

中华人民共和国通信行业标准

YD/T 3315—2018

电信网和互联网安全服务实施要求

Telecommunication network and internet security service
implementation requirements

2018-02-09 发布

2018-04-01 实施

中华人民共和国工业和信息化部 发布

目 次

前言.....	III
1 范围.....	1
2 规范性引用文件.....	1
3 术语、定义和缩略语.....	1
3.1 术语和定义.....	1
3.2 缩略语.....	2
4 电信网和互联网安全服务概述.....	3
5 安全服务提供方基本要求.....	4
5.1 组织要求.....	4
5.2 设备、设施与环境要求.....	4
5.3 质量保障要求.....	5
5.4 项目管理要求.....	5
5.5 保密管理.....	6
6 安全风险评估服务要求.....	7
6.1 需求分析.....	7
6.2 方案编制与确认.....	8
6.3 资产识别.....	8
6.4 威胁评估.....	9
6.5 脆弱性评估.....	9
6.6 安全证据确认与保存.....	9
6.7 风险评估报告及处置建议.....	10
7 安全集成服务要求.....	11
7.1 安全集成概述.....	11
7.2 集成准备.....	11
7.3 方案设计.....	12
7.4 建设实施.....	13
7.5 安全保证.....	14
7.6 运行维护.....	16
7.7 培训.....	16
8 应急响应服务要求.....	17
8.1 网络安全应急响应服务概述.....	17
8.2 准备阶段.....	17
8.3 检测阶段.....	20

8.4	抑制阶段.....	21
8.5	根除阶段.....	22
8.6	恢复阶段.....	23
8.7	总结和报告阶段.....	23
9	安全培训服务要求.....	24
9.1	概述.....	24
9.2	培训需求分析.....	24
9.3	培训计划.....	25
9.4	培训准备工作.....	26
9.5	培训实施.....	27
9.6	培训效果评价.....	28
10	符合性评测服务要求.....	29
10.1	概述.....	29
10.2	测评准备工作.....	29
10.3	测评方案制定.....	29
10.4	测评实施.....	29
10.5	安全证据确认与保存.....	30
10.6	测评报告要求.....	30

前 言

本标准按照 GB/T1.1-2009 给出的规则起草。

随着电信网和互联网的发展，将不断补充和完善电信网和互联网安全防护体系的相关标准。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国通信企业协会通信网络安全专业委员会、中国信息通信研究院、国家计算机网络应急技术处理协调中心、中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团有限公司、数据通信科学技术研究所、河南省信息咨询设计研究有限公司。

本标准主要起草人：李晶晶、江浩洁、谢玮、王卫东、王华、曹一生、郑涛、李燕伟、马铮、姜楠、何友斌、陈禹、王鹏翮、汪志、闻蕾、杨振杰。

电信网和互联网安全服务实施要求

1 范围

本标准规定了第三方安全服务组织为电信网和互联网实施安全服务过程中所需满足的实施要求。
本标准适用于第三方安全服务组织。

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，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 2669—2013 电信网和互联网第三方安全服务能力评定准则

YD/T 1799—2008 网络与信息安全应急处理服务资质评估方法

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

电信网和互联网安全服务 telecommunication network and internet security service

面向组织或个人的各类网络安全保障需求，由服务提供方按照服务协议所执行的一个网络安全过程或任务。

通常是基于网络安全技术、产品或管理体系的，通过外包的形式，由专业网络安全人员所提供的支持和帮助。

3.1.2

电信网和互联网安全服务提供方 telecom network and internet security service provider

按照服务协议，通过专业的网络安全人员提供网络安全服务的各类组织机构。网络安全服务提供方在每项具体的服务中，其服务角色和服务职责应该是明确的。如果服务内容仅涉及供需双方的，则服务提供方为乙方角色；在上述服务的基础上，就所涉及的问题，独立于有关各方提供评估、证明等服务并承担相关社会责任的，则服务提供方为第三方角色。服务角色与服务提供方的组织机构类型无关。

3.1.3

电信网和互联网安全服务需求方 telecom network and internet security service demander

使用外部所提供的网络安全服务，以满足电信网和互联网安全保障需求，实现自身业务目标的组织（或个人用户）。

3.1.4

安全风险评估 security risk assessment

运用科学的方法与手段，系统地分析通信网络及相关系统所面临的威胁及其存在的脆弱性，评估安全事件可能造成的危害程度，并提出有针对性的防护对策和安全措施，防范和化解通信网络及相关系统安全风险，将风险控制在可接受的水平，为最大限度地保障通信网络及相关系统的安全提供科学依据。

3.1.5

安全集成 security integration

对所服务的通信网络的安全框架进行设计，形成安全建设规划，并对计划实施的安全策略细化，在安全解决方案的基础上，实施安全产品集成、安全软件定制开发、安全加固或其他的安全技术和咨询服务。

3.1.6

应急响应 emergency response

在处置网络与信息安全事件时提供紧急现场或远程援助的一系列技术和非技术的措施和行动，以降低安全事情给用户造成的损失或影响。

3.1.7

安全培训 security training

针对电信网和互联网的安全管理、建设、运行维护等与网络安全相关的岗位人员所开展的，以提高安全意识、安全素质和安全技能为目的教育培训活动。服务提供方按照培训需求提供网络与信息安全法律、政策、标准、技术、管理、体系和工程等方面的培训内容。

3.1.8

符合性测评 conformance test and assessment

针对定级的电信网和互联网网络单元进行检测，评价其是否符合相关安全防护标准的规定要求。

3.2 缩略语

下列缩略语适用于本文件。

BIA	业务影响分析	Business Impact Analysis
CRM	客户关系管理	Customer Relationship Management
IDS	入侵检测系统	Intrusion Detection Systems
RPO	恢复点目标	Recovery Point Objective

RTO 恢复目标时间 Recovery Time Object

4 电信网和互联网安全服务概述

电信网和互联网安全服务实施要求按照要素分为对服务提供方的基本要求和安全服务过程实施要求两大类。

对安全服务提供方的基本要求是指电信网和互联网安全服务提供方所应满足的基本要素，包括管理与组织、服务企业资质要求两个方面。

按照安全服务实施内容的不同，电信网和互联网安全服务分为安全风险评估、符合性测评、安全集成、应急响应、安全培训等 5 个类型，针对不同安全服务类型的内容和特点，需要满足相应的过程实施要求。

