和数据的操作可被租户审计；应核查云服务商与云服务客户收集的审计数据，查看云服务商对云服务客户系统和数据的操作是否可被云服务客户审计。 测评单元（L4-ADS2-06） 应核查云服务客户是否不能访问其他云服务客户审计数据；应核查是否采取云服务客户审计数据隔离存放措施。

C.3 移动互联安全设计要求测评验证表

C.3.1 第一级

适用范围	功能要求	设计要求	测评要求
5.3.1 安全计算环境设计技术要求	5.3.1.3 移动互联安全计算环境设计技术要求	a) 用户身份鉴别 应采用口令、解锁图案以及其它具有相应安全强度的机制进行用户身份鉴别。	通用测评要求 测评单元（L1-ECS1-01） 1) 应核查用户在登录时是否采用了身份鉴别措施；2) 应核查用户列表，核查用户身份标识是否具有唯一性；3) 应核查用户配置信息或访谈系统管理员，核查是否存在空口令用户；4) 应核查用户鉴别信息是否具有复杂度要求并定期更换。
		b) 应用管控 应提供应用程序签名认证机制，拒绝未经过认证签名的应用软件安装和执行。	测评单元（L1-CMS3-01） 应访谈安全管理员，移动终端安装、运行的应用软件是否采用国家认可的证书签名或采用指定的可靠分发渠道；

		c) 安全域隔离 应能够为重要应用提供应用级隔离的运行环境，保证应用的输入、输出、存储信息不被非法获取。	— —

C.3.2 第二级

适用范围	功能要求	设计要求	测评要求
6.3.1 安全计算环境设计技术要求	6.3.1.3 移动互联安全计算环境设计技术要求	a) 用户身份鉴别 应采用口令、解锁图案以及其它具有相应安全强度的机制进行用户身份鉴别。	通用测评要求 测评单元 (L2-ECS1-01) 1) 应核查用户在登录时是否采用了身份鉴别措施；2) 应核查用户列表，核查用户身份标识是否具有唯一性；3) 应核查用户配置信息或访谈系统管理员，核查是否不存在空口令用户；4) 应核查用户鉴别信息是否具有复杂度要求并定期更换。
		b) 应用管控 应提供应用程序签名认证机制，拒绝未经过认证签名的应用软件安装和执行。	测评单元 (L2-ECS3-04) 应核查允许使用的签名证书；
		c) 安全域隔离 应能够为重要应用提供应用级隔离的运行环境，保证应用的输入、输出、存储信息不被非法获取。	测评单元 (L2-ECS3-05) 应核查是否采用安全隔离手段或措施进行应用级隔离；
		d) 数据保密性保护 应采取加密、混淆等措施，对移动应用程序进行保密性保护，防止被反编译；移动设备丢失或被盗后，应基于移动设备管理软件，搜寻设备的位置、远程锁定设备、远程擦除设备上的数据、使手机发出警报音，确保在能够定位和检索的同时最大程度地保护数据。	— —
		e) 可信验证	测评单元 (L2-ECS3-04)

		应能对移动终端的操作系统、应用等程序的可信性进行验证，阻止非可信程序的执行。	应核查允许使用的签名证书； 测评单元（L2-ECS3-05） 应核查是否采用安全隔离手段或措施进行应用级隔离；
6.3.2 安全区域边界设计技术要求	6.3.2.3 移动互联区域边界设计技术要求	a) 区域边界访问控制 应对接入系统的移动终端，采取基于 SIM 卡、证书等信息的强认证措施；应能限制移动设备在不同工作场景下对 WIFI、3G、4G 等网络的访问能力；	测评单元（L2-NCS3-04） 应核查是否能够检测、记录非授权移动终端的接入行为；
		b) 区域边界完整性 应能够对非授权设备私自联到内部网络以及内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断；移动终端区域边界检测设备监控范围应完整覆盖移动终端办公区，并具备无线路由器设备位置检测功能，对于非法无线路由器设备接入进行报警和阻断。	测评单元（L2-PES3-01） 应核查物理位置与无线信号的覆盖范围；2) 应测试无线信号的覆盖范围并测试在一定范围内是否可以进行电磁干扰。 测评单元（L2-NCS3-03） 应核查是否能够检测、记录非授权无线接入设备；
6.3.3 安全通信网络设计技术要求	6.3.3.3 移动互联通信网络设计技术要求	a) 通信网络可信保护 应通过 VPDN 等技术实现基于密码算法的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入。	测评单元（L2-NCS3-01） 应核查有线网络与无线网络边界之间是否部署无线接入网关设备； 测评单元（L2-NCS3-02） 应核查是否开启接入认证功能，是否使用除 WEP 方式以外的其它方式进行认证，密钥长度不小于 8 位； 测评单元（L2-NCS3-03） 应核查是否能够检测、记录非授权无线接入设备；

C.3.3 第三级

适用范围	功能要求	设计要求	测评要求

7.3.1 安全计算环境设计技术要求	7.3.1.3 移动互联安全计算环境设计技术要求	a) 用户身份鉴别 应对移动终端用户实现基于口令或解锁图案、数字证书或动态口令、生物特征等方式的两种或两种以上的组合身份鉴别；	通用测评要求 测评单元 (L3-ECS1-04) 应核查系统是否采用两种或两种以上组合的鉴别技术对用户身份进行鉴别，其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现；
		b) 标记和强制访问控制 应确保用户或进程对移动终端系统资源的最小使用权限；应根据安全策略，控制移动终端接入访问外设，外设类型至少应包括扩展存储卡、GPS 等定位设备、蓝牙、NFC 等通信外设，并记录日志。	测评单元 (L3-ECS3-01) 应核查移动终端管理系统，查看移动终端客户端软件的安装、注册与管理策略； 测评单元 (L3-ECS3-02) 1) 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等安全策略；2) 应测试是否能够对移动终端进行远程锁定和远程擦除等。 测评单元 (L3-ECS3-03) 应核查是否具有选择应用软件安装、运行的功能； 测评单元 (L3-ECS3-05) 1) 应核查是否具有应用软件权限控制功能；2) 应测试是否可以对移动终端中资源的访问进行限制。
		c) 应用管控 应具有软件白名单功能，能根据白名单控制应用软件安装、运行；应提供应用程序签名认证机制，拒绝未经过认证签名的应用软件安装和执行。	测评单元 (L3-ECS3-04) 1) 应核查是否具有软件白名单功能； 2) 应测试使用白名单控制应用软件安装、运行。 测评单元 (L3-ECS3-06) 应核查允许使用的签名证书，且证书是否由系统管理者指定；
		d) 安全域隔离 应能够为重要应用提供基于容器、虚拟化等系统级隔离的运行环境，保证应用的输入、输出、存储信息不被非法获取。	测评单元 (L3-ECS3-08) 应核查是否采用安装双系统或其它安全隔离措施进行操作系统级隔离；
		e) 数据保密性保护 应采取加密、混淆等措施，对移动应用程序进行保密性保护，防止被反编译；移动	测评单元 (L3-ECS3-02) 1) 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等安全策略 2) 应测试是否能够对移动终端进行远程锁定

		设备丢失或被盗后，应基于移动设备管理软件，搜寻设备的位置、远程锁定设备、远程擦除设备上的数据、使手机发出警报音，确保在能够定位和检索的同时最大程度地保护数据；应实现对扩展存储设备的加密功能，确保数据存储的安全。	和远程擦除等。 通用测评要求 测评单元（L3-ADS1-28） 1)应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性；2)应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性。
		f) 可信验证 应能对移动终端的引导程序、操作系统内核、应用程序等进行可信验证，确保每个部件在加载前的真实性和完整性。	测评单元（L3-ECS3-06） 应核查允许使用的签名证书，且证书是否由系统管理者指定； 测评单元（L3-ECS3-08） 应核查是否采用安装双系统或其它安全隔离措施进行操作系统级隔离；
7.3.2 安全区域边界设计技术要求	7.3.2.3 移动互联区域边界设计技术要求	a) 区域边界访问控制 应对接入系统的移动终端，采取基于 SIM 卡、证书等信息的强认证措施；应能限制移动设备在不同工作场景下对 WIFI、3G、4G 等网络的访问能力；	测评单元（L3-NCS3-02） 应核查无线接入设备是否开启接入认证功能，是否采用认证服务器或国家密码管理机构批准的密码模块进行认证； 测评单元（L3-ECS3-02） 应核查移动终端客户端软件的安装、注册与管理策略； 测评单元（L3-ECS3-03） 1)应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等策略；2)应测试是否能够对移动终端进行远程锁定和远程擦除等。测评单元（L3-NCS3-04） 1)应核查是否能够检测、记录并定位非授权移动终端的接入行为；2)测试是否能够检测、记录、定位非授权移动终端接入。
		b) 区域边界完整性 应能够对非授权设备私自联到内部网络以及内部网络用户私自联到外部网络的	测评单元（L3-ECS3-02） 应核查移动终端管理系统，查看移动终端客户端软件的安装、注册与管理策略； 测评单元（L3-PES3-01）

		行为进行检查，准确定出位置，并对其进行有效阻断；移动终端区域边界检测设备监控范围应完整覆盖移动终端办公区，并具备无线路由器设备位置检测功能，对于非法无线路由器设备接入进行报警和阻断。	1)应核查物理位置与无线信号的覆盖范围；2)应测试无线信号的覆盖范围并测试在一定范围内是否可以进行电磁干扰。 测评单元（L3-NCS3-03） 1)应核查是否能够检测、记录并定位非授权无线接入设备；2)应测试是否能够检测、记录、定位非授权无线接入设备。 测评单元（L3-NCS3-04） 1)应核查是否能够检测、记录、定位并阻断非授权移动终端的接入行为；2)应测试是否能够检测、记录、定位并阻断非授权移动终端接入。
7.3.3 安全通信网络设计技术要求	7.3.3.3 移动互联通信网络设计技术要求	a) 通信网络可信保护 应通过 VPDN 等技术实现基于密码算法的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入。	测评单元（L3-NCS3-01） 应核查有线网络与无线网络边界之间是否部署无线接入网关设备； 测评单元（L3-NCS3-02） 应核查无线接入设备是否开启接入认证功能，是否采用认证服务器或国家密码管理机构批准的密码模块进行认证； 测评单元（L3-NCS3-03） 1)应核查是否能够检测、记录、定位非授权无线接入设备；2)应测试是否能够检测、记录、定位非授权无线接入设备。

C.3.4 第四级

适用范围	功能要求	设计要求	测评要求
8.3.1 安全计算环境设计技术要求	8.3.1.3 移动互联安全计算环境设计技术要求	a) 用户身份鉴别 应对移动终端用户实现基于口令或解锁图案、数字证书或动态口令、生物特征等方式的两种或两种以上的组合身份鉴别；应基于硬件为身份鉴别机制构建隔离的运行环境。	通用测评要求 测评单元（L4-ECS1-04） 应核查系统是否采用两种或两种以上组合的鉴别技术对用户身份进行鉴别，其中一种鉴别技术至少应使用密码技术或生物技术来实现； 测评单元（L4-ECS3-08）

			应核查是否为专用终端，仅处理访问指定业务；
		b) 标记和强制访问控制 应确保用户或进程对移动终端系统资源的最小使用权限；应根据安全策略，控制移动终端接入访问外设，外设类型至少应包括扩展存储卡、GPS 等定位设备、蓝牙、NFC 等通信外设，并记录日志。	测评单元 (L4-ECS3-06) 1) 应核查是否具有应用软件权限控制功能；2) 应测试是否可以对移动终端中资源的访问进行限制。 测评单元 (L4-ECS3-01) 应核查是否为专用终端，仅处理指定的相关业务； 测评单元 (L4-ECS3-02) 应核查移动终端管理系统，查看移动终端客户端软件的安装、注册与管理策略； 测评单元 (L4-ECS3-03) 1) 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等策略；2) 应测试是否能够对移动终端进行远程锁定和远程擦除等。
		c) 应用管控 应具有软件白名单功能，能根据白名单控制应用软件安装、运行；应提供应用程序签名认证机制，拒绝未经过认证签名的应用软件安装和执行。应确保移动终端为专用终端，不得处理与定级系统无关的业务。	测评单元 (L4-ECS3-05) 1) 应核查是否具有软件白名单功能；2) 应测试使用白名单控制应用软件安装、运行。 测评单元 (L4-ECS3-07) 应核查允许使用的签名证书，且证书是否由系统管理者指定； 测评单元 (L4-ECS3-08) 应核查是否为专用终端，仅处理访问指定业务；
		d) 安全域隔离 应能够为重要应用提供基于容器、虚拟化等系统级隔离的运行环境，保证应用的输入、输出、存储信息不被非法获取。	测评单元 (L4-ECS3-08) 应核查是否为专用终端，仅处理访问指定业务；
		e) 数据保密性保护 应采取加密、混淆等措施，对移动应用程序进行保密性保护，防止被反编译；移动设备丢失或被盗后，应基于移动设备管理软件，搜寻设备的位置、远程锁定设备、	测评单元 (L4-ECS3-03) 1) 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等策略； 2) 应测试是否能够对移动终端进行远程锁定和远程擦除等。

		远程擦除设备上的数据、使手机发出警报音，确保在能够定位和检索的同时最大程度地保护数据；应实现对扩展存储设备的加密功能，确保数据存储的安全。	通用测评要求 测评单元（L4-ADS1-28） 1) 应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性；2) 应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性。
		f) 可信验证 应能对移动终端的引导程序、操作系统内核、应用程序等进行可信验证，确保每个部件在加载前的真实性和完整性。	测评单元（L4-ECS3-06） 应核查允许使用的签名证书，且证书是否由系统管理者指定； 测评单元（L4-ECS3-08） 应核查是否为专用终端，仅处理访问指定业务；
8.3.2 安全区域边界设计技术要求	8.3.2.3 移动互联区域边界设计技术要求	a) 区域边界访问控制 应对接入系统的移动终端，采取基于 SIM 卡、证书等信息的强认证措施；应能限制移动设备在不同工作场景下对 WIFI、3G、4G 等网络的访问能力；	测评单元（L4-NCS3-02） 应核查无线接入设备是否开启接入认证功能，是否采用认证服务器或国家密码管理机构批准的密码模块进行认证； 测评单元（L4-ECS3-02） 应核查移动终端客户端软件的安装、注册与管理策略； 测评单元（L4-ECS3-03） 1) 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等策略；2) 应测试是否能够对移动终端进行远程锁定和远程擦除等。测评单元（L3-NCS3-04） 1) 应核查是否能够检测、记录并定位非授权移动终端的接入行为；2) 测试是否能够检测、记录、定位非授权移动终端接入。
		b) 区域边界完整性 应能够对非授权设备私自联到内部网络以及内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断；移动终端区域边界检测设备	测评单元（L4-ECS3-02） 应核查移动终端管理系统，查看移动终端客户端软件的安装、注册与管理策略； 测评单元（L4-PES3-01） 1) 应核查物理位置与无线信号的覆盖范围；2) 应测试无线信号的覆盖范围并测试在一定范围内是

		监控范围应完整覆盖移动终端办公区，并具备无线路由器设备位置检测功能，对于非法无线路由器设备接入进行报警和阻断。	否可以进行电磁干扰。 测评单元（L4-NCS3-03） 1) 应核查是否能够检测、记录并定位非授权无线接入设备；2) 应测试是否能够检测、记录、定位非授权无线接入设备。 测评单元（L4-NCS3-04） 1) 应核查是否能够检测、记录、定位并阻断非授权移动终端的接入行为； 2) 应测试是否能够检测、记录、定位并阻断非授权移动终端接入。
8.3.3 安全通信网络设计技术要求	8.3.3.3 移动互联通信网络设计技术要求	a) 通信网络可信保护 应通过 VPDN 等技术实现基于密码算法的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入。	测评单元（L4-NCS3-02） 应核查是否开启接入认证功能，是否采用认证服务器或国家密码管理机构批准的密码模块进行认证； 测评单元（L4-NCS3-03） 1) 应核查是否能够检测、记录并定位非授权无线接入设备；2) 应测试是否能够检测、记录、定位非授权无线接入设备。

C.4 物联网安全设计要求测评验证表

C.4.1 第一级

适用范围	功能要求	设计要求	测评要求
5.3.1 物联网系统安全计算环境设计技术要求	5.3.1.4 物联网系统安全计算环境设计技术要求	a) 物联网设备身份鉴别 感知设备和感知层网关的设备口令应有复杂度要求并定期更换；应采用常规鉴别机制对感知设备发送的数据进行鉴别，确保数据来源于正确的感知设备；应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码	测评单元（L1-ECS1-01） 应核查用户在登录时是否采用了身份鉴别措施；应核查用户列表，核查用户身份标识是否具有唯一性；应核查用户配置或访谈系统管理员，是否存在空口令用户；应核查用户鉴别信息是否具有复杂度要求并定期更换。 测评单元（L2-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关

		国家标准和行业标准。	服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。
		b) 物联网设备访问控制 应通过制定安全策略如访问控制列表，实现对感知设备的访问控制；感知设备和其他设备（感知层网关、其他感知设备）通信时，应根据安全策略对其他设备进行权限检查。	测评单元（L1-ADS1-03） 应核查是否提供访问控制功能；应核查是否有管理用户负责对系统用户进行账户分配和权限管理。 测评单元（L1-NCS4-01） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术或其他技术手段，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制描述。
5.3.2 物联网系统安全区域边界设计技术要求	5.3.2.4 物联网系统区域边界设计技术要求	a) 物联网系统区域边界准入控制 应在安全区域边界设置准入控制机制，保证合法设备接入。	测评单元（L1-NCS4-01） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术或其他技术手段，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制描述。
5.3.3 物联网系统安全通信网络设计技术要求	5.3.3.4 物联网系统通信网络设计技术要求	a) 感知层网络数据传输新鲜性保护 应在感知层网络传输的数据中加入数据发布的序列信息如时间戳、计数器等，以实现感知层网络数据传输新鲜性保护。	测评单元（L3-ADS4-01） 应核查感知节点设备鉴别数据新鲜性的措施，是否能够避免历史数据重放；应将感知节点设备历史数据进行重放测试，验证其保护措施是否生效。 测评单元（L3-ADS4-02） 应访谈安全管理员针对感知节点设备历史数据的保护措施，具体措施有哪些，是否具有对历史数据被非法修改的检测措施，检测措施有哪些；应核查感知层是否配备检测感知节点设备历史数据被非法篡改的措施，在检测到被修改时是否能采取必要的恢复措施；应测试检测措施的有效性，是否能够避免数据的修改重放攻击。
		b) 异构网安全接入保护 应采用接入认证等技术建立异构网络的接入认证系统，保障控制信息的安全传	测评单元（L1-NCS4-01） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术或其他技术手段，具体措施有哪

		输。	些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制描述。

C.4.2 第二级

适用范围	功能要求	设计要求	测评要求
6.3.1 物联网系统安全计算环境设计技术要求	6.3.1.4 物联网系统安全计算环境设计技术要求	a) 物联网设备身份鉴别 感知设备和感知层网关的设备口令应有复杂度要求并定期更换；应采用常规鉴别机制对感知设备发送的数据进行鉴别，确保数据来源于正确的感知设备；应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准。	测评单元（L2-ECS1-01） 应核查用户在登录时是否采用了身份鉴别措施； 应核查用户列表，核查用户身份标识是否具有唯一性；应核查用户配置或访谈系统管理员，是否不存在空口令用户；应核查用户鉴别信息是否具有复杂度要求并定期更换。 测评单元（L2-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。 测评单元（L2-NCS4-03） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术或其他技术手段，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制描述。
		b) 物联网设备访问控制 应通过制定安全策略如访问控制列表，实现对感知设备的访问控制；感知设备和其他设备（感知层网关、其他感知设备）通信时，应根据安全策略对其他设备进行权限检查。	测评单元（L2-ADS1-05） 应核查是否提供访问控制功能；应核查是否有管理用户负责对系统用户进行账户分配和权限管理。 测评单元（L2-NCS4-03） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术或其他技术手段，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制描