网络安全服务要素如图 1 所示。

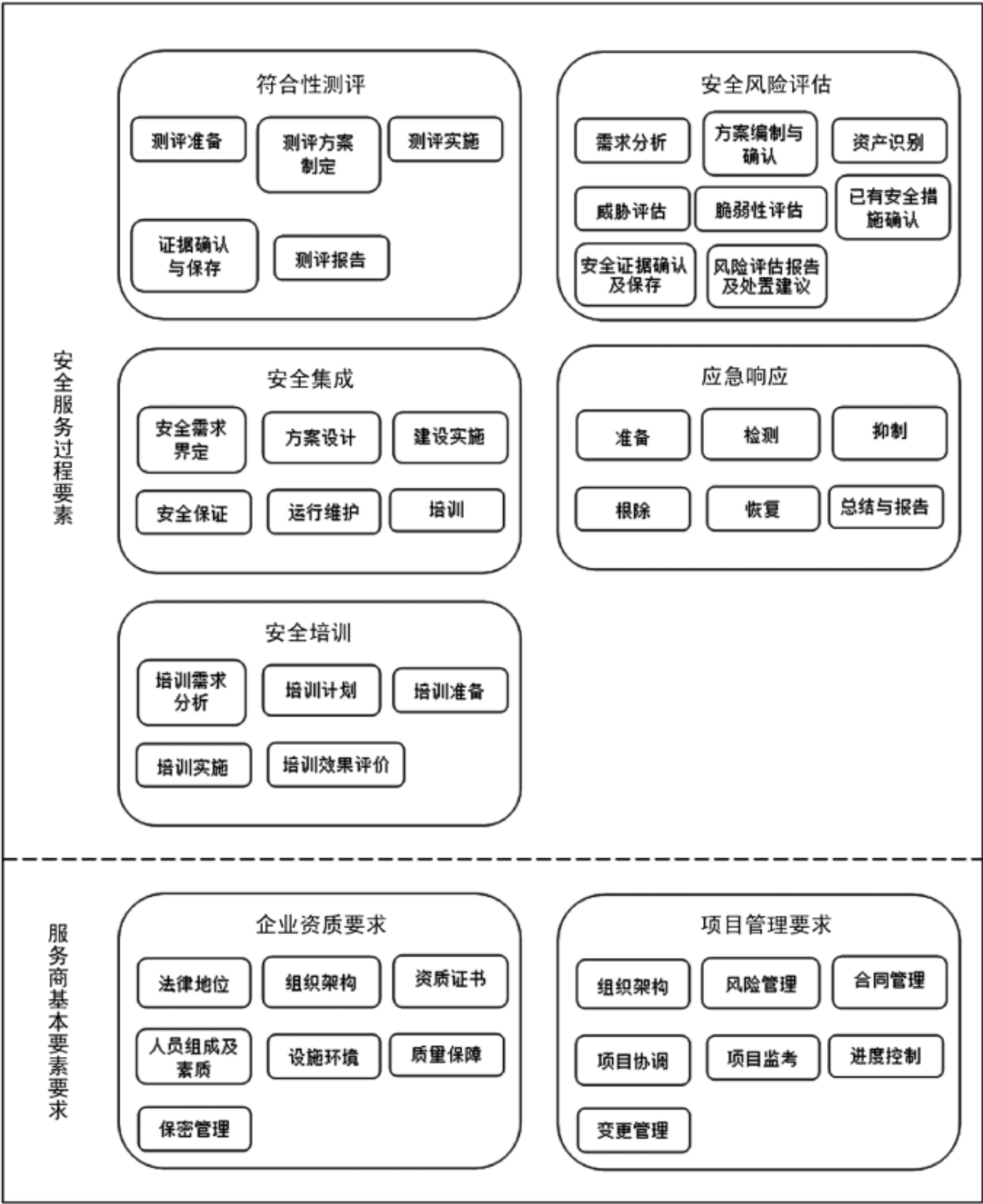


图1 网络安全服务要素

5 安全服务提供方基本要求

5.1 组织要求

5.1.1 法律要求

提供电信网和互联网安全服务的组织应是一个独立的实体，由中国公民投资、中国法人投资或者国家投资的，具有独立法人资格及相关部门颁发的合法经营资格的企事业单位；

从事电信网和互联网安全服务的组织应拥有健全的组织与管理体系，应制定并落实保密制度，执行保密技术标准。如从事涉及国家秘密的电信网和互联网安全服务的组织应制定符合国家保密部门规定的相关要求，具体应符合 YD/T 2669—2013 中规定的通信网络安全服务能力等级基本要求。

5.1.2 资质证书要求

5.1.2.1

从事电信网和互联网安全服务的组织应具备相关行业组织颁发的网络安全服务能力评定资格证书。

5.1.2.2

从事涉及国家秘密的电信网和互联网安全服务的组织应获得国家保密机关的资质认证；

5.1.3 人员构成和素质要求

从事电信网和互联网安全服务的组织应具有充足的人力资源和合理的人员结构，具备与资质范围相适应的技术负责人。具体要求为：

1) 组织内获得权威机构安全认证工程师至少应有 2 名。直接从事安全服务的人员不少于 5 人，大学本科以上学历不少于 80%。至少有项目经理 1 人、高级项目经理 1 人。应有一批相对稳定的技术队伍，有至少 3 人具有 2 年以上的安全服务项目经验。

2) 所有与电信网和互联网安全服务有关的人员等应具有基本的信息安全知识，骨干技术人员应系统地掌握信息安全基础理论和核心技术，并具有足够的专业工作经验。

3) 应有相对稳定的电信网和互联网 7 安全专业技术队伍。

4) 法人及主要业务、技术人员无犯罪记录。

5.2 设备、设施与环境要求

5.2.1 基本要求

从事电信网和互联网安全服务的组织：

1) 应具有固定的工作场所，良好的工作环境，具有实施相关服务的必需的开发、生产、测试和管理工具；

2) 应确保所提供服务及承载业务数据和用户数据的设备、设施均位于中国境内。

5.2.2 安全风险评估服务/符合性测评

应具有专门从事电信网和互联网安全风险评估服务/符合性测评服务的相关工具或软件，如漏洞扫

描工具、安全基线核查、网站安全检测工具等。

5.2.3 安全集成

应具有针对安全设计与集成产品的开发、测试和实验环境，有自主研发的安全产品，安全产品研发团队具有较高的技术水平和切实有效的安全服务行业的研发成果。

5.2.4 应急响应

从事电信网和互联网安全服务的组织：

- 1) 应具有实施应急处理服务的必需的研究和实验环境；
- 2) 应有处理安全事件的工具或软件，如入侵检测工具、日志分析工具、取证工具等。

5.2.5 安全培训

从事电信网和互联网安全服务的组织：

- 1) 应具有进行安全培训服务的必需的培训场所、培训环境、讲师队伍等；
- 2) 应有进行安全培训的安全课件、实验环境、实验工具或软件等。

5.3 质量保障要求

项目应具备明确的工作目标，与服务需求方进行充分的沟通，明确项目的目标并记录，明确项目对完成目标的考核要求。服务方应具备以下条件：

- 1) 服务方为保证项目目标的完成，应建立并落实质量管理体系：从项目需求、项目计划、项目实施、项目总结等各个方面建立完善的管理流程，应具备质量保证、纠正和预防措施管理的规范性文件。
- 2) 服务方应建立自行评估服务质量的体系，并能对服务质量进行持续改进的管理流程：编制并建立内部质量管理手册，并对所有项目人员进行培训，使项目成员充分了解、掌握并严格执行质量管理手册，并按照质量保证控制程序进行工作。
- 3) 服务方应建立完善的内部质量管理制度：包括保密制度、质量申诉处理制度、定期业务培训、业务交流教育制度、文件资料的档案管理制度，所有项目成员应充分了解并熟悉以上制度，在项目实施过程中遵守相关制度。

5.4 项目管理要求

提供电信网和互联网安全服务的组织应对整个安全服务项目进行科学的管理，实现组织架构、风险管理、合同管理、协调管理、监控管理、进度控制、变更管理的严格控制。

5.4.1 项目组织架构

服务方应具备独立的法人资格，并能够提供足以实施安全服务活动以及包括绩效测量和监测工作的人力、专项技能与技术、财力资源，具备与资质范围相适应的技术负责人；应拥有健全的组织结构和管理体系，有专门的安全服务部门或团队。

5.4.2 项目风险管理

服务方应具有项目风险管理部门或风险管理人员，并就项目风险进行有效的管理。具体为：

- 1) 服务方应建立项目风险管理相关的管理制度，并能提供项目风险管理制度有效运行的证据；
- 2) 安全服务项目的风险主要来自安全服务过程的不确定性、安全服务实施人员素质、客户工作环境的特殊要求等。在项目实施之时，应该充分考虑到各种风险因素，识别项目中存在的各种风险，制定风险规避措施和风险计划，并培训项目实施人员，使项目成员能了解并熟悉项目风险，并严格落实项目风险规避的措施。

5.4.3 项目合同管理

服务提供方应完成以下事项：

- 1) 应签订服务合同或协议；
- 2) 应明确双方的职责和责任；
- 3) 应明确评估的具体行为，明确哪些具体的评估行为是可接受或者禁止的，哪些行为需要系统管理者的事先批准，尤其是对于关键系统的拒绝服务尝试、对敏感信息的破解尝试。

5.4.4 项目协调管理

项目中，将采用正规的项目沟通程序，保证参与项目的各方能够保持对项目的了解和支持。这些管理和沟通措施将对项目过程的质量和结果的质量具有重要的作用。应具有成文的项目协调制度，并符合相关项目管理标准。

5.4.5 项目监控管理

项目的技术活动监控指通过对项目资源的协调使得项目过程达到最优的状态，同时通过对各种变化的监控，及时做出对项目执行有利的响应。项目的监控应包括项目计划制定、项目计划执行和项目过程控制。

5.4.6 项目进度控制

服务方应按照项目计划开展工作，对项目进度要进行严格的管理，并具备项目进度管理制度。应能提供项目进度管理制度可以有效运行的证据。涉及项目计划变更的情况，应双方协商一致解决并更新项目计划书。

5.4.7 项目变更管理

不受控制的项目变更，包括目标变更、范围变更、人员变更、环境变更、文档修改等等是对项目质量的重大威胁。具体为：

- 1) 在项目中，应围绕对项目计划的维护为核心，对项目计划及其衍生文档进行正规的变更控制管理；
- 2) 应对项目变更要进行严格的管理，并具备项目变更管理制度；
- 3) 应能提供项目变更管理制度可以有效运行的证据。

5.5 保密管理

服务提供方应与服务对象签订服务合同或协议，明确双方的职责和责任，承诺对所进行的安全服务工作保密，确保不泄露安全服务工作的重要和敏感信息。具体为：

- 1) 应制定符合国家保密部门要求的工作保密制度和建立相应的组织监管体系;
- 2) 安全服务人员应与安全服务提供者签订保密协议, 并遵守有关法律法规;
- 3) 建立人员管理程序, 明确保密岗位与职责, 定期对安全服务人员进行安全保密教育与培训, 并签订保密责任书, 规定应当履行的安全保密义务和承担的法律法律责任。

6 安全风险评估服务要求

6.1 需求分析

在风险评估实施前, 应进行风险评估需求分析, 具体包括确定风险评估的目标, 确定风险评估的范围, 以及进行系统调研。

6.1.1 确定目标

风险评估的准备阶段应根据电信网和互联网业务持续发展在安全方面的需求, 明确风险评估的目标, 为风险评估的过程提供导向。

6.1.2 确定范围

基于风险评估目标确定是完成风险评估的前提, 应明确风险评估的范围。电信网和互联网及相关系统的安全风险评估内容, 可以是整个电信网和互联网及相关系统中全部资产、管理机构, 也可以是电信网和互联网及相关系统中的某个部分的独立资产、相关的部门等。

6.1.3 网络或系统调研

风险评估团队应对电信网和互联网及相关系统中的评估对象进行充分的调研。评估对象调研可以采取问卷调查、现场面谈相结合的方式进行。

网络或系统调研内容至少应包括:

- 1) 业务战略及管理制度;
- 2) 主要的业务功能和要求;
- 3) 网络结构与网络环境, 包括内部连接和外部连接;
- 4) 网络或系统边界;
- 5) 主要的硬件、软件;
- 6) 数据和信息;
- 7) 网络或系统数据的敏感性;
- 8) 支持和使用系统的人员;
- 9) 网络或系统之前风险评估的情况;
- 10) 其他。