			述。
6.3.2 物联网系统安全区域边界设计技术要求	6.3.2.4 物联网系统区域边界设计技术要求	a) 物联网系统区域边界准入控制 应在安全区域边界设置准入控制机制，能够对设备进行认证。	测评单元（L2-NCS4-03） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术或其他技术手段，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制描述。
		b) 物联网系统区域边界协议过滤与控制 应在安全区域边界设置协议检查，对通信报文进行合规检查。	测评单元（L2-NCS1-09） 应核查设备访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数。
6.3.3 物联网系统安全通信网络设计技术要求	6.3.3.4 物联网系统通信网络设计技术要求	a) 感知层网络数据传输完整性保护 应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准。	测评单元（L2-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。
		b) 感知层网络敏感数据传输保密性保护 应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准。	测评单元（L2-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。
		c) 感知层网络数据传输新鲜性保护 应在感知层网络传输的数据中加入数据发布的序列信息如时间戳、计数器等，以实现感知层网络数据传输新鲜性保护。	测评单元（L3-ADS4-01） 应核查感知节点设备鉴别数据新鲜性的措施，是否能够避免历史数据重放；应将感知节点设备历史数据进行重放测试，验证其保护措施是否生效。 测评单元（L3-ADS4-02） 应访谈安全管理员针对感知节点设备历史数据的保护措施，具体措施有哪些，是否具有对历史数据被非法修改的检测措施，检测措施有哪些；应核查感知层是否配备检测感知节点设备历史数据被非法篡改的措施，在检测到被修改时是否能采取必要的恢复措施；应测试检测措施的有效性，是否能够避免数据的修改重放攻击。

		d) 异构网安全接入保护 应采用接入认证等技术建立异构网络的接入认证系统，保障控制信息的安全传输；应采用入侵检测等技术拒绝恶意设备的接入，保证合法设备不被恶意设备攻击而被拒绝接入，保证网络资源的可使用性。	测评单元（L2-NCS4-03） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术或其他技术手段，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制描述。 测评单元（L2-NCS1-11） 应核查相关系统或设备是否能够检测到以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；应核查相关系统或设备的规则库版本是否已经更新到最新版本；应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点。应测试相关系统或设备验证其安全策略是否有效。
6.3.4 安全管理中心设计技术要求	6.3.4.1 系统管理	在进行物联网系统安全设计时，可通过系统管理员对系统的可信基准库进行配置。	测评单元（L3-ECS1-23） 核查是否采用可信计算技术建立从系统到应用的信任链；

C.4.3 第三级

适用范围	功能要求	设计要求	测评要求
7.3.1 物联网系统安全计算环境设计技术要求	7.3.1.4 物联网系统安全计算环境设计技术要求	a) 物联网设备身份鉴别 感知设备和感知层网关的设备口令应有复杂度要求并定期更换；感知层网关与感知设备之间应实现双向的身份鉴别；应对感知设备发送的数据进行鉴别，确保数据来源于正确的感知设备且没有被恶意注入虚假信息；应采取措施对感知设备组成的组进行组认证以减少网络拥塞；应支持国家密码管理主管部门批准	测评单元（L3-ECS1-01） 应核查用户在登录时是否采用了身份鉴别措施；应核查用户列表，核查用户身份标识是否具有唯一性；应核查用户配置或访谈系统管理员，是否不存在空口令用户；应核查用户鉴别信息是否具有复杂度要求并定期更换。 测评单元（L3-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家

		使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准。	密码管理主管部门的要求。 测评单元（L3-NCS4-03） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术、身份鉴别技术等，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述；应对边界和感知层网络进行渗透测试，测试是否不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。 测评单元（L3-ECS4-02） 应核查是否对连接的网关节点设备（包括读卡器）设备进行身份标识与鉴别，是否配置了符合安全策略的参数；应进行渗透测试，验证是否不存在绕过身份标识与鉴别功能的方法。 测评单元（L3-ECS4-03） 应核查是否对连接的其他感知节点设备（包括路由节点）设备进行身份标识与鉴别，是否配置了符合安全策略的参数；应进行渗透测试，验证是否不存在绕过身份标识与鉴别功能的方法。 测评单元（L3-ECS4-05） 应核查网关节点设备是否能够对连接设备（包括终端节点、路由节点、数据处理中心）进行标识并配置了鉴别功能；应进行渗透测试，验证是否不存在绕过身份标识与鉴别功能的方法。 测评单元（L4-ECS4-06） 应核查网关节点设备是否设置了过滤非法节点和伪造节点发送的数据的配置；应测试网关节点设备，是否能够过滤非法节点和伪造节点发送的数据。
		b) 物联网设备访问控制 应通过制定安全策略如访问控制列表，实现对感知设备的访问控制；感知设备	测评单元（L3-ADS1-10） 应核查是否由管理用户负责配置访问控制策略；应核查授权主体是否依据安全策略配置了主体对客体的访问规则；应测试用户是否有可越权访问情

		和其他设备（感知层网关、其他感知设备）通信时，根据安全策略对其他设备进行权限检查；感知设备进行更新配置时，根据安全策略对用户进行权限检查。	形。 测评单元（L3-ADS1-11） 应核查访问控制策略的控制粒度是否达到主体为用户级，客体为文件、数据库表、记录或字段级。 测评单元（L3-NCS4-03） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术、身份鉴别技术等，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述；应对边界和感知层网络进行渗透测试，测试是否存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。 测评单元（L3-ECS4-01） 应核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更；应测试感知节点设备，可通过试图接入和控制传感网访问未授权的资源，验证访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效。 测评单元（L3-ECS4-07） 应访谈安全管理员有哪些感知节点设备需要采用密钥进行通信，是否对设备的关键密钥进行在线更新；应核查感知节点设备是否对其关键密钥进行在线更新。 测评单元（L3-ECS4-08） 应访谈安全管理员感知节点设备是否支持对其关键配置参数进行在线更新；应核查感知节点设备在线更新方式是否有效。
		c) 数据完整性保护 应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码	测评单元（L3-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。

		国家标准和行业标准。	
		d) 数据保密性保护 应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准。	测评单元（L3-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。
		e) 可信验证 可基于可信根对计算节点的 BIOS、引导程序、操作系统内核、应用程序等进行可信验证，并在应用程序的关键执行环节对系统调用、中断、关键内存区域等进行可信验证，并在检测到其完整性受到破坏时采取措施恢复。	测评单元（L3-ECS1-23） 应核查防恶意代码工具的安装和使用情况，核查是否定期进行升级和更新防恶意代码库，或核查是否采用可信计算技术建立从系统到应用的信任链；应访谈系统管理员，核查是否有保护重要系统程序或文件完整性的措施；应当检测到程序或文件受到破坏后，是否具备恢复的措施。
7.3.2 物联网系统安全区域边界设计技术要求	7.3.2.4 物联网系统区域边界设计技术要求	a) 物联网系统区域边界访问控制 应能根据数据的时间戳为数据流提供明确的允许/拒绝访问的能力；应提供网络最大流量及网络连接数限制机制；应能够根据通信协议特性，控制不规范数据包的出入；	测评单元（L3-NCS1-12） 应核查在网络边界或区域之间是否部署访问控制设备，是否启用访问控制策略；应核查设备的最后一条访问控制策略是否为禁止所有网络通信。 测评单元（L3-NCS4-01） 应核查感知层安全设计文档，是否有对感知节点通信目标地址的控制措施说明；应核查感知节点设备，是否配置了对感知节点通信目标地址的控制措施，相关参数配置是否符合设计要求；应对感知节点设备进行渗透测试，测试是否能够限制感知节点设备对违反访问控制策略的通信目标地址进行访问或攻击。 测评单元（L3-NCS4-02） 应核查感知层安全设计文档，是否有对网关节点通信目标地址的控制措施说明；应核查网关节点设备，是否配置了对网关节点通信目标地址的控制措施，相关参数配置是否符合设计要求；应对感知节点设备进行渗透测试，测试是否能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击。

			测评单元（L3-ECS4-04） 应核查网关节点设备是否配置了最大并发连接数参数。 测评单元（L3-ECS4-06） 应核查网关节点设备是否设置了过滤非法节点和伪造节点发送的数据的配置；应测试网关节点设备，是否能够过滤非法节点和伪造节点发送的数据。
		b) 物联网系统区域边界完整性保护 应在区域边界设置轻量级的双向认证机制，能够保证防止数据的违规传输。	测评单元（L3-NCS4-03） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术、身份鉴别技术等，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述；应对边界和感知层网络进行渗透测试，测试是否存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。
		c) 物联网系统区域边界准入控制 应在安全区域边界设置准入控制机制，能够对设备进行认证，保证合法设备接入，拒绝恶意设备接入；应根据感知设备特点收集感知设备的健康性相关信息如固件版本、标识、配置信息校验值等，并能够对接入的感知设备进行健康性检查。	测评单元（L3-NCS1-09） 应核查是否采用技术措施防止非授权设备接入内部网络，并进行有效阻断；应核查所有路由器和交换机等相关设备闲置端口是否均已关闭。 测评单元（L3-NCS1-10） 应核查是否采用技术措施防止内部用户非法外联行为； 测评单元（L3-NCS4-03） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术、身份鉴别技术等，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述；应对边界和感知层网络进行渗透测试，测试是否存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。 测评单元（L3-MMS4-02） 应核查感知节点设备、网关节点设备部署环境维护

			记录是否包括了感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息）核查、对网关设备进行现场维护（除尘、充电、修理等）等方面内容。
		d) 物联网系统区域边界协议过滤与控制 应在安全区域边界设置协议过滤，能够对物联网通信内容进行过滤，对通信报文进行合规检查，根据协议特性，设置相对应控制机制。	测评单元（L3-NCS1-14） 应核查设备访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数。 测评单元（L3-NCS1-16） 应核查在关键网络节点处是否部署相关设备，是否启用访问控制策略；应测试设备访问控制策略是否能够对进出网络的信息内容进行过滤，实现对内容的访问控制。
7.3.3 物联网系统安全通信网络设计技术要求	7.3.3.4 物联网系统通信网络设计技术要求	a) 感知层网络数据传输新鲜性保护 应在感知层网络传输的数据中加入数据发布的序列信息如时间戳、计数器等，以实现感知层网络数据传输新鲜性保护。	测评单元（L3-ADS4-01） 应核查感知节点设备鉴别数据新鲜性的措施，是否能够避免历史数据重放；应将感知节点设备历史数据进行重放测试，验证其保护措施是否生效。 测评单元（L3-ADS4-02） 应访谈安全管理员针对感知节点设备历史数据的保护措施，具体措施有哪些，是否具有对历史数据被非法修改的检测措施，检测措施有哪些；应核查感知层是否配备检测感知节点设备历史数据被非法篡改的措施，在检测到被修改时是否能采取必要的恢复措施；应测试检测措施的有效性，是否能够避免数据的修改重放攻击。
		b) 异构网安全接入保护 应采用接入认证等技术建立异构网络的接入认证系统，保障控制信息的安全传输；应采用入侵检测等技术拒绝恶意设备的接入，保证合法设备不被恶意设备攻击而被拒绝接入，保证网络资源的可使用性；应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循	测评单元（L3-NCS1-09） 应核查是否采用技术措施防止非授权设备接入内部网络，并进行有效阻断；应核查所有路由器和交换机闲置端口是否均已关闭。 测评单元（L3-NCS1-03） 应核查是否依据某种原则划分不同的网络区域；应核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致。 测评单元（L3-CMS1-09）

		相关密码国家标准和行业标准；应根据各接入网的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并采取相应的防护措施。	应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。 测评单元（L3-NCS4-03） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术、身份鉴别技术等，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述；应对边界和感知层网络进行渗透测试，测试是否不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。
		c) 通信网络可信连接保护 可采用由可信根支持的可信网络连接机制，通过对连接到通信网络的设备进行可信验证，确保接入通信网络的设备真实可信，防止设备的非法接入。	测评单元（L4-NCS1-15） 应核查是否采用可信验证机制对接入到网络中的设备进行可信验证；应测试验证是否能够对连接到内部网络的设备进行可信验证。
7.3.4 安全管理中心设计技术要求	7.3.4.1 系统管理	在进行物联网系统安全设计时，应通过系统管理员对感知设备状态（电力供应情况、是否在线、位置等）进行统一监测和处理；应通过系统管理员对下载到感知设备上的应用软件进行授权；可通过系统管理员对系统的可信基准库进行配置。	测评单元（L3-ECS4-01） 应核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更；应测试感知节点设备，可通过试图接入和控制传感网访问未授权的资源，验证访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效。 测评单元（L3-ECS4-08） 应访谈安全管理员感知节点设备是否支持对其关键配置参数进行在线更新；应核查感知节点设备在线更新方式是否有效。
	7.3.4.2 安全管理	在进行物联网系统安全设计时，应通过安全管理员对系统中所使用的密钥进行统一管理，包括密钥的生成、分发、更新、存储、备份、销毁等，并采取必要措施保证密钥安全；应支持国家密码管理主管部门批准使用的密码算法，使用	测评单元（L3-ECS4-07） 应访谈安全管理员有哪些感知节点设备需要采用密钥进行通信，是否对设备的关键密钥进行在线更新；应核查感知节点设备是否对其关键密钥进行在线更新。 测评单元（L3-CMS1-09）

		国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准；应通过安全管理员配置可信验证策略。	应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。

C.4.4 第四级

适用范围	功能要求	设计要求	测评要求
8.3.1 物联网系统安全计算环境设计技术要求	8.3.1.4 物联网系统安全计算环境设计技术要求	a) 物联网设备身份鉴别 感知设备和感知层网关的设备口令应有复杂度要求并定期更换；感知层网关与感知设备之间应实现双向的身份鉴别；应采用密码技术支持的鉴别机制，对感知设备发送的数据进行鉴别，确保数据来源于正确的感知设备且没有被恶意注入虚假信息；应采取措施对感知设备组成的组进行组认证，以减少网络拥塞；应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准。	测评单元（L4-ECS1-01） 应核查用户在登录时是否采用了身份鉴别措施；应核查用户列表，核查用户身份标识是否具有唯一性；应核查用户配置或访谈系统管理员，是否存在空口令用户；应核查用户鉴别信息是否具有复杂度要求并定期更换。 测评单元（L4-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。 测评单元（L4-NCS4-03） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术、身份鉴别技术等，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述；应对边界和感知层网络进行渗透测试，测试是否不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。 测评单元（L4-ECS4-02） 应核查是否对连接的网关节点设备（包括读卡器）设备进行身份标识与鉴别，是否配置了符合安全策略的参数；应进行渗透测试，验证是否不存在绕过身份标识与鉴别功能的方法。 测评单元（L4-ECS4-03）

		应核查是否对连接的其他感知节点设备（包括路由节点）设备进行身份标识与鉴别，是否配置了符合安全策略的参数；应进行渗透测试，验证是否不存在绕过身份标识与鉴别功能的方法。 测评单元（L4-ECS4-05） 应核查网关节点设备是否能够对连接设备（包括终端节点、路由节点、数据处理中心）进行标识并配置了鉴别功能；应进行渗透测试，验证是否不存在绕过身份标识与鉴别功能的方法。 测评单元（L4-ECS4-06） 应核查网关节点设备是否设置了过滤非法节点和伪造节点发送的数据的配置；应测试网关节点设备，是否能够过滤非法节点和伪造节点发送的数据。	
		b) 物联网设备访问控制 应通过制定安全策略如访问控制列表，实现对感知设备的访问控制；感知设备和其他设备（感知层网关、其他感知设备）通信时，应根据安全策略对其他设备进行权限检查；感知设备进行更新配置时，应根据安全策略对用户进行权限检查；由授权主体配置访问控制策略，严格限制默认账户的访问权限，并授予不同账户为完成各自承担任务所需的最小权限。	测评单元（L4-ECS1-06） 应核查是否已经重命名默认账号或默认账号已被删除；应核查是否已修改默认账号的默认口令。 测评单元（L4-ECS1-08） 应核查是否进行角色划分；应核查访问控制策略，查看管理用户的权限是否已进行分离；应核查管理用户权限是否为其工作任务所需的最小权限。 测评单元（L4-ADS1-11） 应核查是否由管理用户负责配置访问控制策略；应核查授权主体是否依据安全策略配置了主体对客体的访问规则；应测试用户是否有可越权访问情形。 测评单元（L4-ADS1-12） 应核查访问控制策略的控制粒度是否达到主体为用户级，客体为文件、数据库表、记录或字段级。 测评单元（L4-NCS4-03） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术、身份鉴别技术等，具体措施有哪些；应核查感知节点设备接入机制设计文档是

		否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述；应对边界和感知层网络进行渗透测试，测试是否不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。 测评单元（L4-ECS4-01） 应核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更；应测试感知节点设备，可通过试图接入和控制传感网访问未授权的资源，验证访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效。 测评单元（L4-ECS4-07） 应访谈安全管理员有哪些感知节点设备需要采用密钥进行通信，是否对设备的关键密钥进行在线更新；应核查感知节点设备是否对其关键密钥进行在线更新。 测评单元（L4-ECS4-08） 应访谈安全管理员感知节点设备是否支持对其关键配置参数进行在线更新；应核查感知节点设备在线更新方式是否有效。	测评单元（L4-ADS1-27） 应核查系统设计文档，鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了密码技术保证完整性；应测试在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。 测评单元（L4-ADS1-28） 应核查设计文档，是否采用了密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过
		c) 数据完整性保护 应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准；应采用专用通信协议或安全通信协议服务，避免来自基于通用协议的攻击破坏数据的完整性。	

			程中的完整性；应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；应测试在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。 测评单元（L4-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。
		d) 数据保密性保护 应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准；应采用专用通信协议或安全通信协议服务，避免来自基于协议的攻击破坏数据的保密性。	测评单元（L4-ADS1-30） 应核查系统设计文档，重鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性；应通过嗅探等方式抓取传输过程中的数据包，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。 测评单元（L4-ADS1-31） 应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性；应核查数据安全保护系统是否能够保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性。 测评单元（L4-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。
		e) 数据可用性保护 应提供关键感知设备和通信线路冗余，保证系统的高可用性。	测评单元（L4-NCS1-05） 应核查系统是否有主要网络设备、安全设备的硬件冗余和通信线路冗余。
		f) 可信验证	测评单元（L4-ECS1-23）

		可基于可信计算技术对计算节点的BIOS、引导程序、操作系统内核、应用程序等进行可信验证，并在应用程序的所有执行环节对系统调用、中断、关键内存区域等进行可信验证，并在检测到其完整性受到破坏时采取措施恢复。	应核查是否采用基准库比对或其他可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证；应核查是否有保护重要系统程序或文件完整性的措施；当检测到程序或文件受到破坏后，核查是否具备恢复的措施。
8.3.2 物联网系统安全区域边界设计技术要求	8.3.2.4 物联网系统区域边界设计技术要求	a) 物联网系统区域边界访问控制 应能根据数据的时间戳为数据流提供明确的允许/拒绝访问的能力，控制粒度为节点级；应提供网络最大流量及网络连接数限制机制；应能够根据通信协议特性，控制不规范数据包的出入；应对进出网络的信息内容进行过滤，实现对通信协议的命令级的控制。	测评单元（L4-NCS1-16） 应核查在网络边界或区域之间是否部署网络访问控制设备，是否启用访问控制策略；应核查设备的访问控制策略，确保手工配置或设备默认的最后一条策略为禁止所有网络通信。 测评单元（L4-NCS4-01） 应核查感知层安全设计文档，是否有对感知节点通信目标地址的控制措施说明；应核查感知节点设备，是否配置了对感知节点通信目标地址的控制措施，相关参数配置是否符合设计要求；应对感知节点设备进行渗透测试，测试是否能够限制感知节点设备对违反访问控制策略的通信目标地址进行访问或攻击。 测评单元（L4-NCS4-02） 应核查感知层安全设计文档，是否有对网关节点通信目标地址的控制措施说明；应核查网关节点设备，是否配置了对网关节点通信目标地址的控制措施，相关参数配置是否符合设计要求；应对感知节点设备进行渗透测试，测试是否能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击。 测评单元（L4-ECS4-04） 应核查网关节点设备是否配置了最大并发连接数参数。 测评单元（L4-ECS4-06） 应核查网关节点设备是否设置了过滤非法节点和伪造节点发送的数据的配置；应测试网关节点设

			备，是否能够过滤非法节点和伪造节点发送的数据。
		b) 物联网系统区域边界准入控制 应在安全区域边界设置准入控制机制，能够对设备进行认证；应根据感知设备特点收集感知设备的健康性相关信息如固件版本、标识、配置信息校验值等，并能够对接入的感知设备进行健康性检查。	测评单元（L4-NCS1-12） 应核查是否采用技术措施防止非授权设备接入内部网络，并进行有效阻断；应核查所有路由器和交换机等相关设备闲置端口是否均已关闭。 测评单元（L4-NCS1-13） 应核查是否采用技术措施防止内部用户非法外联行为； 测评单元（L4-NCS4-03） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术、身份鉴别技术等，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述；应对边界和感知层网络进行渗透测试，测试是否存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。 测评单元（L4-MMS4-02） 应核查感知节点设备、网关节点设备部署环境维护记录是否包括了感知节点设备、网关节点设备的状态（包括外观、电量、指示灯等信息）核查、对网关设备进行现场维护（除尘、充电、修理等）等方面内容。
		c) 物联网系统区域边界协议过滤与控制 应在安全区域边界设置协议过滤，能够对物联网通信内容进行深度检测和过滤，对通信报文进行合规检查。根据协议特性，设置相对应基于白名单控制机制。	测评单元（L4-NCS1-16） 应核查在网络边界或区域之间是否部署访问控制设备，是否启用访问控制策略；应核查设备的最后一条访问控制策略是否为禁止所有网络通信。 测评单元（L4-NCS1-18） 应核查设备是否采取协议转换或其他相应的控制措施来实现禁止数据带通用协议通过；应通过发送带通用协议的数据等测试方式，测试验证设备是否能够有效阻断。
		d) 物联网系统区域边界恶意代码防范	测评单元（L4-NCS1-19）