6.1.4 需求确认

上述所有内容确定完成后, 应形成较为完整的需求分析报告, 得到组织管理者的确认、批准; 并将

本次风险评估确定的目标和范围向管理层和技术人员进行传达。

根据风险评估的具体情况，需求分析报告可以单独成文，也可以包含在风险评估实施方案中。

6.2 方案编制与确认

评估方应确定评估依据和方法，在此基础上编制风险评估方案并获得管理者对风险评估工作的确认。

6.2.1 确定依据

应根据系统调研结果，确定评估依据和评估方法。评估依据应包括(但不限于)：

- 1) 现行国际标准、国家标准、行业标准；
- 2) 行业主管部门业务系统的要求和制度；
- 3) 网络或系统安全保护等级要求；
- 4) 网络或系统互联单位的安全要求；
- 5) 网络或系统本身的实时性或性能要求等。

根据评估依据，应考虑评估的目的、范围、时间、效果、人员素质等因素来选择具体的风险计算方法，并依据业务实施对系统安全运行的需求，确定相关的判断依据，使之能够与组织环境和安全要求相适应。

6.2.2 制定方案

评估方应制定风险评估方案，用于指导实施方开展后续工作。风险评估方案的内容应包括(但不限于)：

- 1) 团队组织：包括评估团队成员、组织结构、角色、责任等内容；
- 2) 工作计划：风险评估各阶段的工作计划，包括工作内容、工作形式、工作成果等内容；
- 3) 时间进度安排：项目实施的时间进度安排。

6.2.3 方案确认

上述所有内容确定后，应形成较为完整的风险评估实施方案，得到组织管理者的确认、批准；在组织范围内就风险评估相关内容进行培训，明确有关人员在风险评估中的任务。

6.3 资产识别

6.3.1 资产分类

在电信网和互联网及相关系统的风险评估中，应将电信网和互联网及相关系统资产进行恰当的分类，以此为基础进行下一步的风险评估。资产分类方法可参见具体网络的安全防护要求。

6.3.2 资产赋值

应综合考虑资产的社会影响力、业务价值和可用性三个安全属性对资产进行赋值，并在此基础上得出一个综合的结果。为确保资产赋值时的一致性和准确性，组织应建立资产价值评价尺度，以指导资产赋值。资产价值评估者可根据资产赋值结果，确定重要资产的范围，并主要围绕重要资产进行下一步的

风险评估。

6.4 威胁评估

6.4.1 威胁分类

应考虑威胁的来源，根据其表现形式将威胁进行分类。

6.4.2 威胁赋值

应对威胁进行赋值，针对电信网和互联网及相关系统中具体网络的威胁可参见具体网络的安全防护要求。

6.5 脆弱性评估

6.5.1 脆弱性识别内容

应从技术和管理两个方面进行脆弱性识别。技术脆弱性涉及物理环境层、设备和系统层、网络层、业务/应用层等各个层面的安全问题。管理脆弱性又可分为技术管理脆弱性和组织管理脆弱性两方面，前者与具体技术活动相关，后者与管理环境相关。

6.5.2 脆弱性赋值

应根据对资产的损坏程度、技术实现的难易程度、脆弱性流行程度等，采用等级方式对已识别的脆弱性的严重程度进行赋值。资产的脆弱性赋值还应参考技术管理和组织管理脆弱性的严重程度。

6.5.3 已有安全措施确认

评估人员应对已采取的安全措施的有效性进行确认。安全措施的确应评估其有效性，即是否真正降低了系统的脆弱性，抵御了威胁。

6.6 安全证据确认与保存

应对安全证据进行确认和保存。安全评估结果会产生包含评估安全证据的结果记录文档，根据项目阶段的不同，将评估结果与被评估方进行反馈，主要包括测试检查阶段、数据分析与报告阶段、项目验收阶段的结果反馈确认。

6.6.1 测试检查阶段

应确保风险评估过程中的各种现场记录可复现，作为产生歧义后解决问题的依据，并需要被评估方签字确认。

6.6.2 数据分析与报告阶段

应对风险评估过程中的各种现场记录进行再次确认，被评估方应进行签字确认。

6.6.3 项目验收阶段

项目组提交项目的成果报告，被评估方负责人对成果报告进行审定，如果需要修改，应由项目组修改后重新提交审定，被评估方通过后，进行项目验收评审会，并签署项目验收报告。

6.6.4 资料保存

对项目实施涉及到的资料的保存，评估方应严守知识产权条款，保护被评估方利益和商业、技术秘密：包括针对项目所开发的软件程序、安全服务文档，被评估方提供的所有业务、技术资料。

6.7 风险评估报告及处置建议

6.7.1 风险评估文档控制要求

记录风险评估过程的相关文档，应符合以下要求(但不仅限于此)：

- 1) 确保文档发布前是得到批准的；
- 2) 确保文档的更改和现行修订状态是可识别的；
- 3) 确保文档的分发得到适当的控制，并确保在使用时可获得有关版本的适用文档；
- 4) 防止作废文档的非预期使用，若因任何目的需保留作废文档时，应对这些文档进行适当的标识。

对于风险评估过程中形成的相关文档，还应规定其标识、存储、保护、检索、保存期限以及处置所需的控制。

6.7.2 风险评估文档内容要求

风险评估文档是指在整个风险评估过程中产生的评估过程文档和评估结果文档，应包括(但不仅限于此)：

- 1) 风险评估方案：阐述风险评估的目标、范围、人员、评估方法、评估结果的形式和实施进度、明确评估的目的、职责、过程、相关的文档要求，以及实施本次评估所需要的各种资产、威胁、脆弱性识别和判断依据；
- 2) 资产识别清单：根据组织在风险评估程序文档中所确定的资产分类方法进行资产识别，形成资产识别清单，明确资产的责任人/部门；
- 3) 重要资产清单：根据资产识别和赋值的结果，形成重要资产列表，包括重要资产名称、描述、类型、重要程度、责任人/部门等；
- 4) 威胁列表：根据威胁识别和赋值的结果，形成威胁列表，包括威胁名称、种类、来源、动机及出现的频率等；
- 5) 脆弱性列表：根据脆弱性识别和赋值的结果，形成脆弱性列表，包括具体脆弱性的名称、描述、类型及严重程度等；
- 6) 已有安全措施确认表：根据对已采取的安全措施确认的结果，形成已有安全措施确认表，包括已有安全措施名称、类型、功能描述及实施效果等；
- 7) 风险评估报告：对整个风险评估过程和结果进行总结，详细说明被评估对象、风险评估方法、资产、威胁、脆弱性的识别结果、风险分析、风险统计和结论等内容；
- 8) 风险处理计划：对评估结果中不可接受的风险制定风险处理计划，选择适当的控制目标及安全措施，明确责任、进度、资源，并通过对残余风险的评价以确定所选择安全措施的有效性；
- 9) 风险评估记录：根据风险评估程序，要求风险评估过程中的各种现场记录可复现评估过程，并作为产生歧义后解决问题的依据。

6.7.3 风险处置建议

应根据风险评估结果，提供安全加固建议，包括网络层面网络架构调整建议、系统层面主机加固建议方案，以及业务层面相关安全加固调整建议方案。例如：漏洞修补；切断攻击路径；加强审计，加强震慑；对业务运行情况进行实时监控等。

7 安全集成服务要求

7.1 安全集成概述

安全集成是指从事计算机应用系统工程和网络系统工程的安全需求界定、安全设计、建设实施、安全保证的活动。

安全集成一般是按照信息系统建设的安全需求，采用信息系统安全工程的方法和理论，将安全单元、产品部件进行集成的行为或活动。安全集成包括在新建信息系统的结构化设计中考虑信息安全保证因素，从而使建设完成后的信息系统满足建设方或使用方的安全需求而开展的活动。也包括在已有信息系统的基础上额外增加信息安全子系统或信息安全设备等，通常被称为安全优化或安全加固。

7.2 集成准备

7.2.1 界定安全需求

风险评估是安全集成的重要基础。依据网络安全风险评估过程中已识别出的风险，明确客户的内外部安全需求，并制定安全目标。

安全需求界定需要根据下面要求输出《安全集成服务项目需求分析》报告，其中，“安全需求”“法律、政策和约束”“安全背景”“安全目标”“安全需求目标（达成安全协议）”为必选的章节。

界定安全需求的目标：在安全需求方面与客户和其他团体达成共识。具体要求如下：

1) 理解安全需求

收集和分析所有有助于全面理解客户安全需求的信息。

2) 识别法律、政策和约束条件

识别影响客户安全需求的法律、法规和行业标准等外部因素，并确定遵从全球性政策和本地政策的优先权。

3) 识别安全背景

识别影响信息系统安全的背景因素，如信息系统的用途(如金融、医疗)、运行场景、技术发展的变化、社会当前热点事件。

4) 获取安全视图

开发组织的高层次安全分析视图，包括业务需求、角色、职责、信息流、资产、资源、人员保护以及物理保护等。

5) 识别安全目标

识别满足信息系统安全需求的安全目标。安全目标应该至少涉及信息系统及其承载信息的可用性、保密性、完整性、可核查性、真实性和可靠性要求。

6) 定义安全要求

定义信息系统的安全要求，并确保安全要求与适用的政策、法律、标准、安全需求以及约束条件保持一致。安全要求应全面体现信息系统的安全需求，并与安全目标建立对应关系。

7) 达成安全协议

依据安全要求和客户需求，与客户和相关的团体达成共识。

7.2.2 确定服务合同

具体要求如下：

- 1) 与客户和供方在服务合同中至少明确服务范围、目标、质量和成本；
- 2) 与客户和供方在服务合同中包括项目保密责任和违约责任。

7.2.3 确定服务人员和组织

与客户和供方确定项目人员构成，并控制由项目人员变更带来的相关风险。

7.2.4 签订保密协议

与客户和供方签订保密协议；注意保密内容与客户要求的一致性。

7.3 方案设计

基于“7.2.1 安全需求界定”中识别的安全需求，为信息系统的规划人员、设计人员、实施人员和客户提供所需的安全输入信息。这些信息至少包括安全体系结构、设计或实施的项目方案以及安全指南。

本要求的目标：评审信息系统中所有涉及安全的问题，并按照安全目标在方案设计中解决；安全集成项目组及各工作组所有成员都应该理解安全问题，各司其职；项目方案应反映所提供的安全需求和要求。

具体要求如下：

1) 理解安全需求

与设计人员、开发人员、客户沟通确认，以确保相关团体对安全输入需求达成共识。

2) 确定安全约束条件和考虑事项

安全集成项目组应分析和确定在需求、设计、实施、配置和文档方面的安全约束条件和考虑事项，以便于在各工作组的具体工作中做出最佳的安全集成选择。

3) 识别安全集成项目方案

根据客户安全需求以及其他约束条件，识别和制定项目方案。

4) 评审项目方案

各工作组和安全集成项目组要利用已识别的安全约束条件和考虑事项评审项目方案。

5) 提供安全集成指南（下一阶段目标）

安全集成项目组应该开发项目相关的安全集成指南，并把它提供给各工作组。各工作组根据相关的安全集成指南对信息系统的体系结构、设计和实现的选择条件做出决定。

6) 提供安全运行指南（下一阶段目标）

安全集成项目组应该设计并开发安全运行指南，并提供给系统用户和管理员。本运行指南指导用户

和管理员以安全的方式进行安装、配置、运行和废弃系统。

7.4 建设实施

7.4.1 协调安全

协调安全的目的是确保所有相关组织和工作组人员都能积极参与安全集成项目。协调安全涉及到保持所有项目人员与外部组织以及工作组之间沟通。

本要求的目标：项目组的所有成员都能主动地参与到安全集成项目中，最大程度地发挥他们的作用；沟通和协调有关安全的决策和建议。

具体要求如下：

1) 制定协调目标

需要相关工作组重视并参与安全集成项目。根据项目组的信息需求和项目要求决定共享信息的目标，并建立与他们之间的合作关系和承诺。

2) 识别协调机制

识别在项目中协调安全的方法，用于与相关组织共享安全集成的决策和建议。

3) 促进安全协调

确保以合适和有效的方式来解决项目开展期间的意见分歧。

4) 协调安全决策和建议

运用已识别的协调机制，与项目组人员、各工作组及其他组织沟通安全决策和建议。

7.4.2 管理安全控制

管理和维护安全控制措施。通过正确实施和配置，确保信息系统的安全措施在其运行状态下达到了预期目标。

本要求的目标：正确配置和使用安全控制措施。

具体要求如下：

1) 建立安全职责

确保相关负责人的行为职责是得到授权且可核查性，并且传达给组织中的所有成员。无论采用什么安全控制措施，都应该确保管理职责是明确和持续适用的。

2) 管理安全控制措施的配置

对信息系统安全控制机制进行配置管理，制定相关流程和要求。

3) 管理安全意识、培训和教育

像管理其他的意识、培训和教育一样，对所有员工的安全意识、培训和教育进行管理。

4) 定期维护与管理安全控制措施

定期维护和管理安全服务和控制措施，包括保护服务和控制机制免受有意或者无意的损坏，并依据法律和政策的要求进行备案。

7.4.3 监控安全态势

监控安全态势的目的是确保识别和报告所有的安全违规行为、试图违规行为或能够潜在地导致安全

违规的错误。监控安全态势需要监控内部和外部环境中可能影响信息系统安全的所有因素。

在安全集成服务实施过程中要持续关注现有风险，并能对发生的安全事件及时做出安全响应。

本要求的目标：检测和跟踪内部与外部的安全事件，并根据策略进行安全响应；根据安全目标，识别并处理安全态势的变化。

具体要求如下：

1) 分析事件记录

检查安全信息相关的事件记录。识别值得关注的事件，以及与其他事件的关联性。根据风险评估识别出重要的安全风险以及项目《项目实施行为规范》，生成《安全实施风险监控检查记录表》，供在实施过程中重点监控。