		应针对感知层网关的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位。	应核查相关系统或设备是否能够检测从外部发起的网络攻击行为；应核查相关系统或设备的规则库版本是否已经更新到最新版本；应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点；应测试相关系统或设备，测试验证其安全策略是否有效。 测评单元（L4-NCS1-20） 应核查相关系统或设备是否能够检测到从内部发起的网络攻击行为；应核查相关系统或设备的规则库版本是否已经更新到最新版本；应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点；应测试相关系统或设备，测试验证其安全策略是否有效。 测评单元（L4-NCS1-21） 应核查是否部署网络回溯系统或抗 APT 攻击系统对新型网络攻击进行检测和分析；应测试验证是否对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析。
8.3.3 物联网系统安全通信网络设计技术要求	8.3.3.4 物联网系统通信网络设计技术要求	a) 感知层网络数据传输完整性保护 应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准。	测评单元（L4-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。
		b) 感知层网络敏感数据传输保密性保护 应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准。	测评单元（L4-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。
		c) 感知层网络数据传输新鲜性保护 应在感知层网络传输的数据中加入数据发布的序列信息如时间戳、计数器等，以实现感知层网络数据传输新鲜性保护。	测评单元（L4-ADS4-01） 应核查感知节点设备鉴别数据新鲜性的措施，是否能够避免历史数据重放；应将感知节点设备历史数据进行重放测试，验证其保护措施是否生效。 测评单元（L4-ADS4-02）

			应访谈安全管理员针对感知节点设备历史数据的保护措施，具体措施有哪些，是否具有对历史数据被非法修改的检测措施，检测措施有哪些；应核查感知层是否配备检测感知节点设备历史数据被非法篡改的措施，在检测到被修改时是否能采取必要的恢复措施；应测试检测措施的有效性，是否能够避免数据的修改重放攻击。
		d) 异构网安全接入保护 应采用接入认证等技术建立异构网络的接入认证系统，保障控制信息的安全传输；应采用入侵检测等技术拒绝恶意设备的接入，保证合法设备不被恶意设备攻击而被拒绝接入，保证网络资源的可使用性；应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准；应根据各接入网的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并采取相应的防护措施。应对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击破坏数据完整性；应针对异构网接入点的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位，防止拒绝服务攻击、中间人攻击和伪造网络消息。	测评单元（L4-NCS1-12） 应核查是否采用技术措施防止非授权设备接入内部网络，并进行有效阻断；应核查所有路由器和交换机闲置端口是否均已关闭。 测评单元（L4-NCS1-03） 应核查是否依据某种原则划分不同的网络区域；应核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致。 测评单元（L4-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。 测评单元（L4-NCS4-03） 应访谈网络管理员感知节点设备接入网络时是否采用白名单技术、身份鉴别技术等，具体措施有哪些；应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述；应对边界和感知层网络进行渗透测试，测试是否存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。 测评单元（L4-NCS1-19） 应核查相关系统或设备是否能够检测从外部发起的网络攻击行为；应核查相关系统或设备的规则库版本是否已经更新到最新版本；应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点；应测试相关系统或设备，测试验

			证其安全策略是否有效。 测评单元（L4-NCS1-20） 应核查相关系统或设备是否能够检测到从内部发起的网络攻击行为；应核查相关系统或设备的规则库版本是否已经更新到最新版本；应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点；应测试相关系统或设备，测试验证其安全策略是否有效。 测评单元（L4-NCS1-21） 应核查是否部署网络回溯系统或抗 APT 攻击系统对新型网络攻击进行检测和分析；应测试验证是否对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析。
8.3.4 安全管理中心设计技术要求	8.3.4.1 系统管理	在进行物联网系统安全设计时，应通过系统管理员对感知设备状态（电力供应情况、是否在线、位置等）进行统一监测和处理；应通过系统管理员对下载到感知设备上的应用软件进行授权；可通过系统管理员对系统的可信基准库进行配置。	测评单元（L4-ECS4-01） 应核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更；应测试感知节点设备，可通过试图接入和控制传感网访问未授权的资源，验证访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效。 测评单元（L4-ECS4-08） 应访谈安全管理员感知节点设备是否支持对其关键配置参数进行在线更新；应核查感知节点设备在线更新方式是否有效。
	8.3.4.2 安全管理	在进行物联网系统安全设计时，应通过安全管理员对系统中所使用的密钥进行统一管理，包括密钥的生成、分发、更新、存储、备份、销毁等，并采取必要措施保证密钥安全；应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准；应通过安全管理员配置可信验证策	测评单元（L4-ECS4-07） 应访谈安全管理员有哪些感知节点设备需要采用密钥进行通信，是否对设备的关键密钥进行在线更新；应核查感知节点设备是否对其关键密钥进行在线更新。 测评单元（L4-CMS1-09） 应访谈建设负责人是否采用了密码产品及其相关服务，密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求。

		略。	

C.5 工业控制系统安全设计要求测评验证表

C.5.1 第一级

适用范围	功能要求	设计要求	测评要求
5.3.1 安全计算环境设计技术要求	5.3.1.5 工业控制系统安全计算环境设计技术要求	a) 工控设备身份鉴别 现场控制层设备及过程监控层设备应实施唯一性的标志、鉴别与认证，保证鉴别认证与功能完整性状态随时能得到实时验证与确认。在控制设备及监控设备上运行的程序、相应的数据集合应有唯一性标识管理。	测评单元（L1-NCS5-04） 应核查无线通信的用户在登录时是否采用了身份鉴别措施；应核查无线通信的用户列表，核查用户身份标识是否具有唯一性。 测评单元（L1-ECS5-01） 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。
		b) 现场设备访问控制 应对通过身份鉴别的用户实施基于角色的访问控制策略，现场设备收到操作命令后，应检验该用户绑定的角色是否拥有执行该操作的权限，拥有权限的该用户获得授权，用户未获授权应向上层发出报警信息。	测评单元（L1-NCS5-01） 应核查工业控制系统的网络是否部署单向隔离设备；应核查在网络边界处是否采用了有效的隔离策略；应核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离强度相同的措施。 测评单元（L1-NCS5-02） 应核查工业控制系统内部不同的子系统类型，是否按照安全等级、安全防护强度等业务特点划分了不同的安全域；应核查各安全域之间交换机、防火墙是否配置了有效的访问控制策略。 测评单元（L1-ECS5-01） 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；如控制设备不具备上述功能，则核查是否由其上位控制或管理设备

			实现同等功能或通过管理手段控制。
		c) 现场设备数据完整性保护 应在规定的时间内完成规定的任务，数据应以授权方式进行处理，确保数据不被非法篡改、不丢失、不延误，确保及时响应和处理事件，保护系统的同步机制、校时机制，保持控制周期稳定、现场总线轮询周期稳定；现场设备应能识别和防范破坏控制过程完整性的攻击行为，应能识别和防止以合法身份、合法路径干扰控制器等设备正常工作节奏的攻击行为；在控制系统遭到攻击无法保持正常运行时，应有故障隔离措施，应使系统导向预先定义好的安全的状态，将危害控制到最小范围。	测评单元（L1-ADS1-07） 应核查系统设计文档，重要管理数据、重要业务数据在传输过程中是否采用了校验码技术或密码技术保证完整性；应测试在传输过程中对重要管理数据、重要业务数据进行篡改，查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。
		d) 现场设备数据保密性保护 现场设备层设备及连接到现场控制层的现场总线设备内存储的有保密需要的数据、程序、配置信息的保密性保护，采取如下机制之一： 1) 应采用密码技术支持的保密性保护机制； 2) 应采用物理保护机制，对要保护的现场设备层设备及线路的邻近区域实施封闭或有人值守保护，防止非法接入、窃听、窃取、篡改、破坏等邻近攻击，对要保护的现场设备层设备及线路连接到现场控制层的 PLC、控制器等的接入点，应实施访问控制、状态监测等安全措施，确保其保护能力不低于同级的应用密码等技术支持的保护强度。	— —
5.3.2 安	5.3.2.5 工	a) 区域边界包过滤 可根据区域边界安全控制策略，通过检	测评单元（L1-NCS1-04） 应确认等级保护对象的网络边界位置，并核查在网

全区域边界设计技术要求	业控制系统区域边界设计技术要求	查数据包的源地址、目的地址、传输层协议和请求的服务等，确定是否允许该数据包通过该区域边界。	络边界处是否部署访问控制设备；应核查设备配置信息，是否指定端口进行跨越边界的网络通信，该端口配置并启用了安全策略；应采用其他技术手段（如非法无线网络设备定位检查、核查设备配置信息等）核查是否不存在其他未受控端口进行跨越边界的网络通信。 测评单元（L1-NCS1-05） 应核查在网络边界是否部署访问控制设备，是否启用访问控制策略；应核查设备的最后一条访问控制策略是否为禁止所有网络通信。 测评单元（L1-NCS1-06） 应核查设备是否不存在多余或无效的访问控制策略；应核查设备的不同访问控制策略之间的逻辑关系及前后排列顺序是否合理。 测评单元（L1-NCS1-07） 应核查设备访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数。
		b) 区域边界恶意代码防范 可在安全区域边界设置防恶意代码软件，并定期进行升级和更新，以防止恶意代码入侵。	— —
5.3.3 安全通信网络设计技术要求	5.3.3.5 工业控制系统通信网络设计技术要求	a) 现场总线网络数据传输完整性保护 对现场总线网络数据完整性保护采取如下机制之一： 1) 应采用适应现场总线特点的报文短、时延小的密码技术支持的完整性校验机制，以实现现场总线网络数据传输完整性保护； 2) 应采取物理保护措施，对要保护的现场总线和设备的邻近区域实施封闭或有人值守保护，防止非法接入、篡改、破坏等邻近攻击。	测评单元（L1-NCS1-03） 应核查是否在数据传输过程中使用校验码技术来保护其完整性。
		b) 无线网络数据传输完整性保护	测评单元（L1-NCS1-03）

		应采用密码技术支持的完整性校验机制，以实现无线网络数据传输完整性保护。	应核查是否在数据传输过程中使用校验码技术来保护其完整性。
		c) 通信网络异常监测 应对工业控制系统的通讯数据、访问异常、业务操作异常、网络和设备流量、工作周期、抖动值、运行模式、各站点状态、冗余机制等进行监测，发生异常进行报警；在有冗余现场总线和表决器的应用场合，可充分监测各冗余链路在同时刻的状态，捕获可能的恶意或入侵行为；应在相应的网关设备上流量监测与管控，对超出最大 PPS 阈值的通信进行控制并报警。	— —
		d) 无线网络攻击的防护 应对通过无线网络攻击的潜在威胁和可能产生的后果进行风险分析，应对可能遭受无线攻击的设备的信息发出（信息外泄）和进入（非法操控）进行屏蔽，可综合采用检测和干扰、电磁屏蔽、微波暗室吸收、物理保护等方法，在可能传播的频谱范围将无线信号衰减到不能有效接收的程度，避免邻近攻击。	测评单元（L1-NCS5-04） 应核查无线通信的用户在登录时是否采用了身份鉴别措施；应核查无线通信的用户列表，核查用户身份标识是否具有唯一性。 测评单元（L1-NCS5-05） 应核查无线配置文件是否对连接的授权、监视及执行进行限制。

C.5.2 第二级

适用范围	功能要求	设计要求	测评要求
6.3.1 安全计算环境设计技术要求	6.3.1.5 工业控制系统安全计算环境设计技术	a) 工控设备身份鉴别 现场控制层设备及过程监控层设备应实施唯一性的标志、鉴别与认证，保证鉴别认证与功能完整性状态随时能得到实时验证与确认。在控制设备及监控设备	测评单元（L2-NCS5-04） 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。 测评单元（L2-ECS5-01）

要求	上运行的程序、相应的数据集合应有唯一性标识管理。	应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。
	b) 现场设备访问控制 应对通过身份鉴别的用户实施基于角色的访问控制策略，现场设备收到操作命令后，应检验该用户绑定的角色是否拥有执行该操作的权限，拥有权限的该用户获得授权，用户未获授权应向上层发出报警信息。	测评单元（L2-NCS5-05） 应核查在工业控制系统与企业其他系统之间的网络边界是否部署访问控制设备，是否配置访问控制策略；应核查设备安全策略，是否禁止 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越边界。 测评单元（L2-NCS5-06） 应核查设备是否可以在策略失效的时候进行告警；应核查是否部署监控预警系统或相关模块，在边界防护机制失效时可及时告警。
	c) 现场设备数据完整性保护 应在规定的时间内完成规定的任务，数据应以授权方式进行处理，确保数据不被非法篡改、不丢失、不延误，确保及时响应和处理事件，保护系统的同步机制、校时机制，保持控制周期稳定、现场总线轮询周期稳定；现场设备应能识别和防范破坏控制过程完整性的攻击行为，应能识别和防止以合法身份、合法路径干扰控制器等设备正常工作节奏的攻击行为；在控制系统遭到攻击无法保持正常运行时，应有故障隔离措施，应使系统导向预先定义好的安全的状态，将危害控制到最小范围。	测评单元（L2-NCS5-04） 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。
	d) 现场设备数据保密性保护 现场设备层设备及连接到现场控制层的现场总线设备内存储的有保密需要的数据、程序、配置信息的保密性保护，采	测评单元（L2-NCS5-04） 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。

		取如下机制之一： 1) 应采用密码技术支持的保密性保护机制； 2) 应采用物理保护机制，对要保护的现场设备层设备及线路的邻近区域实施封闭或有人值守保护，防止非法接入、窃听、窃取、篡改、破坏等邻近攻击，对要保护的现场设备层设备及线路连接到现场控制层的 PLC、控制器等的接入点，应实施访问控制、状态监测等安全措施，确保其保护能力不低于同级的应用密码等技术支持的保护强度。	测评单元（L2-NCS5-01） 应核查工业控制系统的网络是否部署单向隔离设备；应核查在网络边界处是否采用了有效的隔离策略。
6.3.2 安全区域边界设计技术要求	6.3.2.5 工业控制系统区域边界设计技术要求	a) 区域边界包过滤 应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议和请求的服务等，确定是否允许该数据包通过该区域边界。	测评单元（L2-NCS5-05） 应核查在工业控制系统与企业其他系统之间的网络边界是否部署访问控制设备，是否配置访问控制策略；应核查设备安全策略，是否禁止 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越边界。
		b) 区域边界安全审计 应在安全区域边界设置审计机制，并由安全管理中心统一管理。	测评单元（L2-NCS1-12） 应核查设备是否开启了日志记录或安全审计功能；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行了审计。 测评单元（L2-NCS1-13） 应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。
		c) 区域边界恶意代码防范 可在安全区域边界设置防恶意代码网关，由安全管理中心管理。	— —
		d) 区域边界完整性保护 应在安全区域边界设置实时监测告警机制，通过安全管理中心集中管理，对确	— —

		认的违规行为及时向安全管理中心和工控值守人员报警并做出相应处置。	
6.3.3 安全通信网络设计技术要求	6.3.3.5 工业控制系统通信网络设计技术要求	a) 现场总线网络数据传输完整性保护 对现场总线网络数据完整性保护采取如下机制之一： 1) 应采用适应现场总线特点的报短文、时延小的密码技术支持的完整性校验机制，以实现现场总线网络数据传输完整性保护； 2) 应采取物理保护措施，对要保护的现场总线和设备的邻近区域实施封闭或有人值守保护，防止非法接入、篡改、破坏等邻近攻击。	测评单元（L2-NCS5-01） 应核查工业控制系统的网络是否部署单向隔离设备；应核查在网络边界处是否采用了有效的隔离策略。 测评单元（L2-NCS5-02） 应核查工业控制系统内部不同的子系统类型，是否按照安全等级和安全防护强度等业务特点划分了不同的安全域；应核查各安全域之间交换机和防火墙是否配置了有效的访问控制策略。 测评单元（L2-NCS5-03） 应核查工业控制系统关键区域的传输数据要求，涉及实时传输数据与控制要求的，核查是否采用独立的网络和设备组网实现关键部位安全防护。
		b) 无线网络数据传输完整性保护 应采用密码技术支持的完整性校验机制，以实现无线网络数据传输完整性保护。	测评单元（L2-NCS5-01） 应核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离强度相同的措施。
		c) 通信网络异常监测 应对工业控制系统的通讯数据、访问异常、业务操作异常、网络和设备流量、工作周期、抖动值、运行模式、各站点状态、冗余机制等进行监测，发生异常进行报警；在有冗余现场总线和表决器的应用场合，可充分监测各冗余链路在同时刻的状态，捕获可能的恶意或入侵行为；应在相应的网关设备上流量监测与管控，对超出最大 PPS 阈值的通信进行控制并报警。	测评单元（L2-NCS5-09） 应核查无线通信过程中是否对用户进行授权，核查具体权限是否合理；核查未授权的使用是否可以被发现及告警。
		d) 无线网络攻击的防护 应对通过无线网络攻击的潜在威胁和可	测评单元（L2-NCS5-01） 应核查使用无线通信的工业控制系统边界是否采

		能产生的后果进行风险分析，应对可能遭受无线攻击的设备的信息发出（信息外泄）和进入（非法操控）进行屏蔽，可综合采用检测和干扰、电磁屏蔽、微波暗室吸收、物理保护等方法，在可能传播的频谱范围将无线信号衰减到不能有效接收的程度，避免邻近攻击。	用与企业其他系统隔离强度相同的措施。
6.3.4 安全管理中心设计技术要求	6.3.4.1 审计管理	在进行工业控制系统安全设计时，通过安全管理员能够对工业控制现场控制设备、信息安全设备、网络设备、服务器、操作站等设备中主体和客体进行登记，并对各设备的信息安全监控和报警、信息安全日志信息进行集中管理。根据安全审计策略对各类信息安全信息进行分类管理与查询，并生成统一的审计报告。	

C.5.3 第三级

适用范围	功能要求	设计要求	测评要求
7.3.1 安全计算环境设计技术要求	7.3.1.5 工业控制系统安全计算环境设计技术要求	a) 工业控制身份鉴别 现场控制层设备及过程监控层设备应实施唯一性的标志、鉴别与认证，保证鉴别认证与功能完整性状态随时能得到实时验证与确认。在控制设备及监控设备上运行的程序、相应的数据集合应有唯一性标识管理，防止未经授权的修改。	测评单元（L3-NCS5-07） 应核查工业控制系统是否确需使用拨号服务； 应核查拨号设备是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用账户/口令等身份鉴别方式，是否采用控制账户权限等访问控制措施。 测评单元（L3-NCS5-09） 应核查无线通信的用户在登录时是否采用了身份鉴别措施；应核查无线通信的用户列表，核查用户身份标识是否具有唯一性。 测评单元（L3-NCS5-10） 应核查无线通信过程中是否对用户进行授权，核查具体权限是否合理；核查未授权的使用是

			否可以被发现及告警。 测评单元（L3-ECS5-01） 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。
		b) 现场设备访问控制 应对通过身份鉴别的用户实施基于角色的访问控制策略，现场设备收到操作命令后，应检验该用户绑定的角色是否拥有执行该操作的权限，拥有权限的该用户获得授权，用户未获授权应向上层发出报警信息。只有获得授权的用户才能对现场设备进行组态下装、软件更新、数据更新、参数设定等操作。	测评单元（L3-NCS5-01） 应核查工业控制系统的网络是否部署单向隔离设备；应核查在网络边界处是否采用了有效的单向隔离策略实施访问控制；应核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离强度相同的措施。 测评单元（L3-NCS5-02） 应核查工业控制系统内部不同的子系统类型，是否按照安全等级和安全防护强度等业务特点划分了不同的安全域；应核查各安全域之间交换机和防火墙是否配置了有效的访问控制策略。 测评单元（L3-NCS5-07） 应核查工业控制系统是否确需使用拨号服务；应核查拨号设备是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用账户/口令等身份鉴别方式，是否采用控制账户权限等访问控制措施。 测评单元（L3-ECS5-01） 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。

		c) 现场设备安全审计 在有冗余的重要应用环境，双重或多重控制器可采用实时审计跟踪技术，确保及时捕获信息安全事件信息并报警。	测评单元（L3-ECS5-01） 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。 测评单元（L3-MMS5-05） 应访谈安全管理员是否建立跨单位处置工业控制系统安全事件流程；应核查跨单位安全事件报告和处置管理制度，核查是否含有工业控制系统联合防护和应急的相关内容。
		d) 现场设备数据完整性保护 现场控制层设备、现场设备层设备和连接到现场设备层的现场总线设备之间点对点通信过程数据完整性保护应采取如下安全机制之一： 1) 应采用密码技术进行会话认证，通过会话密钥建立、会话失效时长设置、会话自动重连等措施保证会话完整性； 2) 应采用物理保护措施，对要保护的现场控制层设备、现场设备层设备和现场总线设备及其邻近区域实施封闭或有人值守保护，防止非法替换、假冒等攻击。	测评单位（L3-NCS5-04） 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。 测评单位（L3-NCS5-08） 应核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施。
		e) 现场设备数据保密性保护 现场设备层设备及连接到现场控制层的现场总线设备内存储的有保密需要的数据、程序、配置信息的保密性保护，采取如下机制之一： 1) 应采用密码技术支持的保密性保护机制； 2) 应采用物理保护机制，对要保护的	测评单位（L3-NCS5-04） 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。 测评单位（L3-NCS5-08） 应核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施。 测评单元（L3-NCS5-11）

		现场设备层的设备、线路的邻近区域实施封闭或有人值守保护,防止非法接入、窃听、窃取、篡改、破坏等邻近攻击; 对于要保护的现场设备层的设备、线路连接到现场控制层的 PLC、控制器等的接入点,应实施访问控制、状态监测等安全措施,确保其保护能力不低于同级的应用密码等技术支持的保护强度。	应核查无线通信传输中是否采用加密措施保证传输报文的机密性。
		f) 控制过程完整性保护 应在规定的时间内完成规定的任务,数据应以授权方式进行处理,确保数据不被非法篡改、不丢失、不延误,确保及时响应和处理事件,保护系统的同步机制、校时机制,保持控制周期稳定、现场总线轮询周期稳定;现场设备应能识别和防范破坏控制过程完整性的攻击行为,应能识别和防止以合法身份、合法路径干扰控制器等设备正常工作节奏的攻击行为;在控制系统遭到攻击无法保持正常运行时,应有故障隔离措施,应使系统导向预先定义好的安全的状态,将危害控制到最小范围。	测评单元 (L3-ECS5-04) 应核查更新控制设备时是否为专用设备和专用软件。 测评单元 (L3-ECS5-05) 应核查控制设备在上线前的检测报告,明确控制设备固件中是否不存在恶意代码程序。
7.3.2 安全区域边界设计技术要求	7.3.2.5 工业控制系统区域边界设计技术要求	a) 工控通信协议的数据过滤 对通过安全区域边界的工控通信协议,应能识别其所承载的数据有可能对工控系统造成攻击或破坏,应控制通信流量、帧数量频度、变量的读取频度稳定且在正常范围内,保护控制器的工作节奏,识别和过滤写变量参数超出正常范围的数据,该控制过滤处理组件可配置在区域边界的网络设备上,也可配置在本安全区域内的工控通信协议的端设备上	测评单位 (L3-NCS5-04) 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。 测评单元 (L3-NCS5-05) 应核查在工业控制系统与企业其他系统之间的网络边界是否部署访问控制设备,是否配置访问控制策略;应核查设备安全策略,是否禁止 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越边界。

		或唯一的通信链路设备上。	
		b) 对工控通信协议信息泄露的防护 对暴露本区域工控通信协议端点设备的用户名和登录密码,应防止其被利用对工控系统造成危害,可采取以下措施之一: 1) 应采用过滤变换技术,隐藏用户名和登录密码等关键信息,防止信息泄漏; 2) 应将工控通信协议端点设备单独划分配置在一个新的安全区域内,与其它设备隔离,对所有进出新的安全区域的信息实施过滤; 3) 其它防止信息泄漏的方法。	测评单元 (L3-NCS5-11) 应核查无线通信传输中是否采用加密措施保证传输报文的机密性。 测评单元 (L3-NCS5-02) 应核查工业控制系统内部不同的子系统类型,是否按照安全等级和安全防护强度等业务特点划分了不同的安全域;应核查各安全域之间交换机和防火墙是否配置了有效的访问控制策略。 测评单元 (L4-NCS5-03) 应核查工业控制系统关键区域的传输数据要求,涉及实时传输数据与控制要求的,核查是否采用独立的网络和设备组网实现关键部位安全防护。
		c) 工控区域边界安全审计 应在安全区域边界设置实时监测告警机制,通过安全管理中心集中管理,对确认的违规行为及时向安全管理中心和工控值守人员报警并做出相应处置。	测评单元 (L3-NCS5-06) 应核查设备是否可以在策略失效的时候进行告警;应核查是否部署监控预警系统或相关模块,在边界防护机制失效时可及时告警。
7.3.3 安全通信网络设计技术要求	7.3.3.5 工业控制系统通信网络设计技术要求	a) 现场总线网络数据传输完整性保护 对现场总线网络数据完整性保护采取如下机制之一: 1) 应采用适应现场总线特点的报文短、时延小的密码技术支持的完整性校验机制,以实现现场总线网络数据传输完整性保护; 2) 应采取物理保护措施,对要保护的现场总线和设备的邻近区域实施封闭或有人值守保护,防止非法接入、篡改、破坏等邻近攻击。	测评单位 (L3-NCS5-04) 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。 测评单位 (L3-NCS5-08) 应核查拨号服务器和客户端是否使用经安全加固的操作系统,并采取加密、数字证书认证和访问控制等安全防护措施。
		b) 无线网络数据传输完整性保护	测评单位 (L3-NCS5-04)

		应采用密码技术支持的完整性校验机制，以实现无线网络数据传输完整性保护。	应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。 测评单位（L3-NCS5-08） 应核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施。
		c) 现场总线网络数据传输保密性保护 对现场总线网络数据保密性保护采取如下机制之一： 1) 应采用适应现场总线特点的报文短、时延小的密码技术支持的保密性保护机制，以实现现场总线网络数据传输保密性保护； 2) 应采取的物理保护措施，对要保护的现场总线和设备的邻近区域实施封闭或有人值守保护，防止非法接入、窃听、破坏等邻近攻击。	测评单位（L3-NCS5-04） 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。 测评单位（L3-NCS5-08） 应核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施。 测评单元（L3-NCS5-11） 应核查无线通信传输中是否采用加密措施保证传输报文的机密性。
		c) 无线网络数据传输保密性保护 应采用由密码技术支持的保密性保护机制，以实现无线网络数据传输保密性保护。	测评单元（L3-NCS5-11） 应核查无线通信传输中是否采用加密措施保证传输报文的机密性。
		d) 工业控制网络实时响应要求 对实时响应和操作要求高的场合，应把工业控制通信会话过程设计为三个阶段：开始阶段，应完成对主客体身份鉴别和授权；运行阶段，应保证对工业控制系统的实时响应和操作，此阶段应对主客体的安全状态实时监测；结束阶段，应以显式的方式结束。在需要连续运行的场合，人员交接应不影响实时性，应保证访问控制机制的持续性。	测评单元（L3-NCS5-07） 应核查工业控制系统是否确需使用拨号服务； 应核查拨号设备是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用账户/口令等身份鉴别方式，是否采用控制账户权限等访问控制措施。 测评单元（L3-NCS5-09） 应核查无线通信的用户在登录时是否采用了身份鉴别措施；应核查无线通信的用户列表，核查用户身份标识是否具有唯一性。

			测评单元（L3-ECS5-01） 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。
		e) 通信网络异常监测 应对工业控制系统的通讯数据、访问异常、业务操作异常、网络和设备流量、工作周期、抖动值、运行模式、各站点状态、冗余机制等进行监测，发生异常进行报警；在有冗余现场总线和表决器的应用场合，可充分监测各冗余链路在同时刻的状态，捕获可能的恶意或入侵行为；应在相应的网关设备上对流量进行监测与管控，对超出最大 PPS 阈值的通信进行控制并报警。	测评单元（L3-NCS5-12） 应核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备应及时发出告警并可以对试图接入的无线设备进行屏蔽。
		f) 无线网络攻击的防护 应对通过无线网络攻击的潜在威胁和可能产生的后果进行风险分析，应对可能遭受无线攻击的设备的信息发出（信息外泄）和进入（非法操控）进行屏蔽，可综合采用检测和干扰、电磁屏蔽、微波暗室吸收、物理保护等方法，在可能传播的频谱范围将无线信号衰减到不能有效接收的程度，避免邻近攻击。	测评单元（L3-NCS5-09） 应核查无线通信的用户在登录时是否采用了身份鉴别措施；应核查无线通信的用户列表，核查用户身份标识是否具有唯一性。 测评单元（L3-NCS5-10） 应核查无线通信过程中是否对用户进行授权，核查具体权限是否合理；核查未授权的使用是否可以被发现及告警。 测评单元（L3-NCS5-11） 应核查无线通信传输中是否采用加密措施保证传输报文的机密性。 测评单元（L3-NCS5-12） 应核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备

			应及时发出告警并可以对试图接入的无线设备进行屏蔽。
7.3.4 安全管理中心设计技术要求	7.3.4.1 安全管理	在进行工业控制系统安全设计时，安全管理还应符合以下要求： a) 通过安全管理员能够对工业控制系统设备的可用性和安全性进行实时监控，可以对监控指标设置告警阈值，触发告警并记录； b) 通过安全管理员能够在安全管理中心呈现工业控制系统设备间的访问关系，形成基于网络访问关系、业务操作指令的工业控制环境的行为白名单，协助安全管理员及时发现未定义的信息通讯行为以及识别重要业务操作指令级的异常。	测评单元（L3-MMS5-05） 应访谈安全管理员是否建立跨单位处置工业控制系统安全事件流程；应核查跨单位安全事件报告和处置管理制度，核查是否含有工业控制系统联合防护和应急的相关内容。 测评单元（L3-NCS5-12） 应核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备应及时发出告警并可以对试图接入的无线设备进行屏蔽。
	7.3.4.3 审计管理	在进行工业控制系统安全设计时，审计管理还应符合以下要求：通过安全管理员能够对工业控制现场控制设备、信息安全设备、网络设备、服务器、工作站等设备中主体和客体进行登记，并对各设备的信息安全监控和报警、信息安全日志信息进行集中管理。根据安全审计策略对各类信息安全信息进行分类管理与查询，并生成统一的审计报告。系统对各类信息安全报警和日志信息进行关联分析。	测评单元（L3-MMS5-05） 应访谈安全管理员是否建立跨单位处置工业控制系统安全事件流程；应核查跨单位安全事件报告和处置管理制度，核查是否含有工业控制系统联合防护和应急的相关内容。 测评单元（L3-NCS5-12） 应核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备应及时发出告警并可以对试图接入的无线设备进行屏蔽。

C.5.4 第四级

适用范围	功能要求	设计要求	测评要求
8.3.1 安全计算环	8.3.1.5 工业控制系统	a) 工控设备身份鉴别 现场控制层设备、现场设备层设备以及	测评单元（L4-NCS5-07） 应核查工业控制系统是否确需使用拨号服务；应核查拨号设备是否限制具有拨号访问权限的用户数

境设计技 术要求	安全计算环 境设计技术 要求	过程监控层设备应实施唯一性的标识、鉴别与认证，保证鉴别认证与功能完整性状态随时能得到实时验证与确认；在关键设施的主体与客体间可实施双向鉴别与认证，防止假冒或未经授权的替代。在控制设备及监控设备上运行的程序、相应的数据集应有唯一性标识管理，防止未经授权的修改。	量，拨号服务器和客户端是否使用账户、口令等身份鉴别方式，是否采用控制账户权限等访问控制措施。 测评单元（L4-NCS5-10） 应核查无线通信的用户在登录时是否采用了身份鉴别措施；应核查无线通信的用户列表，核查用户身份标识是否具有唯一性。 测评单元（L4-ECS5-01） 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。
		b) 现场设备访问控制 应对通过身份鉴别的用户实施基于角色的访问控制策略，现场设备收到操作命令后，应检验该用户绑定的角色是否拥有执行该操作的权限，拥有权限的该用户获得授权，用户未获授权应向上层发出报警信息。只有获得授权的用户才能对现场设备进行组态下装、软件更新、数据更新、参数设定等操作，才能对控制器的操作界面进行操作； OPC 服务器和客户机可分别单独放置在各自的安全区内，以访问控制设备进行隔离保护，应对进出安全区的信息实行访问控制等安全策略。	测评单元（L4-NCS5-01） 应核查工业控制系统的网络是否部署单向隔离设备；应核查在网络边界处是否采用了有效的单向安全隔离策略实施访问控制；应核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离强度相同的措施；应核查所使用的专用产品是否符合国家规定，如有行业特殊规定的是否符合行业规定。测评单元（L4-NCS5-02） 应核查工业控制系统内部不同的子系统类型，是否按照安全等级、安全防护强度等业务特点划分了不同的安全域；应核查各安全域之间交换机、防火墙是否配置了有效的访问控制策略。 测评单元（L4-NCS5-03） 应核查工业控制系统关键区域的传输数据要求，涉及实时传输数据与控制要求的，核查是否采用独立的网络和设备组网实现关键部位安全防护。 测评单元（L4-NCS5-05） 应核查在工业控制系统与企业其他系统之间的网络边界是否部署访问控制设备，是否配置访问控制策略；应核查设备安全策略，是否禁止 E-Mail、Web、

		Telnet、Rlogin、FTP 等通用网络服务穿越边界。 测评单元（L4-NCS5-07） 应核查工业控制系统是否确需使用拨号服务；应核查拨号设备是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用账户、口令等身份鉴别方式，是否采用控制账户权限等访问控制措施。 测评单元（L4-NCS5-09） 应核查涉及实时控制和数据传输的工业控制系统内是否禁止使用拨号访问服务。 测评单元（L4-NCS5-11） 应核查无线通信过程中是否对用户进行授权，核查具体权限是否合理；核查未授权的使用是否可以被发现及告警。 测评单元（L4-ECS5-01） 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。 测评单元（L4-ECS5-02） 应核查测试环境或测试报告，核查是否有测试评估记录；应核查控制设备版本、补丁及固件是否经过测试后进行了更新。 测评单元（L4-ECS5-04） 应核查更新控制设备时是否为专用设备和专用软件。	Telnet、Rlogin、FTP 等通用网络服务穿越边界。 测评单元（L4-NCS5-07） 应核查工业控制系统是否确需使用拨号服务；应核查拨号设备是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用账户、口令等身份鉴别方式，是否采用控制账户权限等访问控制措施。 测评单元（L4-NCS5-09） 应核查涉及实时控制和数据传输的工业控制系统内是否禁止使用拨号访问服务。 测评单元（L4-NCS5-11） 应核查无线通信过程中是否对用户进行授权，核查具体权限是否合理；核查未授权的使用是否可以被发现及告警。 测评单元（L4-ECS5-01） 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。 测评单元（L4-ECS5-02） 应核查测试环境或测试报告，核查是否有测试评估记录；应核查控制设备版本、补丁及固件是否经过测试后进行了更新。 测评单元（L4-ECS5-04） 应核查更新控制设备时是否为专用设备和专用软件。
		c) 现场设备安全审计 在有冗余的重要应用环境，双重或多重控制器应采用实时审计跟踪技术，确保及时捕获信息安全事件信息并报警。	测评单元（L4-NCS5-13） 应核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备应及时发出告警并可以对试图接入的无线设备进行屏蔽； 测评单元（L4-MMS5-05） 应访谈安全管理员是否建立跨单位处置工业控制

			系统安全事件流程；应核查跨单位安全事件报告和处置管理制度，核查是否含有工业控制系统联合防护和应急的相关内容。
		d) 现场设备数据完整性保护 现场控制层设备、现场设备层设备和连接到现场设备层的现场总线设备之间点对点通信过程数据完整性保护应采取如下安全机制之一： 1) 应采用密码技术进行会话认证，通过会话密钥建立、会话失效时长设置、会话自动重连等措施保证会话完整性； 2) 应采用物理保护措施，对要保护的现场控制层设备、现场设备层设备和现场总线设备及其邻近区域实施封闭或有人值守保护，防止非法替换、假冒等攻击。	测评单位（L4-NCS5-04） 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。 测评单位（L4-NCS5-08） 应核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施。
		e) 现场设备数据保密性保护 现场设备层设备及连接到现场控制层的现场总线设备内存储的有保密需要的数据、程序、配置信息的保密性保护，采取如下机制之一： 1) 应采用密码技术支持的保密性保护机制； 2) 应采用物理保护机制，对要保护的现场设备层的设备、线路的邻近区域实施封闭或有人值守保护，防止非法接入、窃听、窃取、篡改、破坏等邻近攻击； 对于要保护的现场设备层的设备、线路连接到现场控制层的 PLC、控制器等的接入点，应实施访问控制、状态监测等安全措施，确保其保护能力不低于同级的应用密码等技术支持的保护强度。	测评单位 L4-NCS5-04 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。 测评单位（L4-NCS5-08） 应核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施。 测评单元（L4-NCS5-12） 应核查无线通信传输中是否采用加密措施保证传输报文的机密性。

	f) 程序安全执行保护 应构建从工程师站组态逻辑通过通讯链路下装到现场控制层的控制设备进行接收、存储的信任链或安全可控链，构建控制回路中从控制设备启动程序到操作系统（如果有的）直至到调用控制应用程序、现场总线的接收-发送模块、现场设备层设备接收-发送模块的程序的信任链或安全可控链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时采取措施恢复；应构建基于系统的整个完整链路的可信的或安全可控的时钟源、可信的或安全可控的同步和校时机制，防范恶意干扰和破坏。	测评单元（L4-ECS5-04） 应核查更新控制设备时是否为专用设备和专用软件。 测评单元（L4-ECS5-05） 应核查控制设备在上线前的检测报告，明确控制设备固件中是否不存在恶意代码程序。
	g) 控制过程完整性保护 应在规定的时间内完成规定的任务，数据应以授权方式进行处理，确保数据不被非法篡改、不丢失、不延误，确保及时响应和处理事件，保护系统的同步机制、校时机制，保持控制周期稳定、现场总线轮询周期稳定；现场设备应能识别和防范破坏控制过程完整性的攻击行为，应能识别和防止以合法身份、合法路径干扰控制器等设备正常工作节奏的攻击行为；在控制系统遭到攻击无法保持正常运行时，应有故障隔离措施，应使系统导向预先定义好的安全的状态，将危害控制到最小范围。	测评单元（L4-ECS5-04） 应核查更新控制设备时是否为专用设备和专用软件。 测评单元（L4-ECS5-05） 应核查控制设备在上线前的检测报告，明确控制设备固件中是否不存在恶意代码程序。
	h) 资源控制 应对访问者进行身份鉴别和访问控制，	测评单元（L4-ECS5-01） 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备

		只有通过授权的访问者才可访问控制系统关键数据。应通过数据采集模块将控制器的 CPU、内存、堆栈等实时数据进行定时采集、分析，以监测控制器的安全状态，对异常情况进行报警。	上述功能，则按照通用要求测评；如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。 测评单元（L4-ECS5-04） 应核查更新控制设备时是否为专用设备和专用软件。
8.3.2 安全区域边界设计技术要求	8.3.2.5 工业控制系统区域边界设计技术要求	a) 工控通信协议的数据过滤 对通过安全区域边界的工控通信协议，应能识别其所承载的数据有可能对工控系统造成攻击或破坏，应控制通信流量、帧数量频度、变量的读取频度稳定且在正常范围内，保护控制器的工作节奏，识别和过滤写变量参数超出正常范围的数据，该控制过滤处理组件可配置在区域边界的网络设备上，也可配置在本安全区域内的工控通信协议的端点设备上或唯一的通信链路设备上。	测评单元（L4-NCS5-04） 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。 测评单元（L4-NCS5-05） 应核查在工业控制系统与企业其他系统之间的网络边界是否部署访问控制设备，是否配置访问控制策略；应核查设备安全策略，是否禁止 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务穿越边界。
		b) 对工控通信协议信息泄露的防护 对暴露本区域工控通信协议端点设备的用户名和登录密码，应防止其被利用对工控系统造成危害，可采取以下措施之一： 1) 应采用过滤变换技术，隐藏用户名和登录密码等关键信息，防止信息泄漏； 2) 应将工控通信协议端点设备单独划分配置在一个新的安全区域内，与其它设备隔离，对所有进出新的安全区域的信息实施过滤； 3) 其它防止信息泄漏的方法。	测评单元（L4-NCS5-12） 应核查无线通信传输中是否采用加密措施保证传输报文的机密性。 测评单元（L4-NCS5-02） 应核查工业控制系统内部不同的子系统类型，是否按照安全等级、安全防护强度等业务特点划分了不同的安全域；应核查各安全域之间交换机、防火墙是否配置了有效的访问控制策略。 测评单元（L4-NCS5-03） 应核查工业控制系统关键区域的传输数据要求，涉及实时传输数据与控制要求的，核查是否采用独立的网络和设备组网实现关键部位安全防护。
		c) 工控区域边界安全审计 应在安全区域边界设置实时监测告警机	测评单元（L4-NCS5-06） 应核查设备是否可以在策略失效的时候进行告警； 应核查是否部署监控预警系统或相关模块，在边界