2) 监控变化

关注可能影响当前安全状态有效性的任何变化。威胁、脆弱性、影响和风险与信息系统的的核心紧密相关。建立《安全实施风险监控检查记录》等文档。

3) 识别安全事件

确定是否发生了安全事件，识别其详细情况并且在必要时向上级报告。建立《安全事件登记》等文档。

4) 监控安全防护措施

经常检查安全防护措施的运行状态，以便识别出其性能的变化和功能的有效性。建立《边界及安全防护措施检查登记表》等文档。

5) 评审安全态势

定期检查安全措施和相关的安全要求，以识别必要的安全变更。建立《安全配置变更规程》等文档。

6) 管理安全事件响应

制定应急响应计划和快速恢复策略和恢复计划；并定期测试和维护应急响应计划。建立《应急响应计划》等文档。

7) 保存安全监控结果

通过《安全监控过程文档管理制度》体现出怎样归档、归档位置、保管人、使用人等封存和归档安全监控日志、审计报告和分析结果。

7.5 安全保证

7.5.1 建立保证论据

建立保证论据的目的是通过相关的证据清楚地表明客户的安全需求已经得到满足。保证论据是由多种保证证据支持的一系列陈述性保证目标，包括识别和定义保证要求、证据的产生和分析活动以及支持保证要求所需的附加证据活动。另外，收集、整理并展示这些活动生成的证据。

在项目实施过程中的各个关键点均需要验证其是否达到阶段目标。

本要求的目标：项目工作结果和工作过程向客户明确地提供了其安全需求已被满足的证据。具体要求如下：

1) 识别保证目标

依据实施方案中的需求目标来识别保证目标。由客户确定的安全保证目标指明了信息系统需要的信

任等级和安全策略实现的信任等级。保证目标的充分性应该由开发商、集成商、客户和信息系统运维人员共同确定。

2) 制定保证策略

制定安全保证策略的目的是策划和确保安全目标被正确地贯彻和落实。本过程所产生的保证证据将会提供安全措施满足安全风险管理的信任等级。通过制定和颁布安全保证策略，实现对安全保证相关活动的有效管理。质量保证保证了整个流程的贯彻和落实，输出质量保证相关文档。

3) 制定测量准则

安全测量准则有利于安全决策、绩效提升和职责核查。测量安全绩效的目的是基于已识别的测量准则监控安全运行的状态，以便于通过实施纠正措施进行过程改进。测量准则有助于监控保证策略和保证目标的完成。

4) 控制保证证据

在安全集成项目各阶段活动中识别并收集各种安全证据。安全证据应该进行控制和管理，以确保与当前工作结果的通用性和与安全保证目标的关联性。SCM 配置管理，测试和配置管理。

5) 分析保证证据

分析保证证据，以提供满足安全目标的证据的信任等级，从而满足客户的安全需求。通过分析保证证据，可以确定安全建设实施过程和安全验证过程是否充分和完善，以便判断安全机制和安全功能的实现是否令人满意。同时，也确保了安全集成项目结果相对于安全基线而言也是完整的和正确的决策分析。

6) 提供保证论据

向客户提供用于表明与安全保证目标相符合的整体安全保证论据。保证论据应该被评审，以确保保证证据的充分性和满足安全保证目标。

7.5.2 验证和确认安全

确保项目方案得到验证和确认。验证表明项目方案被正确地实施，而确认则证明项目方案是有效的。根据安全要求、体系结构和安全设计方面的信息，通过观察、演示、分析和测试来验证项目方案。通过客户的安全需求和安全目标确认项目方案。

本要求的目标：用事实证明项目方案满足客户的安全需求和要求。具体要求如下：

1) 识别项目方案

分别识别验证和确认活动的目标。这涉及在安全集成项目的整个生命周期内与所有工作组的协调。

2) 定义验证和确认方法

识别待验证和确认项目方案的方法，涉及如何验证和确认每一项安全需求的方法。严格等级用于指明验证和确认工作的细致程度，而且这受到“建立保证论据”中“制定面向所有安全目标的安全保证策略”预期输出结果的影响。

3) 执行验证

通过确认安全要求(包括“建立保证论据”识别的安全保证要求)来验证项目方案是正确的。

4) 执行确认

确认项目方案的目的是表明项目方案能够有效地满足客户的安全需求。有多种方式提供确认证据证明客户安全需求已经得到满足，比如在运行环境或者代表性测试环境中测试项目方案。

5) 获取验证和确认结果

获取并提供验证和确认的结果。验证和确认的结果应该以一种容易理解和使用的方式提供。结果应该能被跟踪，以保持从安全需求到安全要求、项目方案、测试结果的可跟踪性。

7.6 运行维护

7.6.1 自调测服务

自调测工作内容应包括以下方面内容：

- 1) 软件版本确认，软件运行状态检测；
- 2) 硬件版本确认，硬件运行状态检测；
- 3) 相关规则库版本确认，系统配置信息的确认；
- 4) 相关产品的功能项目运行正常，功能可实现；
- 5) 检查施工工艺是否符合标准，设备安装是否到位。

7.6.2 售后服务

网络系统安全集成售后服务工作应由以下几个方面组成：

- 1) 网络系统安全集成远程维护工作；
- 2) 网络系统安全集成现场维护工作；
- 3) 网络系统安全集成交付后期回访工作。

对于客户的维护申请，可以通过远程维护和现场维护两种方式进行处理：

7.6.2.1 远程维护

远程维护工作内容应包括以下方面内容：

- 1) 应通过远程维护确定故障点，提供故障解决方式方法；
- 2) 故障处理后，应完善客户档案，定期回访客户；
- 3) 如故障无法确定或 48 小时内无法解决，应申请现场维护服务。