		制，通过安全管理中心集中管理，对确认的违规行为及时向安全管理中心和工控值守人员报警并做出相应处置。	防护机制失效时可及时告警。
8.3.3 安全通信网络设计技术要求	8.3.3.5 工业控制系统通信网络设计技术要求	a) 总线网络安全审计 应支持工控总线网络审计，可通过工控交换机做安全审计或提供总线审计的接口对访问控制、请求错误、系统事件、备份和存储事件、配置变更、潜在的侦查行为等事件进行审计。	测评单元 (L4-MMS5-05) 应访谈安全管理员是否建立跨单位处置工业控制系统安全事件流程；应核查跨单位安全事件报告和处置管理制度，核查是否含有工业控制系统联合防护和应急的相关内容。
		b) 现场总线网络数据传输完整性保护 对现场总线网络数据完整性保护采取如下机制之一： 1) 应采用适应现场总线特点的报文短、时延小的密码技术支持的完整性校验机制，以实现现场总线网络数据传输完整性保护； 2) 应采取物理保护措施，对要保护的现场总线和设备的邻近区域实施封闭或有人值守保护，防止非法接入、篡改、破坏等邻近攻击。	测评单位 (L4-NCS5-04) 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。 测评单位 (L4-NCS5-08) 应核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施。
		c) 无线网络数据传输完整性保护 应采用密码技术支持的完整性校验机制，以实现无线网络数据传输完整性保护。	测评单元 (L4-NCS5-12) 应核查无线通信传输中是否采用加密措施保证传输报文的机密性。 测评单位 (L4-NCS5-04) 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。 测评单位 (L4-NCS5-08) 应核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施。

		d) 现场总线网络数据传输保密性保护 对现场总线网络数据保密性保护采取如下机制之一： 1) 应采用适应现场总线特点的报文短、时延小的密码技术支持的保密性保护机制，以实现现场总线网络数据传输保密性保护； 2) 应采取的物理保护措施，对要保护的现场总线和设备的邻近区域实施封闭或有人值守保护，防止非法接入、窃听、破坏等邻近攻击。	测评单位（L4-NCS5-04） 应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。 测评单位（L4-NCS5-08） 应核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施。 测评单元（L4-NCS5-12） 应核查无线通信传输中是否采用加密措施保证传输报文的机密性。
		e) 无线网络数据传输保密性保护 应采用由密码技术支持的保密性保护机制，以实现无线网络数据传输保密性保护。	测评单元（L4-NCS5-12） 应核查无线通信传输中是否采用加密措施保证传输报文的机密性。
		f) 工业控制网络实时响应要求 对实时响应和操作要求高的场合，应把工业控制通信会话过程设计为三个阶段：开始阶段，应完成对主客体身份鉴别和授权；运行阶段，应保证对工业控制系统的实时响应和操作，此阶段应对主客体的安全状态实时监测；结束阶段，应以显式的方式结束。在需要连续运行的场合，人员交接应不影响实时性，应保证访问控制机制的持续性。	测评单元（L4-NCS5-07） 应核查工业控制系统是否确需使用拨号服务；应核查拨号设备是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用账户、口令等身份鉴别方式，是否采用控制账户权限等访问控制措施。 测评单元（L4-NCS5-10） 应核查无线通信的用户在登录时是否采用了身份鉴别措施；应核查无线通信的用户列表，核查用户身份标识是否具有唯一性。 测评单元（L4-ECS5-01） 应核查控制设备是否具有身份鉴别、访问控制和安全审计等设备和计算方面的功能，如控制设备具备上述功能，则按照通用要求测评；如控制设备不具备上述功能，则核查是否由其上位控制或管理设备实现同等功能或通过管理手段控制。
		g) 通信网络异常监测	测评单元（L4-NCS5-13）

		应对工业控制系统的通讯数据、访问异常、业务操作异常、网络和设备流量、工作周期、抖动值、运行模式、各站点状态、冗余机制等进行监测，发生异常进行报警；在有冗余现场总线和表决器的应用场合，可充分监测各冗余链路在同时刻的状态，捕获可能的恶意或入侵行为；应在相应的网关设备上流量监测与管控，对超出最大 PPS 阈值的通信进行控制并报警。	应核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备应及时发出告警并可以对试图接入的无线设备进行屏蔽。
		h) 无线网络攻击的防护 应对通过无线网络攻击的潜在威胁和可能产生的后果进行风险分析，应对可能遭受无线攻击的设备的信息发出（信息外泄）和进入（非法操控）进行屏蔽，可综合采用检测和干扰、电磁屏蔽、微波暗室吸收、物理保护等方法，在可能传播的频谱范围将无线信号衰减到不能有效接收的程度，避免邻近攻击。	测评单元（L4-NCS5-10） 应核查无线通信的用户在登录时是否采用了身份鉴别措施；应核查无线通信的用户列表，核查用户身份标识是否具有唯一性。 测评单元（L4-NCS5-11） 应核查无线通信过程中是否对用户进行授权，核查具体权限是否合理；核查未授权的使用是否可以被发现及告警。 测评单元（L4-NCS5-12） 应核查无线通信传输中是否采用加密措施保证传输报文的机密性。 测评单元（L4-NCS5-13） 应核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备应及时发出告警并可以对试图接入的无线设备进行屏蔽。
8.3.4 安全管理中心设计技术要求	8.3.4.1 系统管理	安全管理中心系统具有自身运行监控与告警、系统日志记录等功能。	测评单元（L4-MMS5-05） 应访谈安全管理员是否建立跨单位处置工业控制系统安全事件流程；应核查跨单位安全事件报告和处置管理制度，核查是否含有工业控制系统联合防护和应急的相关内容。 测评单元（L4-NCS5-13） 应核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备应及时

			发出告警并可以对试图接入的无线设备进行屏蔽。
8.3.4.2 安全管理	在进行工业控制系统安全设计时，安全管理还应符合以下要求： a) 通过安全管理员能够对工业控制系统设备的可用性和安全性进行实时监控，可以对监控指标设置告警阈值，触发告警并记录； b) 通过安全管理员能够在安全管理中心呈现工业控制系统设备间的访问关系，形成基于网络访问关系、业务操作指令的工业控制环境的行为白名单，协助管理员及时发现未定义的信息通讯行为以及识别重要业务操作指令级的异常。 c) 通过安全管理员能够结合工业控制系统设备的资产信息、威胁信息、脆弱性信息分析工业控制设备以及工业控制系统面临的安全风险和安全态势。	测评单元（L4-MMS5-05） 应访谈安全管理员是否建立跨单位处置工业控制系统安全事件流程；应核查跨单位安全事件报告和处置管理制度，核查是否含有工业控制系统联合防护和应急的相关内容。 测评单元（L4-NCS5-13） 应核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备应及时发出告警并可以对试图接入的无线设备进行屏蔽。	
8.3.4.3 审计管理	在进行工业控制系统安全设计时，审计管理还应符合以下要求：通过安全管理员能够对工业控制现场控制设备、信息安全设备、网络设备、服务器、操作站等设备中主体和客体进行登记，并对各设备的信息安全监控和报警、信息安全日志信息进行集中管理。根据安全审计策略对各类信息安全信息进行分类管理与查询，并生成统一的审计报告。系统对各类信息安全报警和日志信息进行关联分析。系统通过各设备信息安全日志信息的关联分析提取出少量的、或者是概括性的重要安全事件或发掘隐藏的攻击规律，进行重点报警和分析，并对全局存在类似风险的系统进行安全预警。	测评单元（L4-MMS5-05） 应访谈安全管理员是否建立跨单位处置工业控制系统安全事件流程；应核查跨单位安全事件报告和处置管理制度，核查是否含有工业控制系统联合防护和应急的相关内容。 测评单元（L4-NCS5-13） 应核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备；监测设备应及时发出告警并可以对试图接入的无线设备进行屏蔽。	

附 录 D
(资料性附录)
测评要求和基本要求对应表

为便于测评实施人员进行快速查询本标准条款与《信息安全技术 网络安全等级保护基本要求》条款的对应关系，本附录进行索引对应。针对大数据等级保护对象的测评实施将另行制定。

D.1 安全测评通用要求和基本要求对应表

D.1.1 第一级

层面	控制点	测评单元编号	基本要求编号
6.1.1 物理和环境安全	6.1.1.1 物理访问控制	L1-PES1-01	6.1.1.1
	6.1.1.2 防盗窃和防破坏	L1-PES1-02	6.1.1.2
	6.1.1.3 防雷击	L1-PES1-03	6.1.1.3
	6.1.1.4 防火	L1-PES1-04	6.1.1.4
	6.1.1.5 防水和防潮	L1-PES1-05	6.1.1.5
	6.1.1.6 温湿度控制	L1-PES1-06	6.1.1.6
	6.1.1.7 电力供应	L1-PES1-07	6.1.1.7
6.1.2 网络和通信安全	6.1.2.1 网络架构	L1-NCS1-01	6.1.2.1 a)
		L1-NCS1-02	6.1.2.1 b)
	6.1.2.2 通信传输	L1-NCS1-03	6.1.2.2
	6.1.2.3 边界防护	L1-NCS1-04	6.1.2.3
	6.1.2.4 访问控制	L1-NCS1-05	6.1.2.4 a)
		L1-NCS1-06	6.1.2.4 b)
		L1-NCS1-07	6.1.2.4 c)
6.1.3 设备和计算安全	6.1.3.1 身份鉴别	L1-ECS1-01	6.1.3.1 a)
		L1-ECS1-02	6.1.3.1 b)
	6.1.3.2 访问控制	L1-ECS1-03	6.1.3.2 a)
		L1-ECS1-04	6.1.3.2 b)
		L1-ECS1-05	6.1.3.2 c)
	6.1.3.3 入侵防范	L1-ECS1-06	6.1.3.3 a)
		L1-ECS1-07	6.1.3.3 b)
	6.1.3.4 恶意代码防范	L1-ECS1-08	6.1.3.4
6.1.4 应用和数据安全	6.1.4.1 身份鉴别	L1-ADS1-01	6.1.4.1 a)
		L1-ADS1-02	6.1.4.1 b)
	6.1.4.2 访问控制	L1-ADS1-03	6.1.4.2 a)
		L1-ADS1-04	6.1.4.2 b)
		L1-ADS1-05	6.1.4.2 c)
	6.1.4.3 软件容错	L1-ADS1-06	6.1.4.3

	6.1.4.4 数据完整性	L1-ADS1-07	6.1.4.4
	6.1.4.5 数据备份恢复	L1-ADS1-08	6.1.4.5
6.1.5 安全策略和管理制度	6.1.5.1 管理制度	L1-PSS1-01	6.1.5.1
6.1.6 安全管理机构和人员	6.1.6.1 岗位设置	L1-ORS1-01	6.1.6.1
	6.1.6.2 人员配备	L1-ORS1-02	6.1.6.2
	6.1.6.3 授权和审批	L1-ORS1-03	6.1.6.3
	6.1.6.4 人员录用	L1-ORS1-04	6.1.6.4
	6.1.6.5 人员离岗	L1-ORS1-05	6.1.6.5
	6.1.6.6 安全意识教育和培训	L1-ORS1-06	6.1.6.6
	6.1.6.7 外部人员访问管理	L1-ORS1-07	6.1.6.7
6.1.7 安全建设管理	6.1.7.1 定级	L1-CMS1-01	6.1.7.1
	6.1.7.2 安全方案设计	L1-CMS1-02	6.1.7.2
	6.1.7.3 产品采购和使用	L1-CMS1-03	6.1.7.3
	6.1.7.4 工程实施	L1-CMS1-04	6.1.7.4
	6.1.7.5 测试验收	L1-CMS1-05	6.1.7.5
	6.1.7.6 系统交付	L1-CMS1-06	6.1.7.6 a)
		L1-CMS1-07	6.1.7.6 b)
	6.1.7.7 服务供应商管理	L1-CMS1-08	6.1.7.7 a)
		L1-CMS1-09	6.1.7.7 b)
6.1.8 安全运维管理	6.1.8.1 环境管理	L1-MMS1-01	6.1.8.1 a)
		L1-MMS1-02	6.1.8.1 b)
	6.1.8.2 介质管理	L1-MMS1-03	6.1.8.2
	6.1.8.3 设备维护管理	L1-MMS1-04	6.1.8.3
	6.1.8.4 漏洞和风险管理	L1-MMS1-05	6.1.8.4
		L1-MMS1-06	6.1.8.5 a)
	6.1.8.5 网络和系统安全管理	L1-MMS1-07	6.1.8.5 b)
		L1-MMS1-08	6.1.8.6 a)
	6.1.8.6 恶意代码防范管理	L1-MMS1-09	6.1.8.6 b)
		L1-MMS1-10	6.1.8.7 a)
	6.1.8.7 备份与恢复管理	L1-MMS1-11	6.1.8.7 b)
		L1-MMS1-12	6.1.8.8 a)
	6.1.8.8 安全事件处置	L1-MMS1-13	6.1.8.8 b)

D.1.2 第二级

层面	控制点	测评单元编号	基本要求编号
7.1.1 物理和环境安全	7.1.1.1 物理位置选择	L2-PES1-01	7.1.1.1 a)
		L2-PES1-02	7.1.1.1 b)
	7.1.1.2 物理访问控制	L2-PES1-03	7.1.1.2 a)
	7.1.1.3 防盗窃和防破坏	L2-PES1-04	7.1.1.3 a)

		L2-PES1-05	7.1.1.3 b)
	7.1.1.4 防雷击	L2-PES1-06	7.1.1.4
	7.1.1.5 防火	L2-PES1-07	7.1.1.5 a)
		L2-PES1-08	7.1.1.5 b)
	7.1.1.6 防水和防潮	L2-PES1-09	7.1.1.6 a)
		L2-PES1-10	7.1.1.6 b)
	7.1.1.7 防静电	L2-PES1-11	7.1.1.7
	7.1.1.8 温湿度控制	L2-PES1-12	7.1.1.8
	7.1.1.9 电力供应	L2-PES1-13	7.1.1.9 a)
		L2-PES1-14	7.1.1.9 b)
	7.1.1.10 电磁防护	L2-PES1-15	7.1.1.10
7.1.2 网络和通信安全	7.1.2.1 网络架构	L2-NCS1-01	7.1.2.1 a)
		L2-NCS1-02	7.1.2.1 b)
		L2-NCS1-03	7.1.2.1 c)
		L2-NCS1-04	7.1.2.1 d)
	7.1.2.2 通信传输	L2-NCS1-05	7.1.2.2
	7.1.2.3 边界防护	L2-NCS1-06	7.1.2.3
	7.1.2.4 访问控制	L2-NCS1-07	7.1.2.4 a)
		L2-NCS1-08	7.1.2.4 b)
		L2-NCS1-09	7.1.2.4 c)
		L2-NCS1-10	7.1.2.4 d)
	7.1.2.5 入侵防范	L2-NCS1-11	7.1.2.5
	7.1.2.6 安全审计	L2-NCS1-12	7.1.2.6 a)
		L2-NCS1-13	7.1.2.6 b)
		L2-NCS1-14	7.1.2.6 c)
		L2-NCS1-15	7.1.2.6 d)
7.1.3 设备和计算安全	7.1.3.1 身份鉴别	L2-ECS1-01	7.1.3.1 a)
		L2-ECS1-02	7.1.3.1 b)
		L2-ECS1-03	7.1.3.1 c)
	7.1.3.2 访问控制	L2-ECS1-04	7.1.3.2 a)
		L2-ECS1-05	7.1.3.2 b)
		L2-ECS1-06	7.1.3.2 c)
		L2-ECS1-07	7.1.3.2 d)
	7.1.3.3 安全审计	L2-ECS1-08	7.1.3.3 a)
		L2-ECS1-09	7.1.3.3 b)
		L2-ECS1-10	7.1.3.3 c)
		L2-ECS1-11	7.1.3.3 d)
	7.1.3.4 入侵防范	L2-ECS1-12	7.1.3.4 a)
		L2-ECS1-13	7.1.3.4 b)
		L2-ECS1-14	7.1.3.4 c)
		L2-ECS1-15	7.1.3.4 d)

	7.1.3.5 恶意代码防范	L2-ECS1-16	7.1.3.5
	7.1.3.6 资源控制	L2-ECS1-17	7.1.3.6
7.1.4 应用和数据安全	7.1.4.1 身份鉴别	L2-ADS1-01	7.1.4.1 a)
		L2-ADS1-02	7.1.4.1 b)
		L2-ADS1-03	7.1.4.1 c)
		L2-ADS1-04	7.1.4.1 d)
	7.1.4.2 访问控制	L2-ADS1-05	7.1.4.2 a)
		L2-ADS1-06	7.1.4.2 b)
		L2-ADS1-07	7.1.4.2 c)
	7.1.4.3 安全审计	L2-ADS1-08	7.1.4.3 a)
		L2-ADS1-09	7.1.4.3 b)
		L2-ADS1-10	7.1.4.3 c)
		L2-ADS1-11	7.1.4.3 d)
	7.1.4.4 软件容错	L2-ADS1-12	7.1.4.4 a)
		L2-ADS1-13	7.1.4.4 b)
	7.1.4.5 资源控制	L2-ADS1-14	7.1.4.5 a)
		L2-ADS1-15	7.1.4.5 b)
		L2-ADS1-16	7.1.4.5 c)
	7.1.4.6 数据完整性	L2-ADS1-17	7.1.4.6
	7.1.4.7 数据备份恢复	L2-ADS1-18	7.1.4.7 a)
		L2-ADS1-19	7.1.4.7 b)
	7.1.4.8 剩余信息保护	L2-ADS1-20	7.1.4.8
	7.1.4.9 个人信息保护	L2-ADS1-21	7.1.4.9 a)
		L2-ADS1-22	7.1.4.9 b)
7.1.5 安全策略和管理制度	7.1.5.1 安全策略	L2-PSS1-01	7.1.5.1
	7.1.5.2 管理制度	L2-PSS1-02	7.1.5.2 a)
		L2-PSS1-03	7.1.5.2 b)
	7.1.5.3 制定和发布	L2-PSS1-04	7.1.5.3 a)
		L2-PSS1-05	7.1.5.3 b)
	7.1.5.4 评审和修订	L2-PSS1-06	7.1.5.4
7.1.6 安全管理机构和人员	7.1.6.1 岗位设置	L2-ORS1-01	7.1.6.1 a)
		L2-ORS1-02	7.1.6.1 b)
	7.1.6.2 人员配备	L2-ORS1-03	7.1.6.2
	7.1.6.3 授权和审批	L2-ORS1-04	7.1.6.3 a)
		L2-ORS1-05	7.1.6.3 b)
	7.1.6.4 沟通和合作	L2-ORS1-06	7.1.6.4 a)
		L2-ORS1-07	7.1.6.4 b)
		L2-ORS1-08	7.1.6.4 c)
	7.1.6.5 审核和检查	L2-ORS1-09	7.1.6.5
	7.1.6.6 人员录用	L2-ORS1-10	7.1.6.6 a)
		L2-ORS1-11	7.1.6.6 b)

	7.1.6.7 人员离岗	L2-ORS1-12	7.1.6.7
	7.1.6.8 安全意识教育和培训	L2-ORS1-13	7.1.6.8
	7.1.6.9 外部人员访问管理	L2-ORS1-14	7.1.6.9 a)
		L2-ORS1-15	7.1.6.9 b)
		L2-ORS1-16	7.1.6.9 c)
7.1.7 安全建设管理	7.1.7.1 定级和备案	L2-CMS1-01	7.1.7.1 a)
		L2-CMS1-02	7.1.7.1 b)
		L2-CMS1-03	7.1.7.1 c)
		L2-CMS1-04	7.1.7.1 d)
	7.1.7.2 安全方案设计	L2-CMS1-05	7.1.7.2 a)
		L2-CMS1-06	7.1.7.2 b)
		L2-CMS1-07	7.1.7.2 c)
	7.1.7.3 产品采购和使用	L2-CMS1-08	7.1.7.3 a)
		L2-CMS1-09	7.1.7.3 b)
	7.1.7.4 自行软件开发	L2-CMS1-10	7.1.7.4 a)
		L2-CMS1-11	7.1.7.4 b)
	7.1.7.5 外包软件开发	L2-CMS1-12	7.1.7.5 a)
		L2-CMS1-13	7.1.7.5 b)
	7.1.7.6 工程实施	L2-CMS1-14	7.1.7.6 a)
		L2-CMS1-15	7.1.7.6 b)
	7.1.7.7 测试验收	L2-CMS1-16	7.1.7.7 a)
		L2-CMS1-17	7.1.7.7 b)
	7.1.7.8 系统交付	L2-CMS1-18	7.1.7.8 a)
		L2-CMS1-19	7.1.7.8 b)
		L2-CMS1-20	7.1.7.8 c)
	7.1.7.9 等级测评	L2-CMS1-21	7.1.7.9 a)
		L2-CMS1-22	7.1.7.9 b)
		L2-CMS1-23	7.1.7.9 c)
	7.1.7.10 服务供应商管理	L2-CMS1-24	7.1.7.10 a)
		L2-CMS1-25	7.1.7.10 b)
7.1.8 安全运维管理	7.1.8.1 环境管理	L2-MMS1-01	7.1.8.1 a)
		L2-MMS1-02	7.1.8.1 b)
		L2-MMS1-03	7.1.8.1 c)
	7.1.8.2 资产管理	L2-MMS1-04	7.1.8.2
	7.1.8.3 介质管理	L2-MMS1-05	7.1.8.3 a)
		L2-MMS1-06	7.1.8.3 b)
	7.1.8.4 设备维护管理	L2-MMS1-07	7.1.8.4 a)
		L2-MMS1-08	7.1.8.4 b)
	7.1.8.5 漏洞和风险管理	L2-MMS1-09	7.1.8.5
	7.1.8.6 网络与系统安全管理	L2-MMS1-10	7.1.8.6 a)
		L2-MMS1-11	7.1.8.6 b)

		L2-MMS1-12	7.1.8.6 c)
		L2-MMS1-13	7.1.8.6 d)
		L2-MMS1-14	7.1.8.6 e)
	7.1.8.7 恶意代码防范管理	L2-MMS1-15	7.1.8.7 a)
		L2-MMS1-16	7.1.8.7 b)
		L2-MMS1-17	7.1.8.7 c)
	7.1.8.8 配置管理	L2-MMS1-18	7.1.8.8
	7.1.8.9 密码管理	L2-MMS1-19	7.1.8.9
	7.1.8.10 变更管理	L2-MMS1-20	7.1.8.10
	7.1.8.11 备份与恢复管理	L2-MMS1-21	7.1.8.11 a)
		L2-MMS1-22	7.1.8.11 b)
		L2-MMS1-23	7.1.8.11 c)
	7.1.8.12 安全事件处置	L2-MMS1-24	7.1.8.12 a)
		L2-MMS1-25	7.1.8.12 b)
		L2-MMS1-26	7.1.8.12 c)
	7.1.8.13 应急预案管理	L2-MMS1-27	7.1.8.13 a)
		L2-MMS1-28	7.1.8.13 b)
	7.1.8.14 外包运维管理	L2-MMS1-29	7.1.8.14 a)
		L2-MMS1-30	7.1.8.14 b)

D.1.3 第三级

层面	控制点	测评单元编号	基本要求编号
8.1.1 物理和环境安全	8.1.1.1 物理位置选择	L3-PES1-01	8.1.1.1 a)
		L3-PES1-02	8.1.1.1 b)
	8.1.1.2 物理访问控制	L3-PES1-03	8.1.1.2
	8.1.1.3 防盗窃和防破坏	L3-PES1-04	8.1.1.3 a)
		L3-PES1-05	8.1.1.3 b)
		L3-PES1-06	8.1.1.3 c)
	8.1.1.4 防雷击	L3-PES1-07	8.1.1.4 a)
		L3-PES1-08	8.1.1.4 b)
	8.1.1.5 防火	L3-PES1-09	8.1.1.5 a)
		L3-PES1-10	8.1.1.5 b)
		L3-PES1-11	8.1.1.5 c)
	8.1.1.6 防水和防潮	L3-PES1-12	8.1.1.6 a)
		L3-PES1-13	8.1.1.6 b)
		L3-PES1-14	8.1.1.6 c)
	8.1.1.7 防静电	L3-PES1-15	8.1.1.7 a)
		L3-PES1-16	8.1.1.7 b)
	8.1.1.8 温湿度控制	L3-PES1-17	8.1.1.8
	8.1.1.9 电力供应	L3-PES1-18	8.1.1.9 a)

		L3-PES1-19	8.1.1.9 b)
		L3-PES1-20	8.1.1.9 c)
	8.1.1.10 电磁防护	L3-PES1-21	8.1.1.10 a)
		L3-PES1-22	8.1.1.10 b)
8.1.2 网络和通信安全	8.1.2.1 网络架构	L3-NCS1-01	8.1.2.1 a)
		L3-NCS1-02	8.1.2.1 b)
		L3-NCS1-03	8.1.2.1 c)
		L3-NCS1-04	8.1.2.1 d)
		L3-NCS1-05	8.1.2.1 e)
	8.1.2.2 通信传输	L3-NCS1-06	8.1.2.2 a)
		L3-NCS1-07	8.1.2.2 b)
	8.1.2.3 边界防护	L3-NCS1-08	8.1.2.3 a)
		L3-NCS1-09	8.1.2.3 b)
		L3-NCS1-10	8.1.2.3 c)
		L3-NCS1-11	8.1.2.3 d)
	8.1.2.4 访问控制	L3-NCS1-12	8.1.2.4 a)
		L3-NCS1-13	8.1.2.4 b)
		L3-NCS1-14	8.1.2.4 c)
		L3-NCS1-15	8.1.2.4 d)
		L3-NCS1-16	8.1.2.4 e)
	8.1.2.5 入侵防范	L3-NCS1-17	8.1.2.5 a)
		L3-NCS1-18	8.1.2.5 b)
		L3-NCS1-19	8.1.2.5 c)
		L3-NCS1-20	8.1.2.5 d)
	8.1.2.6 恶意代码防范	L3-NCS1-21	8.1.2.6 a)
		L3-NCS1-22	8.1.2.6 b)
	8.1.2.7 安全审计	L3-NCS1-23	8.1.2.7 a)
		L3-NCS1-24	8.1.2.7 b)
		L3-NCS1-25	8.1.2.7 c)
		L3-NCS1-26	8.1.2.7 d)
		L3-NCS1-27	8.1.2.7 e)
	8.1.2.8 集中管控	L3-NCS1-28	8.1.2.8 a)
		L3-NCS1-29	8.1.2.8 b)
		L3-NCS1-30	8.1.2.8 c)
		L3-NCS1-31	8.1.2.8 d)
		L3-NCS1-32	8.1.2.8 e)
		L3-NCS1-33	8.1.2.8 f)
8.1.3 设备和计算安全	8.1.3.1 身份鉴别	L3-ECS1-01	8.1.3.1 a)
		L3-ECS1-02	8.1.3.1 b)
		L3-ECS1-03	8.1.3.1 c)
		L3-ECS1-04	8.1.3.1 d)

8.1.4 应用和数据安全	8.1.3.2 访问控制	L3-ECS1-05	8.1.3.2 a)
		L3-ECS1-06	8.1.3.2 b)
		L3-ECS1-07	8.1.3.2 c)
		L3-ECS1-08	8.1.3.2 d)
		L3-ECS1-09	8.1.3.2 e)
		L3-ECS1-10	8.1.3.2 f)
		L3-ECS1-11	8.1.3.2 g)
	8.1.3.3 安全审计	L3-ECS1-12	8.1.3.3 a)
		L3-ECS1-13	8.1.3.3 b)
		L3-ECS1-14	8.1.3.3 c)
		L3-ECS1-15	8.1.3.3 d)
		L3-ECS1-16	8.1.3.3 e)
	8.1.3.4 入侵防范	L3-ECS1-17	8.1.3.4 a)
		L3-ECS1-18	8.1.3.4 b)
		L3-ECS1-19	8.1.3.4 c)
		L3-ECS1-20	8.1.3.4 d)
		L3-ECS1-21	8.1.3.4 e)
	8.1.3.5 恶意代码防范	L3-ECS1-22	8.1.3.5
	8.1.3.6 资源控制	L3-ECS1-23	8.1.3.6 a)
		L3-ECS1-24	8.1.3.6 b)
		L3-ECS1-25	8.1.3.6 c)
		L3-ECS1-26	8.1.3.6 d)
	8.1.4.1 身份鉴别	L3-ADS1-01	8.1.4.1 a)
		L3-ADS1-02	8.1.4.1 b)
		L3-ADS1-03	8.1.4.1 c)
		L3-ADS1-04	8.1.4.1 d)
		L3-ADS1-05	8.1.4.1 e)
	8.1.4.2 访问控制	L3-ADS1-06	8.1.4.2 a)
		L3-ADS1-07	8.1.4.2 b)
		L3-ADS1-08	8.1.4.2 c)
		L3-ADS1-09	8.1.4.2 d)
		L3-ADS1-10	8.1.4.2 e)
		L3-ADS1-11	8.1.4.2 f)
		L3-ADS1-12	8.1.4.2 g)
	8.1.4.3 安全审计	L3-ADS1-13	8.1.4.3 a)
		L3-ADS1-14	8.1.4.3 b)
		L3-ADS1-15	8.1.4.3 c)
		L3-ADS1-16	8.1.4.3 d)
		L3-ADS1-17	8.1.4.3 e)
	8.1.4.4 软件容错	L3-ADS1-18	8.1.4.4 a)
		L3-ADS1-19	8.1.4.4 b)

		L3-ADS1-20	8.1.4.4 c)
	8.1.4.5 资源控制	L3-ADS1-21	8.1.4.5 a)
		L3-ADS1-22	8.1.4.5 b)
		L3-ADS1-23	8.1.4.5 c)
	8.1.4.6 数据完整性	L3-ADS1-24	8.1.4.6 a)
		L3-ADS1-25	8.1.4.6 b)
	8.1.4.7 数据保密性	L3-ADS1-26	8.1.4.7 a)
		L3-ADS1-27	8.1.4.7 b)
	8.1.4.8 数据备份恢复	L3-ADS1-28	8.1.4.8 a)
		L3-ADS1-29	8.1.4.8 b)
		L3-ADS1-30	8.1.4.8 c)
	8.1.4.9 剩余信息保护	L3-ADS1-31	8.1.4.9 a)
		L3-ADS1-32	8.1.4.9 b)
	8.1.4.10 个人信息保护	L3-ADS1-33	8.1.4.10 a)
L3-ADS1-34		8.1.4.10 b)	
8.1.5 安全策略和管理制度	8.1.5.1 安全策略	L3-PSS1-01	8.1.5.1
	8.1.5.2 管理制度	L3-PSS1-02	8.1.5.2 a)
		L3-PSS1-03	8.1.5.2 b)
		L3-PSS1-04	8.1.5.2 c)
	8.1.5.3 制定和发布	L3-PSS1-05	8.2.1.3 a)
		L3-PSS1-06	8.2.1.3 b)
8.1.5.4 评审和修订	L3-PSS1-07	8.2.1.4	
8.1.6 安全管理机构和人员	8.1.6.1 岗位设置	L3-ORS1-01	8.1.6.1 a)
		L3-ORS1-02	8.1.6.1 b)
		L3-ORS1-03	8.1.6.1 c)
	8.1.6.2 人员配备	L3-ORS1-04	8.1.6.2 a)
		L3-ORS1-05	8.1.6.2 b)
	8.1.6.3 授权和审批	L3-ORS1-06	8.1.6.3 a)
		L3-ORS1-07	8.1.6.3 b)
		L3-ORS1-08	8.1.6.3 c)
	8.1.6.4 沟通和合作	L3-ORS1-09	8.1.6.4 a)
		L3-ORS1-10	8.1.6.4 b)
		L3-ORS1-11	8.1.6.4 c)
	8.1.6.5 审核和核查	L3-ORS1-12	8.1.6.5 a)
		L3-ORS1-13	8.1.6.5 b)
		L3-ORS1-14	8.1.6.5 c)
	8.1.6.6 人员录用	L3-ORS1-15	8.1.6.6 a)
		L3-ORS1-16	8.1.6.6 b)
		L3-ORS1-17	8.1.6.6 c)
	8.1.6.7 人员离岗	L3-ORS1-18	8.1.6.7 a)
		L3-ORS1-19	8.1.6.7 b)

8.1.7 安全建设管理	8.1.6.8 安全意识教育和培训	L3-ORS1-20	8.1.6.8 a)
		L3-ORS1-21	8.1.6.8 b)
		L3-ORS1-22	8.1.6.8 c)
	8.1.6.9 外部人员访问管理	L3-ORS1-23	8.1.6.9 a)
		L3-ORS1-24	8.1.6.9 b)
		L3-ORS1-25	8.1.6.9 c)
		L3-ORS1-26	8.1.6.9 d)
	8.1.7.1 定级和备案	L3-CMS1-01	8.1.7.1 a)
		L3-CMS1-02	8.1.7.1 b)
		L3-CMS1-03	8.1.7.1 c)
		L3-CMS1-04	8.1.7.1 d)
	8.1.7.2 安全方案设计	L3-CMS1-05	8.1.7.2 a)
		L3-CMS1-06	8.1.7.2 b)
		L3-CMS1-07	8.1.7.2 c)
	8.1.7.3 产品采购和使用	L3-CMS1-08	8.1.7.3 a)
		L3-CMS1-09	8.1.7.3 b)
		L3-CMS1-10	8.1.7.3 c)
	8.1.7.4 自行软件开发	L3-CMS1-11	8.1.7.4 a)
		L3-CMS1-12	8.1.7.4 b)
		L3-CMS1-13	8.1.7.4 c)
		L3-CMS1-14	8.1.7.4 d)
		L3-CMS1-15	8.1.7.4 e)
		L3-CMS1-16	8.1.7.4 f)
		L3-CMS1-17	8.1.7.4 g)
	8.1.7.5 外包软件开发	L3-CMS1-18	8.1.7.5 a)
		L3-CMS1-19	8.1.7.5 b)
		L3-CMS1-20	8.1.7.5 c)
	8.1.7.6 工程实施	L3-CMS1-21	8.1.7.6 a)
		L3-CMS1-22	8.1.7.6 b)
		L3-CMS1-23	8.1.7.6 c)
	8.1.7.7 测试验收	L3-CMS1-24	8.1.7.7 a)
		L3-CMS1-25	8.1.7.7 b)
	8.1.7.8 系统交付	L3-CMS1-26	8.1.7.8 a)
		L3-CMS1-27	8.1.7.8 b)
		L3-CMS1-28	8.1.7.8 c)
	8.1.7.9 等级测评	L3-CMS1-29	8.1.7.9 a)
		L3-CMS1-30	8.1.7.9 b)
		L3-CMS1-31	8.1.7.9 c)
	8.1.7.10 服务供应商管理	L3-CMS1-32	8.1.7.10 a)
		L3-CMS1-33	8.1.7.10 b)
		L3-CMS1-34	8.1.7.10 c)

8.1.8 安全运维管理	8.1.8.1 环境管理	L3-MMS1-01	8.1.8.1 a)
		L3-MMS1-02	8.1.8.1 b)
		L3-MMS1-03	8.1.8.1 c)
	8.1.8.2 资产管理	L3-MMS1-04	8.1.8.2 a)
		L3-MMS1-05	8.1.8.2 b)
		L3-MMS1-06	8.1.8.2 c)
	8.1.8.3 介质管理	L3-MMS1-07	8.1.8.3 a)
		L3-MMS1-08	8.1.8.3 b)
	8.1.8.4 设备维护管理	L3-MMS1-09	8.1.8.4 a)
		L3-MMS1-10	8.1.8.4 b)
		L3-MMS1-11	8.1.8.4 c)
		L3-MMS1-12	8.1.8.4 d)
	8.1.8.5 漏洞和风险管理	L3-MMS1-13	8.1.8.5 a)
		L3-MMS1-14	8.1.8.5 b)
	8.1.8.6 网络和系统安全管理	L3-MMS1-15	8.1.8.6 a)
		L3-MMS1-16	8.1.8.6 b)
		L3-MMS1-17	8.1.8.6 c)
		L3-MMS1-18	8.1.8.6 d)
		L3-MMS1-19	8.1.8.6 e)
		L3-MMS1-20	8.1.8.6 f)
		L3-MMS1-21	8.1.8.6 g)
		L3-MMS1-22	8.1.8.6 h)
		L3-MMS1-23	8.1.8.6 i)
		L3-MMS1-24	8.1.8.6 j)
	8.1.8.7 恶意代码防范管理	L3-MMS1-25	8.1.8.7 a)
		L3-MMS1-26	8.1.8.7 b)
		L3-MMS1-27	8.1.8.7 c)
	8.1.8.8 配置管理	L3-MMS1-28	8.1.8.8 a)
		L3-MMS1-29	8.1.8.8 b)
	8.1.8.9 密码管理	L3-MMS1-30	8.1.8.9
	8.1.8.10 变更管理	L3-MMS1-31	8.1.8.10 a)
		L3-MMS1-32	8.1.8.10 b)
		L3-MMS1-33	8.1.8.10 c)
	8.1.8.11 备份与恢复管理	L3-MMS1-34	8.1.8.11 a)
		L3-MMS1-35	8.1.8.11 b)
		L3-MMS1-36	8.1.8.11 c)
	8.1.8.12 安全事件处置	L3-MMS1-37	8.1.8.12 a)
		L3-MMS1-38	8.1.8.12 b)
		L3-MMS1-39	8.1.8.12 c)
		L3-MMS1-40	8.1.8.12 d)
	8.1.8.13 安全预案管理	L3-MMS1-41	8.1.8.13 a)

		L3-MMS1-42	8.1.8.13 b)
		L3-MMS1-43	8.1.8.13 c)
		L3-MMS1-44	8.1.8.13 d)
	8.1.8.14 外部运维管理	L3-MMS1-45	8.1.8.14 a)
		L3-MMS1-46	8.1.8.14 b)
		L3-MMS1-47	8.1.8.14 c)
		L3-MMS1-48	8.1.8.14 d)

D.1.4 第四级

层面	控制点	测评单元编号	基本要求编号
9.1.1 物理和环境安全	9.1.1.1 物理位置选择	L4-PES1-01	9.1.1.1 a)
		L4-PES1-02	9.1.1.1 b)
	9.1.1.2 物理访问控制	L4-PES1-03	9.1.1.2 a)
		L4-PES1-04	9.1.1.2 b)
	9.1.1.3 防盗窃和防破坏	L4-PES1-05	9.1.1.3 a)
		L4-PES1-06	9.1.1.3 b)
		L4-PES1-07	9.1.1.3 c)
	9.1.1.4 防雷击	L4-PES1-08	9.1.1.4 a)
		L4-PES1-09	9.1.1.4 b)
	9.1.1.5 防火	L4-PES1-10	9.1.1.5 a)
		L4-PES1-11	9.1.1.5 b)
		L4-PES1-12	9.1.1.5 c)
	9.1.1.6 防水和防潮	L4-PES1-13	9.1.1.6 a)
		L4-PES1-14	9.1.1.6 b)
		L4-PES1-15	9.1.1.6 c)
	9.1.1.7 防静电	L4-PES1-16	9.1.1.7 a)
		L4-PES1-17	9.1.1.7 b)
	9.1.1.8 温湿度控制	L4-PES1-18	9.1.1.8
	9.1.1.9 电力供应	L4-PES1-19	9.1.1.9 a)
		L4-PES1-20	9.1.1.9 b)
		L4-PES1-21	9.1.1.9 c)
		L4-PES1-22	9.1.1.9 d)
	9.1.1.10 电磁防护	L4-PES1-23	9.1.1.10 a)
		L4-PES1-24	9.1.1.10 b)
9.1.2 网络和通信安全	9.1.2.1 网络架构	L4-NCS1-01	9.1.2.1 a)
		L4-NCS1-02	9.1.2.1 b)
		L4-NCS1-03	9.1.2.1 c)
		L4-NCS1-04	9.1.2.1 d)
		L4-NCS1-05	9.1.2.1 e)
		L4-NCS1-06	9.1.2.1 f)

	9.1.2.2 通信传输	L4-NCS1-07	9.1.2.2 a)
		L4-NCS1-08	9.1.2.2 b)
		L4-NCS1-09	9.1.2.2 c)
		L4-NCS1-10	9.1.2.2 d)
	9.1.2.3 边界防护	L4-NCS1-11	9.1.2.3 a)
		L4-NCS1-12	9.1.2.3 b)
		L4-NCS1-13	9.1.2.3 c)
		L4-NCS1-14	9.1.2.3 d)
		L4-NCS1-15	9.1.2.3 e)
	9.1.2.4 访问控制	L4-NCS1-16	9.1.2.4 a)
		L4-NCS1-17	9.1.2.4 b)
		L4-NCS1-18	9.1.2.4 c)
	9.1.2.5 入侵防范	L4-NCS1-19	9.1.2.5 a)
		L4-NCS1-20	9.1.2.5 b)
		L4-NCS1-21	9.1.2.5 c)
		L4-NCS1-22	9.1.2.5 d)
	9.1.2.6 恶意代码防范	L4-NCS1-23	9.1.2.6 a)
		L4-NCS1-24	9.1.2.6 b)
	9.1.2.7 安全审计	L4-NCS1-25	9.1.2.7 a)
		L4-NCS1-26	9.1.2.7 b)
		L4-NCS1-27	9.1.2.7 c)
		L4-NCS1-28	9.1.2.7 d)
		L4-NCS1-29	9.1.2.7 e)
	9.1.2.8 集中管控	L4-NCS1-30	9.1.2.8 a)
		L4-NCS1-31	9.1.2.8 b)
		L4-NCS1-32	9.1.2.8 c)
		L4-NCS1-33	9.1.2.8 d)
		L4-NCS1-34	9.1.2.8 e)
		L4-NCS1-35	9.1.2.8 f)
9.1.3 设备和计算安全	9.1.3.1 身份鉴别	L4-ECS1-01	9.1.3.1 a)
		L4-ECS1-02	9.1.3.1 b)
		L4-ECS1-03	9.1.3.1 c)
		L4-ECS1-04	9.1.3.1 d)
	9.1.3.2 访问控制	L4-ECS1-05	9.1.3.2 a)
		L4-ECS1-06	9.1.3.2 b)
		L4-ECS1-07	9.1.3.2 c)
		L4-ECS1-08	9.1.3.2 d)
		L4-ECS1-09	9.1.3.2 e)
		L4-ECS1-10	9.1.3.2 f)
		L4-ECS1-11	9.1.3.2 g)
	9.1.3.3 安全审计	L4-ECS1-12	9.1.3.3 a)