7.6.2.2 现场维护

现场维护工作内容应包括以下方面内容：

- 1) 应遵守客户相关管理制度，办理入场手续；
- 2) 应对网络系统安全集成系统进行整体检测，进一步确认故障点，确定解决方案；
- 3) 应在系统运行后进行一段时间的观察工作，保证系统的安全、稳定的运行；
- 4) 应清理维护现场，保持现场环境整洁，做好离场工作；
- 5) 应对客户进行必要的培训工作；
- 6) 应填写客户维修记录，并进行客户回访工作。

7.7 培训

培训工作内容应包括以下方面内容：

- 1) 集成方应根据合同要求，针对项目实施内容提供必要的培训；

2) 应制定针对性的培训计划, 按照计划实施培训, 并且对培训效果进行评价。

8 应急响应服务要求

8.1 网络安全应急响应服务概述

8.1.1 应急响应服务过程概述

网络安全应急响应服务是指服务提供方通过制定应急响应计划, 在电信运营企业发生安全事件时提供紧急现场或远程援助, 处理影响网络安全事件的服务, 在网络安全事件发生后对其进行标识、记录、分析和处理, 直到受到影响的业务恢复正常运行。网络安全应急响应服务涵盖了安全事件发生后为维持和恢复网络而进行的一系列活动, 包括准备、检测、抑制、根除、恢复、总结等 6 个阶段。

8.1.2 应急响应服务原则

8.1.2.1 保密性原则

服务提供方应对应急响应服务过程中获知的任何服务对象的系统信息承担保密责任和义务, 不得泄露给第三方单位或个人, 不得利用这些信息进行任何侵害服务对象的行为。

8.1.2.2 规范性原则

服务提供方应要求服务人员依照规范的操作流程进行应急响应服务, 所有服务人员应对各自的操作过程和结果进行详细记录, 最终按照规范的报告格式提供完整的服务报告。

8.1.2.3 最小影响原则

应急响应服务工作应尽可能减少对原系统和网络正常运行的影响, 尽量避免对原有网络运行和业务正常运转产生重大影响 (包括系统性能明显下降、网络阻塞、服务中断等), 如无法避免, 则应向服务对象予以说明, 具体应符合 YD/T 1799-2008 中规定的最小影响原则。

8.2 准备阶段

8.2.1 风险评估

应对网络系统进行风险评估, 识别网络资产、脆弱性及面临的威胁, 确定网络面临的安全风险。

8.2.2 业务影响分析

8.2.2.1 分析业务功能和相关资源配置

应对服务对象的各项业务功能及各项业务功能之间的相关性进行分析, 确定支持各种业务功能的相应网络系统资源及其他资源, 明确相关信息的保密性、完整性和可用性要求。

8.2.2.2 确定网络系统关键资源

应对网络系统进行评估, 以确定系统所执行的关键功能, 并确定执行这些功能所需的特定系统资源。

8.2.2.3 确定网络安全事件影响

应采用如下的定量和 / 或定性的方法,对业务中断、系统宕机、网络瘫痪等信息安全事件造成的影响进行评估,包括:

- 1) 定量分析——以量化方法,评估业务中断、系统宕机、网络瘫痪等可能给组织带来的直接经济损失和间接经济损失;
- 2) 定性分析——运用归纳与演绎、分析与综合以及抽象与概括等方法,评估业务中断、系统宕机、网络瘫痪等可能给组织带来的非经济损失,包括组织的声誉、顾客的忠诚度、员工的信心、社会和政治影响等。

8.2.2.4 确定应急响应的恢复目标

应根据业务影响分析的结果,同时结合不同业务的重要性、业务正常运行时的状态等因素,确定应急响应的恢复目标,包括:

- 1) 关键业务功能及恢复的优先顺序;
- 2) 恢复时间范围,即恢复时间目标(RTO)和恢复点目标(RPO)的范围。

8.2.3 应急响应预案

应急响应预案是在网络安全事件发生之前制定的规范性文件,应当参照相关的法律法规、国家标准、行业标准等进行制定,成为应急响应工作的指导性文件,能够在网络安全事件发生时切实地组织服务提供方和客户相关人员实施应急响应行为,减少事件带来的损失和影响。

服务提供方应当帮助或协助客户的应急响应预案的制定,并协助客户依照预案进行应急响应演练。

8.2.3.1 应急响应预案的编制

应急响应预案应当符合以下要求:

- 1) 符合国家相关法律,国家、行业和所在地区的相关法规、标准的规定;
- 2) 结合客户实际情况和危险性分析情况;
- 3) 有明确、具体的事故预防措施和应急程序,并与其应急能力相适应;
- 4) 明确的应急保障措施,并能满足客户的应急工作要求;
- 5) 预案基本要素齐全、完整,预案附件提供的信息准确;
- 6) 简洁规范,通俗易懂。

应急预案应包括以下基本内容:

- 1) 总则,包括指导思想、编制目的、编制依据、适用范围和工作原则等;
- 2) 应急组织机构,包括领导机构、工作机构、联动机构、现场指挥机构、专家组等;
- 3) 预防与预警机制,包括预测预警系统、预警分级指标、预警发布及解除、预警响应措施等;
- 4) 应急响应,包括预案启动条件、事件通告、先期处置、分级响应、应急结束等;
- 5) 后期处置,包括信息系统重建、应急响应评估与总结、信息发布等;
- 6) 应急保障,包括人力保障、物质条件保障、技术支撑保障等;
- 7) 监督管理,包括宣传教育、培训、演练等;

8) 附则, 包括名词术语和预案解释等;

9) 附件, 包括组织结构关系图、工作流程图、联系人清单表和呼叫树、信息安全事件报告表等。

此外, 应急响应预案还应当根据可能出现的各种网络安全事件编制相应的应急响应场景, 对于各个场景中有别于其他场景的特殊之处、需特别注意之处等进行单独的说明和规定, 如有必要可有针对性地编制子预案。

8.2.3.2 应急响应预案的评审和修订

服务提供方制定应急响应预案后应当交由客户进行评审, 对于客户提出的修改意见等应当进行讨论并修订。通过评审后进行存档备案, 并保证在网络安全事件发生的第一时间启动。

服务提供方应当根据网络安全环境和态势的变化对应急响应预案进行修订, 并结合客户的应急响应演练、网络安全事件等的实际情况, 针对所暴露出的问题、缺陷、隐患, 对应急响应预案进行相应的修改和调整。