		L4-ECS1-13	9.1.3.3 b)
		L4-ECS1-14	9.1.3.3 c)
		L4-ECS1-15	9.1.3.3 d)
		L4-ECS1-16	9.1.3.3 e)
		L4-ECS1-17	9.1.3.3 f)
	9.1.3.4 入侵防范	L4-ECS1-18	9.1.3.4 a)
		L4-ECS1-19	9.1.3.4 b)
		L4-ECS1-20	9.1.3.4 c)
		L4-ECS1-21	9.1.3.4 d)
		L4-ECS1-22	9.1.3.4 e)
	9.1.3.5 恶意代码防范	L4-ECS1-23	9.1.3.5
	9.1.3.6 资源控制	L4-ECS1-24	9.1.3.6 a)
		L4-ECS1-25	9.1.3.6 b)
		L4-ECS1-26	9.1.3.6 c)
		L4-ECS1-27	9.1.3.6 d)
9.1.4 应用和数据安全	9.1.4.1 身份鉴别	L4-ADS1-01	9.1.4.1 a)
		L4-ADS1-02	9.1.4.1 b)
		L4-ADS1-03	9.1.4.1 c)
		L4-ADS1-04	9.1.4.1 d)
		L4-ADS1-05	9.1.4.1 e)
		L4-ADS1-06	9.1.4.1 f)
	9.1.4.2 访问控制	L4-ADS1-07	9.1.4.2 a)
		L4-ADS1-08	9.1.4.2 b)
		L4-ADS1-09	9.1.4.2 c)
		L4-ADS1-10	9.1.4.2 d)
		L4-ADS1-11	9.1.4.2 e)
		L4-ADS1-12	9.1.4.2 f)
		L4-ADS1-13	9.1.4.2 g)
	9.1.4.3 安全审计	L4-ADS1-14	9.1.4.3 a)
		L4-ADS1-15	9.1.4.3 b)
		L4-ADS1-16	9.1.4.3 c)
		L4-ADS1-17	9.1.4.3 d)
		L4-ADS1-18	9.1.4.3 e)
		L4-ADS1-19	9.1.4.3 f)
	9.1.4.4 软件容错	L4-ADS1-20	9.1.4.4 a)
		L4-ADS1-21	9.1.4.4 b)
		L4-ADS1-22	9.1.4.4 c)
	9.1.4.5 资源控制	L4-ADS1-23	9.1.4.5 a)
		L4-ADS1-24	9.1.4.5 b)
		L4-ADS1-25	9.1.4.5 c)
	9.1.4.6 数据完整性	L4-ADS1-26	9.1.4.6 a)

		L4-ADS1-27	9.1.4.6 b)
		L4-ADS1-28	9.1.4.6 c)
	9.1.4.7 数据保密性	L4-ADS1-29	9.1.4.7 a)
		L4-ADS1-30	9.1.4.7 b)
	9.1.4.8 数据备份恢复	L4-ADS1-31	9.1.4.8 a)
		L4-ADS1-32	9.1.4.8 b)
		L4-ADS1-33	9.1.4.8 c)
		L4-ADS1-34	9.1.4.8 d)
	9.1.4.9 剩余信息保护	L4-ADS1-35	9.1.4.9 a)
		L4-ADS1-36	9.1.4.9 b)
	9.1.4.10 个人信息保护	L4-ADS1-37	9.1.4.10 a)
		L4-ADS1-38	9.1.4.10 b)
9.1.5 安全策略和管理制度	9.1.5.1 安全策略	L4-PSS1-01	9.1.5.1
	9.1.5.2 管理制度	L4-PSS1-02	9.1.5.2 a)
		L4-PSS1-03	9.1.5.2 b)
		L4-PSS1-04	9.1.5.2 c)
	9.1.5.3 制定和发布	L4-PSS1-05	9.1.5.3 a)
		L4-PSS1-06	9.1.5.3 b)
	9.1.5.4 评审和修订	L4-PSS1-07	9.1.5.4
9.1.6 安全管理机构和人员	9.1.6.1 岗位设置	L4-ORS1-01	9.1.6.1 a)
		L4-ORS1-02	9.1.6.1 b)
		L4-ORS1-03	9.1.6.1 c)
	9.1.6.2 人员配备	L4-ORS1-04	9.1.6.2 a)
		L4-ORS1-05	9.1.6.2 b)
		L4-ORS1-06	9.1.6.2 c)
	9.1.6.3 授权和审批	L4-ORS1-07	9.1.6.3 a)
		L4-ORS1-08	9.1.6.3 b)
		L4-ORS1-09	9.1.6.3 c)
	9.1.6.4 沟通和合作	L4-ORS1-10	9.1.6.4 a)
		L4-ORS1-11	9.1.6.4 b)
		L4-ORS1-12	9.1.6.4 c)
	9.1.6.5 审核和检查	L4-ORS1-13	9.1.6.5 a)
		L4-ORS1-14	9.1.6.5 b)
		L4-ORS1-15	9.1.6.5 c)
	9.1.6.6 人员录用	L4-ORS1-16	9.1.6.6 a)
		L4-ORS1-17	9.1.6.6 b)
		L4-ORS1-18	9.1.6.6 c)
		L4-ORS1-19	9.1.6.6 d)
	9.1.6.7 人员离岗	L4-ORS1-20	9.1.6.7 a)
		L4-ORS1-21	9.1.6.7 b)
	9.1.6.8 安全意识教育和培训	L4-ORS1-22	9.1.6.8 a)

		L4-ORS1-23	9.1.6.8 b)
		L4-ORS1-24	9.1.6.8 c)
	9.1.6.9 外部人员访问管理	L4-ORS1-25	9.1.6.9 a)
		L4-ORS1-26	9.1.6.9 b)
		L4-ORS1-27	9.1.6.9 c)
		L4-ORS1-28	9.1.6.9 d)
		L4-ORS1-29	9.1.6.9 e)
9.1.7 安全建设管理	9.1.7.1 定级和备案	L4-CMS1-01	9.1.7.1 a)
		L4-CMS1-02	9.1.7.1 b)
		L4-CMS1-03	9.1.7.1 c)
		L4-CMS1-04	9.1.7.1 d)
	9.1.7.2 安全方案设计	L4-CMS1-05	9.1.7.2 a)
		L4-CMS1-06	9.1.7.2 b)
		L4-CMS1-07	9.1.7.2 c)
	9.1.7.3 产品采购和使用	L4-CMS1-08	9.1.7.3 a)
		L4-CMS1-09	9.1.7.3 b)
		L4-CMS1-10	9.1.7.3 c)
		L4-CMS1-11	9.1.7.3 d)
	9.1.7.4 自行软件开发	L4-CMS1-12	9.1.7.4 a)
		L4-CMS1-13	9.1.7.4 b)
		L4-CMS1-14	9.1.7.4 c)
		L4-CMS1-15	9.1.7.4 d)
		L4-CMS1-16	9.1.7.4 e)
		L4-CMS1-17	9.1.7.4 f)
		L4-CMS1-18	9.1.7.4 g)
	9.1.7.5 外包软件开发	L4-CMS1-19	9.1.7.5 a)
		L4-CMS1-20	9.1.7.5 b)
		L4-CMS1-21	9.1.7.5 c)
	9.1.7.6 工程实施	L4-CMS1-22	9.1.7.6 a)
		L4-CMS1-23	9.1.7.6 b)
		L4-CMS1-24	9.1.7.6 c)
	9.1.7.7 测试验收	L4-CMS1-25	9.1.7.7 a)
		L4-CMS1-26	9.1.7.7 b)
	9.1.7.8 系统交付	L4-CMS1-27	9.1.7.8 a)
		L4-CMS1-28	9.1.7.8 b)
		L4-CMS1-29	9.1.7.8 c)
	9.1.7.9 等级测评	L4-CMS1-30	9.1.7.9 a)
		L4-CMS1-31	9.1.7.9 b)
		L4-CMS1-32	9.1.7.9 c)
	9.1.7.10 服务供应商管理	L4-CMS1-33	9.1.7.10 a)
		L4-CMS1-34	9.1.7.10 b)

		L4-CMS1-35	9.1.7.10 c)
9.1.8 安全运维管理	9.1.8.1 环境管理	L4-MMS1-01	9.1.8.1 a)
		L4-MMS1-02	9.1.8.1 b)
		L4-MMS1-03	9.1.8.1 c)
		L4-MMS1-04	9.1.8.1 d)
	9.1.8.2 资产管理	L4-MMS1-05	9.1.8.2 a)
		L4-MMS1-06	9.1.8.2 b)
		L4-MMS1-07	9.1.8.2 c)
	9.1.8.3 介质管理	L4-MMS1-08	9.1.8.3 a)
		L4-MMS1-09	9.1.8.3 b)
	9.1.8.4 设备维护管理	L4-MMS1-10	9.1.8.4 a)
		L4-MMS1-11	9.1.8.4 b)
		L4-MMS1-12	9.1.8.4 c)
		L4-MMS1-13	9.1.8.4 d)
	9.1.8.5 漏洞和风险管理	L4-MMS1-14	9.1.8.5 a)
		L4-MMS1-15	9.1.8.5 b)
	9.1.8.6 网络与系统安全管理	L4-MMS1-16	9.1.8.6 a)
		L4-MMS1-17	9.1.8.6 b)
		L4-MMS1-18	9.1.8.6 c)
		L4-MMS1-19	9.1.8.6 d)
		L4-MMS1-20	9.1.8.6 e)
		L4-MMS1-21	9.1.8.6 f)
		L4-MMS1-22	9.1.8.6 g)
		L4-MMS1-23	9.1.8.6 h)
		L4-MMS1-24	9.1.8.6 i)
		L4-MMS1-25	9.1.8.6 j)
	9.1.8.7 恶意代码防范管理	L4-MMS1-26	9.1.8.7 a)
		L4-MMS1-27	9.1.8.7 b)
		L4-MMS1-28	9.1.8.7 c)
	9.1.8.8 配置管理	L4-MMS1-29	9.1.8.8 a)
		L4-MMS1-30	9.1.8.8 b)
	9.1.8.9 密码管理	L4-MMS1-31	9.1.8.9 a)
		L4-MMS1-32	9.1.8.9 b)
	9.1.8.10 变更管理	L4-MMS1-33	9.1.8.10 a)
		L4-MMS1-34	9.1.8.10 b)
		L4-MMS1-35	9.1.8.10 c)
	9.1.8.11 备份与恢复管理	L4-MMS1-36	9.1.8.11 a)
		L4-MMS1-37	9.1.8.11 b)
		L4-MMS1-38	9.1.8.11 c)
	9.1.8.12 安全事件处置	L4-MMS1-39	9.1.8.12 a)
		L4-MMS1-40	9.1.8.12 b)

		L4-MMS1-41	9.1.8.12 c)
		L4-MMS1-42	9.1.8.12 d)
	9.1.8.13 应急预案管理	L4-MMS1-43	9.1.8.13 a)
		L4-MMS1-44	9.1.8.13 b)
		L4-MMS1-45	9.1.8.13 c)
		L4-MMS1-46	9.1.8.13 d)
	9.1.8.14 外包运维管理	L4-MMS1-47	9.1.8.14 a)
		L4-MMS1-48	9.1.8.14 b)
		L4-MMS1-49	9.1.8.14 c)
		L4-MMS1-50	9.1.8.14 d)

D.2 云计算安全测评扩展要求和基本要求对应表

D.2.1 第一级

层面	控制点	测评单元编号	基本要求编号
6.2.1 网络和通信安全	6.2.1.1 网络架构	L1-NCS2-01	6.2.1.1 a)
	6.2.1.2 访问控制	L1-NCS2-03	6.2.1.2 a)
		L1-NCS2-04	6.2.1.2 b)
		L1-NCS2-05	6.2.1.2 c)
6.2.2 设备和计算安全	6.2.2.1 镜像和快照保护	L1-ECS2-01	6.2.2.1 a)
6.2.3 应用和数据安全	6.2.3.1 数据完整性	L1-ADS1-01	6.2.3.1 a)
	6.2.3.2 数据备份恢复	L1-ADS1-02	6.2.3.2 a)
6.2.4 安全建设管理	6.2.4.1 云服务商选择	L1-CMS2-01	6.2.4.1 a)
		L1-CMS2-02	6.2.4.1 b)
		L1-CMS2-03	6.2.4.1 c)
	6.2.4.2 供应链管理	L1-CMS2-04	6.2.4.2 a)

D.2.2 第二级

层面	控制点	测评单元编号	基本要求编号
7.2.1 物理和环境安全	7.2.1.1 物理位置选择	L2-PES2-01	7.2.1.1
7.2.2 网络和通信安全	7.2.2.1 网络架构	L2-NCS2-01	7.2.2.1 a)
		L2-NCS2-02	7.2.2.1 b)
		L2-NCS2-03	7.2.2.1 c)
		L2-NCS2-04	7.2.2.1 d)
	7.2.2.2 访问控制	L2-NCS2-05	7.2.2.2 a)
		L2-NCS2-06	7.2.2.2 b)
		L2-NCS2-07	7.2.2.2 c)
		L2-NCS2-08	7.2.2.2 d)
	7.2.2.3 入侵防范	L2-NCS2-09	7.2.2.3 a)

		L2-NCS2-10	7.2.2.3 b)
		L2-NCS2-11	7.2.2.3 c)
	7.2.2.4 安全审计	L2-NCS2-12	7.2.2.4
7.2.3 设备和计算安全	7.2.3.1 身份鉴别	L2-ECS2-01	7.2.3.1 a)
	7.2.3.2 访问控制	L2-ECS2-02	7.2.3.2 a)
	7.2.3.3 安全审计	L2-ECS2-03	7.2.3.3 a)
	7.2.3.5 资源控制	L2-ECS2-04	7.2.3.5 a)
		L2-ECS2-05	7.2.3.5 b)
		L2-ECS2-06	7.2.3.5 c)
	7.2.3.6 镜像和快照保护	L2-ECS2-07	7.2.3.6 a)
		L2-ECS2-08	7.2.3.6 b)
7.2.4 应用和数据安全	7.2.4.1 数据完整性	L2-ADS1-01	7.2.4.1 a)
	7.2.4.2 数据备份恢复	L2-ADS1-02	7.2.4.2 a)
		L2-ADS1-03	7.2.4.2 b)
	7.2.4.3 剩余信息保护	L2-ADS1-04	7.2.4.3 a)
		L2-ADS1-05	7.2.4.3 b)
	7.2.4.4 个人信息保护	L2-ADS1-06	7.2.4.4 a)
7.2.5 安全建设管理	7.2.5.1 云服务商选择	L2-CMS2-01	7.2.5.1 a)
		L2-CMS2-02	7.2.5.1 b)
		L2-CMS2-03	7.2.5.1 c)
		L2-CMS2-04	7.2.5.1 d)
	7.2.5.2 供应链管理	L2-CMS2-05	7.2.5.2 a)
		L2-CMS2-06	7.2.5.2 b)
7.2.6 安全运维管理	7.2.6.1 云计算环境管理	L2-MMS2-01	7.2.6.1 a)
		L2-MMS2-02	7.2.6.1 b)

D.2.3 第三级

层面	控制点	测评单元编号	基本要求编号
8.2.1 物理和环境安全	8.2.1.1 物理位置选择	L3-PES2-01	8.2.1.1
8.2.2 网络和通信安全	8.2.2.1 网络架构	L3-NCS2-01	8.2.2.1 a)
		L3-NCS2-02	8.2.2.1 b)
		L3-NCS2-03	8.2.2.1 c)
		L3-NCS2-04	8.2.2.1 d)
		L3-NCS2-05	8.2.2.1 e)
		L3-NCS2-06	8.2.2.1 f)
		L3-NCS2-07	8.2.2.1 g)
	8.2.2.2 访问控制	L3-NCS2-08	8.2.2.2 a)
		L3-NCS2-09	8.2.2.2 b)
		L3-NCS2-10	8.2.2.2 c)
		L3-NCS2-11	8.2.2.2 d)

		L3-NCS2-12	8.2.2.2 e)
	8.2.2.3 入侵防范	L3-NCS2-13	8.2.2.3 a)
		L3-NCS2-14	8.2.2.3 b)
		L3-NCS2-15	8.2.2.3 c)
		L3-NCS2-16	8.2.2.3 d)
	8.2.2.4 安全审计	L3-NCS2-17	8.2.2.4 a)
		L3-NCS2-18	8.2.2.4 b)
	8.2.2.5 集中管控	L3-NCS2-19	8.2.2.5
8.2.3 设备和计算安全	8.2.3.1 身份鉴别	L3-ECS2-01	8.2.3.1 a)
		L3-ECS2-02	8.2.3.1 b)
	8.2.3.2 访问控制	L3-ECS2-03	8.2.3.2 a)
		L3-ECS2-04	8.2.3.2 b)
	8.2.3.3 安全审计	L3-ECS2-05	8.2.3.3 a)
		L3-ECS2-06	8.2.3.4 a)
	8.2.3.4 入侵防范	L3-ECS2-07	8.2.3.4 b)
		L3-ECS2-08	8.2.3.4 c)
		L3-ECS2-09	8.2.3.5 a)
	8.2.3.5 资源控制	L3-ECS2-10	8.2.3.5 b)
		L3-ECS2-11	8.2.3.5 c)
		L3-ECS2-12	8.2.3.5 d)
		L3-ECS2-13	8.2.3.5 e)
	8.2.3.6 镜像和快照保护	L3-ECS2-14	8.2.3.6 a)
		L3-ECS2-15	8.2.3.6 b)
		L3-ECS2-16	8.2.3.6 c)
8.2.4 应用和数据安全	8.2.4.1 数据完整性	L3-ADS1-01	8.2.4.1 a)
		L3-ADS1-02	8.2.4.1 b)
	8.2.4.2 数据保密性	L3-ADS1-03	8.2.4.2 a)
		L3-ADS1-04	8.2.4.2 b)
	8.2.4.3 数据备份恢复	L3-ADS1-05	8.2.4.3 a)
		L3-ADS1-06	8.2.4.3 b)
		L3-ADS1-07	8.2.4.3 c)
		L3-ADS1-08	8.2.4.3 d)
		L3-ADS1-09	8.2.4.3 e)
	8.2.4.4 剩余信息保护	L3-ADS1-10	8.2.4.4 a)
		L3-ADS1-11	8.2.4.4 b)
	8.2.4.5 个人信息保护	L3-ADS1-12	8.2.4.5 a)
8.2.5 安全建设管理	8.2.5.1 云服务商选择	L3-CMS2-01	8.2.5.1 a)
		L3-CMS2-02	8.2.5.1 b)
		L3-CMS2-03	8.2.5.1 c)
		L3-CMS2-04	8.2.5.1 d)
		L3-CMS2-05	8.2.5.1 e)

	8.2.5.2 供应链管理	L3-CMS2-06	8.2.5.1 f)
		L3-CMS2-07	8.2.5.2 a)
		L3-CMS2-08	8.2.5.2 b)
		L3-CMS2-09	8.2.5.2 c)
8.2.6 安全运维管理	8.2.6.1 云计算环境管理	L3-MMS2-01	8.2.6.1 a)
		L3-MMS2-02	8.2.6.1 b)

D.2.4 第四级

层面	控制点	测评单元编号	基本要求编号
9.2.1 物理和环境安全	9.2.1.1 物理位置选择	L4-PES2-01	9.2.1.1
9.2.2 网络和通信安全	9.2.2.1 网络架构	L4-NCS2-01	9.2.2.1 a)
		L4-NCS2-02	9.2.2.1 b)
		L4-NCS2-03	9.2.2.1 c)
		L4-NCS2-04	9.2.2.1 d)
		L4-NCS2-05	9.2.2.1 e)
		L4-NCS2-06	9.2.2.1 f)
		L4-NCS2-07	9.2.2.1 g)
		L4-NCS2-08	9.2.2.1 h)
	9.2.2.2 访问控制	L4-NCS2-09	9.2.2.2 a)
		L4-NCS2-10	9.2.2.2 b)
		L4-NCS2-11	9.2.2.2 c)
		L4-NCS2-12	9.2.2.2 d)
		L4-NCS2-13	9.2.2.2 e)
	9.2.2.3 入侵防范	L4-NCS2-14	9.2.2.3 a)
		L4-NCS2-15	9.2.2.3 b)
		L4-NCS2-16	9.2.2.3 c)
		L4-NCS2-17	9.2.2.3 d)
	9.2.2.4 安全审计	L4-NCS2-18	9.2.2.4 a)
		L4-NCS2-19	9.2.2.4 b)
	9.2.2.5 集中管控	L4-NCS2-20	9.2.2.5
9.2.3 设备和计算安全	9.2.3.1 身份鉴别	L4-ECS2-01	9.2.3.1 a)
		L4-ECS2-02	9.2.3.1 b)
	9.2.3.2 访问控制	L4-ECS2-03	9.2.3.2 a)
		L4-ECS2-04	9.2.3.2 b)
	9.2.3.3 安全审计	L4-ECS2-05	9.2.3.3 a)
	9.2.3.4 入侵防范	L4-ECS2-06	9.2.3.4 a)
		L4-ECS2-07	9.2.3.4 b)
		L4-ECS2-08	9.2.3.4 c)
	9.2.3.5 资源控制	L4-ECS2-09	9.2.3.5 a)
		L4-ECS2-10	9.2.3.5 b)

		L4-ECS2-11	9.2.3.5 c)
		L4-ECS2-12	9.2.3.5 d)
		L4-ECS2-13	9.2.3.5 e)
	9.2.3.6 镜像和快照保护	L4-ECS2-14	9.2.3.6 a)
		L4-ECS2-15	9.2.3.6 b)
		L4-ECS2-16	9.2.3.6 c)
9.2.4 应用和数据安全	9.2.4.1 数据完整性	L4-ADS2-01	9.2.4.1 a)
		L4-ADS2-02	9.2.4.1 b)
	9.2.4.2 数据保密性	L4-ADS2-03	9.2.4.2 a)
		L4-ADS2-04	9.2.4.2 b)
	9.2.4.3 数据备份恢复	L4-ADS2-05	9.2.4.3 a)
		L4-ADS2-06	9.2.4.3 b)
		L4-ADS2-07	9.2.4.3 c)
		L4-ADS2-08	9.2.4.3 d)
		L4-ADS2-09	9.2.4.3 e)
	9.2.4.4 剩余信息保护	L4-ADS2-10	9.2.4.4 a)
		L4-ADS2-11	9.2.4.4 b)
	9.2.4.5 个人信息保护	L4-ADS2-12	9.2.4.5 a)
9.2.5 安全建设管理	9.2.5.1 云服务商选择	L4-CMS2-01	9.2.5.1 a)
		L4-CMS2-02	9.2.5.1 b)
		L4-CMS2-03	9.2.5.1 c)
		L4-CMS2-04	9.2.5.1 d)
		L4-CMS2-05	9.2.5.1 e)
		L4-CMS2-06	9.2.5.1 f)
	9.2.5.2 供应链管理	L4-CMS2-07	9.2.5.2 a)
		L4-CMS2-08	9.2.5.2 b)
		L4-CMS2-09	9.2.5.2 c)
9.2.6 安全运维管理	9.2.6.1 云计算环境管理	L4-MMS2-01	9.2.6.1 a)
		L4-MMS2-02	9.2.6.1 b)

D.3 移动互联安全测评扩展要求和基本要求对应表

D.3.1 第一级

层面	控制点	测评单元编号	基本要求编号
6.3.1 物理和环境安全	6.3.1.1 无线接入点的物理位置	L1-PES3-01	6.3.1.1
6.3.2 网络和通信安全	6.3.2.1 边界防护	L1-NCS3-01	6.3.2.1
	6.3.2.2 访问控制	L1-NCS3-02	6.3.2.2
6.3.3 设备和计算安全	6.3.3.1 移动应用管控	L1-ECS3-01	6.3.3.1

6.3.4 安全建设管理	6.3.4.1 移动应用软件采购	L1-CMS3-01	6.3.4.1

D.3.2 第二级

层面	控制点	测评单元编号	基本要求编号
7.3.1 物理和环境安全	7.3.1.1 无线接入点的物理位置	L2-PES3-01	7.3.1.1
7.3.2 网络和通信安全	7.3.2.1 边界防护	L2-NCS3-01	7.3.2.1
	7.3.2.2 访问控制	L2-NCS3-02	7.3.2.2
	7.3.2.3 入侵防范	L2-NCS3-03	7.3.2.3 a)
		L2-NCS3-04	7.3.2.3 b)
		L2-NCS3-05	7.3.2.3 c)
		L2-NCS3-06	7.3.2.3 d)
		L2-NCS3-07	7.3.2.3 e)
		L2-NCS3-08	7.3.2.3 f)
7.3.3 设备和计算安全	7.3.3.1 移动应用管控	L2-ECS3-01	7.3.3.1 a)
		L2-ECS3-02	7.3.3.1 b)
		L2-ECS3-03	7.3.3.1 c)
		L2-ECS3-04	7.3.3.1 d)
	7.3.3.2 资源控制	L2-ECS3-01	7.3.3.2 a)
		L2-ECS3-02	7.3.3.2 b)
7.3.4 安全建设管理	7.3.4.1 移动应用软件采购	L2-CMS3-01	7.3.4.1 a)
		L2-CMS3-02	7.3.4.1 b)
	7.3.4.2 移动应用软件开发	L2-CMS3-03	7.3.4.2 a)
		L2-CMS3-04	7.3.4.2 b)

D.3.3 第三级

层面	控制点	测评单元编号	基本要求编号
8.3.1 物理和环境安全	8.3.1.1 无线接入点的物理位置	L3-PES3-01	8.3.1.1
8.3.2 网络和通信安全	8.3.2.1 边界防护	L3-NCS3-01	8.3.2.1
	8.3.2.2 访问控制	L3-NCS3-02	8.3.2.2
	8.3.2.3 入侵防范	L3-NCS3-03	8.3.2.3 a)
		L3-NCS3-04	8.3.2.3 b)
		L3-NCS3-05	8.3.2.3 c)
		L3-NCS3-06	8.3.2.3 d)
		L3-NCS3-07	8.3.2.3 e)
		L3-NCS3-08	8.3.2.3 f)
8.3.3 设备和计算安全	8.3.3.1 移动终端管控	L3-ECS3-01	8.3.3.1 a)
		L3-ECS3-02	8.3.3.1 b)
	8.3.3.2 移动应用管控	L3-ECS3-01	8.3.3.2 a)

		L3-ECS3-02	8.3.3.2 b)
		L3-ECS3-03	8.3.3.2 c)
		L3-ECS3-04	8.3.3.2 d)
		L3-ECS3-05	8.3.3.2 e)
	8.3.3.3 资源控制	L3-ECS3-01	8.3.3.3 a)
8.3.4 安全建设管理	8.3.4.1 移动应用软件采购	L3-CMS3-01	8.3.4.1 a)
		L3-CMS3-02	8.3.4.1 b)
	8.3.4.2 移动应用软件开发	L3-CMS3-01	8.3.4.2 a)
		L3-CMS3-02	8.3.4.2 b)
8.3.5 安全运维管理	8.3.5.1 配置管理	L3-MMS3-01	8.3.5.1

D.3.4 第四级

层面	控制点	测评单元编号	基本要求编号
9.3.1 物理和环境安全	9.3.1.1 无线接入点的物理位置	L4-PES3-01	9.3.1.1
9.3.2 网络和通信安全	9.3.2.1 边界防护	L4-NCS3-01	9.3.2.1
	9.3.2.2 访问控制	L4-NCS3-02	9.3.2.2
	9.3.2.3 入侵防范	L4-NCS3-03	9.3.2.3 a)
		L4-NCS3-04	9.3.2.3 b)
		L4-NCS3-05	9.3.2.3 c)
		L4-NCS3-06	9.3.2.3 d)
		L4-NCS3-07	9.3.2.3 e)
		L4-NCS3-08	9.3.2.3 f)
9.3.3 设备和计算安全	9.3.3.1 移动终端管控	L4-ECS3-01	9.3.3.1 a)
		L4-ECS3-02	9.3.3.1 b)
	9.3.3.2 移动应用管控	L4-ECS3-03	9.3.3.2 a)
		L4-ECS3-04	9.3.3.2 b)
		L4-ECS3-05	9.3.3.2 c)
		L4-ECS3-06	9.3.3.2 d)
		L4-ECS3-07	9.3.3.2 e)
	9.3.3.3 资源控制	L4-ECS3-08	9.3.3.3 a)
		L4-ECS3-09	9.3.3.3 b)
9.3.4 安全建设管理	9.3.4.1 移动应用软件采购	L4-CMS3-01	9.3.4.1 a)
		L4-CMS3-02	9.3.4.1 b)
	9.3.4.2 移动应用软件开发	L4-CMS3-01	9.3.4.2 a)
		L4-CMS3-02	9.3.4.2 b)
9.3.5 安全运维管理	9.3.5.1 配置管理	L4-MMS3-01	9.3.5.1

D.4 物联网安全测评扩展要求和基本要求对应表

D.4.1 第一级

层面	控制点	测评单元编号	基本要求编号
6.4.1 物理和环境安全	6.4.1.1 感知节点设备物理防护	L1-PES4-01	6.4.1.1 a)
		L1-PES4-02	6.4.1.1 b)
6.4.2 网络和通信安全	6.4.2.1 接入控制	L1-NCS4-01	6.4.2.1
6.4.3 安全运维管理	6.4.3.1 感知节点管理	L1-MMS4-01	6.4.3.1 a)
		L1-MMS4-02	6.4.3.1 b)
		L1-MMS4-03	6.4.3.1 c)
		L1-MMS4-04	6.4.3.1 d)

D.4.2 第二级

层面	控制点	测评单元编号	基本要求编号
7.4.1 物理和环境安全	7.4.1.1 感知节点设备物理防护	L2-PES4-01	7.4.1.1 a)
		L2-PES4-02	7.4.1.1 b)
7.4.2 网络和通信安全	7.4.2.1 入侵防范	L2-NCS4-01	7.4.2.1 a)
		L2-NCS4-02	7.4.2.1 b)
	7.4.2.2 接入控制	L2-NCS4-03	7.4.2.2
7.4.3 安全运维管理	7.4.3.1 感知节点管理	L2-MMS4-01	7.4.3.1 a)
		L2-MMS4-02	7.4.3.1 b)
		L2-MMS4-03	7.4.3.1 c)
		L2-MMS4-04	7.4.3.1 d)

D.4.3 第三级

层面	控制点	测评单元编号	基本要求编号
8.4.1 物理和环境安全	8.4.1.1 感知节点设备物理防护	L3-PES4-01	8.4.1.1 a)
		L3-PES4-02	8.4.1.1 b)
		L3-PES4-03	8.4.1.1 c)
		L3-PES4-04	8.4.1.1 d)
8.4.2 网络和通信安全	8.4.2.1 入侵防范	L3-NCS4-01	8.4.2.1 a)
		L3-NCS4-02	8.4.2.1 b)
	8.4.2.2 接入控制	L3-NCS4-03	8.4.2.2
8.4.3 设备和计算安全	8.4.3.1 感知节点设备安全	L3-ECS4-01	8.4.3.1 a)
		L3-ECS4-02	8.4.3.1 b)
		L3-ECS4-03	8.4.3.1 c)
	8.4.3.2 网关节点设备安全	L3-ECS4-04	8.4.3.2 a)
		L3-ECS4-05	8.4.3.2 b)
		L3-ECS4-06	8.4.3.2 c)

8.4.4 应用和数据安全		L3-ECS4-07	8.4.3.2 d)
		L3-ECS4-08	8.4.3.2 e)
	8.4.4.1 抗数据重放	L3-ADS4-01	8.4.4.1 a)
		L3-ADS4-02	8.4.4.1 b)
	8.4.4.2 数据融合处理	L3-ADS4-03	8.4.4.2
8.4.5 安全运维管理	8.4.5.1 感知节点管理	L3-MMS4-01	8.4.5.1 a)
		L3-MMS4-02	8.4.5.1 b)
		L3-MMS4-03	8.4.5.1 c)
		L3-MMS4-04	8.4.5.1 d)
		L3-MMS4-05	8.4.5.1 e)

D.4.4 第四级

层面	控制点	测评单元编号	基本要求编号
9.4.1 物理和环境安全	9.4.1.1 感知节点设备物理防护	L4-PES4-01	9.4.1.1 a)
		L4-PES4-02	9.4.1.1 b)
		L4-PES4-03	9.4.1.1 c)
		L4-PES4-04	9.4.1.1 d)
9.4.2 网络和通信安全	9.4.2.1 入侵防范	L4-NCS4-01	9.4.2.1 a)
		L4-NCS4-02	9.4.2.1 b)
	9.4.2.2 接入控制	L4-NCS4-03	9.4.2.2
9.4.3 设备和计算安全	9.4.3.1 感知节点设备安全	L4-ECS4-01	9.4.3.1 a)
		L4-ECS4-02	9.4.3.1 b)
		L4-ECS4-03	9.4.3.1 c)
	9.4.3.2 网关节点设备安全	L4-ECS4-04	9.4.3.2 a)
		L4-ECS4-05	9.4.3.2 b)
		L4-ECS4-06	9.4.3.2 c)
		L4-ECS4-07	9.4.3.2 d)
		L4-ECS4-08	9.4.3.2 e)
9.4.4 应用和数据安全	9.4.4.1 抗数据重放	L4-ADS4-01	9.4.4.1 a)
		L4-ADS4-02	9.4.4.1 b)
	9.4.4.2 数据融合处理	L4-ADS4-03	9.4.4.2 a)
		L4-ADS4-04	9.4.4.2 b)
9.4.4 安全运维管理	9.4.5.1 感知节点管理	L4-MMS4-01	9.4.5.1 a)
		L4-MMS4-02	9.4.5.1 b)
		L4-MMS4-03	9.4.5.1 c)
		L4-MMS4-04	9.4.5.1 d)
		L4-MMS4-05	9.4.5.1 e)

D.5 工业控制系统安全测评扩展要求和基本要求对应表

D.5.1 第一级

层面	控制点	测评单元编号	基本要求编号
6.5.1 物理和环境安全	6.5.1.1 室外控制设备物理防护	L1-PES5-01	6.5.1.1 a)
		L1-PES5-02	6.5.1.1 b)
6.5.2 网络和通信安全	6.5.2.1 网络架构	L1-NCS5-01	6.5.2.1 a)
		L1-NCS5-02	6.5.2.1 b)
	6.5.2.2 访问控制	L1-NCS5-03	6.5.2.2
	6.5.2.3 无线使用控制	L1-NCS5-04	6.5.2.3 a)
		L1-NCS5-05	6.5.2.3 b)
6.5.3 设备和计算安全	6.5.3.1 控制设备安全	L1-ECS5-01	6.5.3.1 a)
		L1-ECS5-02	6.5.3.1 b)
6.5.4 安全运维管理	6.5.4.1 漏洞和风险管理	L1-MMS5-01	6.5.4.1

D.5.2 第二级

层面	控制点	测评单元编号	基本要求编号
7.5.1 物理和环境安全	7.5.1.1 室外控制设备物理防护	L2-PES5-01	7.5.1.1 a)
		L2-PES5-02	7.5.1.1 b)
7.5.2 网络和通信安全	7.5.2.1 网络架构	L2-NCS5-01	7.5.2.1 a)
		L2-NCS5-02	7.5.2.1 b)
		L2-NCS5-03	7.5.2.1 c)
	7.5.2.2 通信传输	L2-NCS5-04	7.5.2.2
	7.5.2.3 访问控制	L2-NCS5-05	7.5.2.3 a)
		L2-NCS5-06	7.5.2.3 b)
	7.5.2.4 拨号使用控制	L2-NCS5-07	7.5.2.4
	7.5.2.5 无线使用控制	L2-NCS5-08	7.5.2.5 a)
		L2-NCS5-09	7.5.2.5 b)
7.5.3 设备和计算安全	7.5.3.1 控制设备安全	L2-ECS5-01	7.5.3.1 a)
		L2-ECS5-02	7.5.3.1 b)
7.5.4 安全建设管理	7.5.4.1 产品采购和使用	L2-CMS5-01	7.5.4.1
	7.5.4.2 外包软件开发	L2-CMS5-02	7.5.4.2
7.5.5 安全运维管理	7.5.5.1 漏洞和风险管理	L2-MMS5-01	7.5.5.1
	7.5.5.2 恶意代码防范管理	L2-MMS5-02	7.5.5.2
	7.5.5.3 安全事件处置	L2-MMS5-03	7.5.5.3

D.5.3 第三级

层面	控制点	测评单元编号	基本要求编号
8.5.1 物理和环境安全	8.5.1.1 室外控制设备物理防护	L3-PES5-01	8.5.1.1 a)
		L3-PES5-02	8.5.1.1 b)
8.5.2 网络和通信安全	8.5.2.1 网络架构	L3-NCS5-01	8.5.2.1 a)

		L3-NCS5-02	8.5.2.1 b)
		L3-NCS5-03	8.5.2.1 c)
	8.5.2.2 通信传输	L3-NCS5-04	8.5.2.2
	8.5.2.3 访问控制	L3-NCS5-05	8.5.2.3 a)
		L3-NCS5-06	8.5.2.3 b)
	8.5.2.4 拨号使用控制	L3-NCS5-07	8.5.2.4 a)
		L3-NCS5-08	8.5.2.4 b)
	8.5.2.5 无线使用控制	L3-NCS5-09	8.5.2.5 a)
		L3-NCS5-10	8.5.2.5 b)
		L3-NCS5-11	8.5.2.5 c)
		L3-NCS5-12	8.5.2.5 d)
8.5.3 设备和计算安全	8.5.3.1 控制设备安全	L3-ECS5-01	8.5.3.1 a)
		L3-ECS5-02	8.5.3.1 b)
		L3-ECS5-03	8.5.3.1 c)
		L3-ECS5-04	8.5.3.1 d)
		L3-ECS5-05	8.5.3.1 e)
8.5.4 安全建设管理	8.5.4.1 产品采购和使用	L3-CMS5-01	8.5.4.1
	8.5.4.2 外包软件开发	L3-CMS5-02	8.5.4.2
8.5.5 安全运维管理	8.5.5.1 漏洞和风险管理	L3-MMS5-01	8.5.5.1 a)
		L3-MMS5-02	8.5.5.1 b)
	8.5.5.2 恶意代码防范管理	L3-MMS5-03	8.5.5.2 a)
		L3-MMS5-04	8.5.5.2 b)
	8.5.5.3 安全事件处置	L3-MMS5-05	8.5.5.3

D.5.4 第四级

层面	控制点	测评单元编号	基本要求编号
9.5.1 物理和环境安全	9.5.1.1 室外控制设备物理防护	L4-PES5-01	9.5.1.1 a)
		L4-PES5-02	9.5.1.1 b)
9.5.2 网络和通信安全	9.5.2.1 网络架构	L4-NCS5-01	9.5.2.1 a)
		L4-NCS5-02	9.5.2.1 b)
		L4-NCS5-03	9.5.2.1 c)
	9.5.2.2 通信传输	L4-NCS5-04	9.5.2.2
	9.5.2.3 访问控制	L4-NCS5-05	9.5.2.3 a)
		L4-NCS5-06	9.5.2.3 b)
	9.5.2.4 拨号使用控制	L4-NCS5-07	9.5.2.4 a)
		L4-NCS5-08	9.5.2.4 b)
		L4-NCS5-09	9.5.2.4 c)
	9.5.2.5 无线使用控制	L4-NCS5-10	9.5.2.5 a)
		L4-NCS5-11	9.5.2.5 b)
		L4-NCS5-12	9.5.2.5 c)

		L4-NCS5-13	9.5.2.5 d)
9.5.3 设备和计算安全	9.5.3.1 控制设备安全	L4-ECS5-01	9.5.3.1 a)
		L4-ECS5-02	9.5.3.1 b)
		L4-ECS5-03	9.5.3.1 c)
		L4-ECS5-04	9.5.3.1 d)
		L4-ECS5-05	9.5.3.1 e)
9.5.4 安全建设管理	9.5.4.1 产品采购和使用	L4-CMS5-01	9.5.4.1
	9.5.4.2 外包软件开发	L4-CMS5-02	9.5.4.2
9.5.5 安全运维管理	9.5.5.1 漏洞和风险管理	L4-MMS5-01	9.5.5.1 a)
		L4-MMS5-02	9.5.5.1 b)
	9.5.5.2 恶意代码防范管理	L4-MMS5-03	9.5.5.2 a)
		L4-MMS5-04	9.5.5.2 b)
	9.5.5.3 安全事件处置	L4-MMS5-05	9.5.5.3

参 考 文 献

- [1] ISO/IEC 27000-2013 信息安全管理体 概述和术语
- [2] ISO/IEC 27001-2013 信息安全管理体 要求
- [3] ISO/IEC 27002-2013 信息安全管理实用规则
- [4] ISO/IEC 27003-2013 信息安全管理体实施指南
- [5] GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
- [6] GB/T 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求
- [7] GB/T 28448-2012 信息安全技术 信息系统安全等级保护测评要求
- [8] GB/T 20269-2006 信息安全技术 信息系统安全管理要求
- [9] GB/T 20270-2006 信息安全技术 网络基础安全技术要求
- [10] GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求
- [11] GB/T 20272-2006 信息安全技术 操作系统安全技术要求
- [12] GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求
- [13] GB/T 20282-2006 信息安全技术 信息系统安全工程管理要求
- [14] GB 50174-2008 电子信息系统机房设计规
- [15] GB/T 18336.1-2015 信息技术 安全技术 信息技术安全评估准则 第1部分：简介和一般模型
- [16] GB/T 18336.2-2015 信息技术 安全技术 信息技术安全评估准则 第2部分：安全功能组件
- [17] GB/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件
- [18] YD/T 2437-2012 物联网总体框架与技术要求
- [19] YDB 101-2012 物联网安全需求
- [20] NIST Special Publication 800-53 联邦信息系统推荐性安全控制措施
- [21] GB/T 30976.1-2014 《工业控制系统信息安全第1部分：评估规范》
- [22] GB/T 30976.2-2014 《工业控制系统信息安全第2部分：验收规范》
- [23] GB/T 32919-2016 《信息安全技术 工业控制系统安全控制应用指南》
- [24] IEC 62264-1 《Enterprise-control system integration - Part 1: Models and terminology》
- [25] IEC 62443-1-1 《Industrial communication networks-network and system security-part 1-1: terminology, concepts and models》
- [26] IEC 62443-3-2 《Industrial communication networks - Network and system security - Part 3-2: Security assurance levels for zones and conduits》
- [27] IEC 62443-3-3 《Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels》
- [28] NIST SP800-82-2011 《Guide to Industrial Control Systems (ICS) Security》