8.2.4 制定应急响应策略

8.2.4.1 概述

应急响应策略应提供在业务中断、系统宕机、网络瘫痪等网络安全事件发生后, 快速有效地恢复网络系统运行的方法。这些策略应涉及到在业务影响分析(BIA)中确定的应急响应的恢复目标。

8.2.4.2 系统恢复能力要求

系统恢复能力指在安全事件发生后, 服务提供方协助客户将系统恢复至安全事件发生前运行状态所需的能力, 相关能力应当在应急响应策略中予以明确。系统恢复能力级别应确定为以下能力级别之一:

- 1) 基本支持;
- 2) 备用场地支持;
- 3) 电子传输和部分设备支持;
- 4) 电子传输及完整设备支持;
- 5) 实时数据传输及完整设备支持;
- 6) 数据零丢失及远程集群支持。

8.2.4.3 系统恢复资源的要求

服务提供商在所制定的应急服务策略中应当明确规定:

- 1) 数据备份系统的要求;
- 2) 备用数据处理系统的要求;
- 3) 备用网络系统的要求;
- 4) 备用基础设施的要求;
- 5) 专业技术支持能力的要求;
- 6) 运行维护管理能力的要求;
- 7) 灾难恢复预案的要求。

8.2.4.4 服务方案制定

具体要求如下：

- 1) 服务提供方应在了解服务对象应急需求的基础上制定服务方案。
- 2) 服务方案应根据业务影响分析的结果，明确应急响应的恢复目标，其中包括关键业务功能、恢复的优先顺序以及恢复时间目标和恢复点的范围。
- 3) 服务方案应带有完善的检测技术规范，检测技术规范至少包含检测目的、工具、步骤等内容。

8.2.4.5 人员和工具准备

具体要求如下：

- 1) 服务提供方应根据服务对象的需求准备处置网络安全事件的工具包，包括常用的系统命令、工具软件等；
- 2) 服务提供方的工具包应保存在不可更改的移动介质上，如一次性可写光盘；
- 3) 服务提供方的工具包应定期更新，并有完善的版本控制；
- 4) 服务提供方应能随时调动一定数量的应急服务人员。

8.2.5 服务合同或协议签订

具体要求如下：

- 1) 服务提供方应与服务对象签订应急响应服务合同或协议，明确双方的责任和权利；
- 2) 服务合同或协议应明确服务提供方的保密责任；
- 3) 服务合同或协议应明确哪些类型安全事件的应急响应行为需要系统管理者批准，哪些需要事先批准。

8.3 检测阶段

8.3.1 检测对象、范围及方案确定

- 1) 服务提供方应对出现异常的系统进行初步分析，判断是否真正发生了安全事件；
- 2) 服务提供方应与服务对象共同确定检测对象及范围；
- 3) 检测对象及范围应得到服务对象的书面授权；
- 4) 服务提供方应和服务对象共同确定检测方案；
- 5) 服务提供方制定的检测方案应明确服务提供方所使用的检测规范和检测范围，其检测范围应仅限于服务对象已授权的与安全事件相关的数据，对服务对象的保密数据信息未经授权不得访问；
- 6) 服务提供方制定的检测方案应包含在实施方案失败时的应变和回退措施；
- 7) 服务提供方应与服务对象充分沟通，并预测应急处理方案可能造成的影响。

8.3.2 检测实施

具体要求如下：

- 1) 服务提供方应按照检测方案实施检测。
- 2) 检测应包含但不限于以下几个方面：

a) 收集并记录系统信息，特别是在执行备份的过程中可能遗失或无法捕获的信息，如所有当前网络连接、所有当前进程、当前登陆的活动用户、所有处于打开状态的文件、其他所有容易丢失的数据，如内存和缓存中的数据。

b) 备份被入侵的系统，至少应备份已确认被攻击了的系统及系统上的用户数据。

c) 隔离被入侵的系统。把备份的文件传到与生产系统相隔离的测试系统，并在测试系统上恢复被入侵系统，或者断开被破坏的系统并且直接在其上进行分析。

d) 查找其他系统上的入侵痕迹。其他系统包括处于同一 IP 地址段或同一网段的系统、处于同一域的其他系统、具有相同网络服务的系统、具有同一操作系统的系统等。

e) 检查防火墙、IDS 和路由器等设备的日志，分析哪些日志信息源于以前从未注意到的系统连接或事件，并且确定哪些系统已经被攻击。

f) 确定攻击者的入侵路径和方法。分析系统的日志或通过使用工具，判断攻击者的入侵路径和方法。

G) 确定入侵者进入系统后的行为。分析各种日志文件或借用一些检测工具和分析工具，确定入侵者如何实施攻击并获得系统的访问权限。

3) 服务提供方的检测工作应在服务对象的监督与配合下完成。

4) 服务提供方应配合服务对象，将所检测到的安全事件向有关部门和人员通报或报告。

8.4 抑制阶段

8.4.1 抑制方法确定及认可

具体要求如下：

1) 服务提供方应在检测分析的基础上确定与安全事件相应的抑制方法。

2) 在确定抑制方法时，需要考虑：

a) 全面评估入侵范围，入侵带来的影响和损失；

b) 通过分析得到的其他结论，例如入侵者的来源；

c) 服务对象的业务和重点决策过程；

d) 服务对象的业务连续性。

3) 服务提供方应告知服务对象所面临的首要问题。

4) 服务提供方所确定的抑制方法和相应的措施应得到服务对象的认可。

5) 在采取抑制措施之前，服务提供方应与服务对象充分沟通，告知可能存在的风险，制定应变和回退措施，并与其达成协议。

8.4.2 抑制实施

具体要求如下：

1) 服务提供方应严格按照相关约定实施抑制，不得随意更改抑制措施和范围，如有必要更改，须获得服务对象的授权。

2) 抑制措施应包含但不限于以下几个方面：

a) 监视系统和网络活动；

- b) 提高系统或网络行为的监控级别;
- c) 修改防火墙、路由器等设备的过滤规则;
- d) 尽可能停用系统服务;
- e) 停止文件共享;
- f) 改变口令;
- g) 停用或删除被攻破的登录账号;
- h) 将被攻陷系统从网络断开;
- I) 暂时关闭被攻陷系统;
- J) 设置陷阱, 如蜜罐系统;
- K) 反击攻击者的系统。

3) 服务提供方应使用可信的工具进行安全事件的抑制处理, 不得使用受害系统已有的不可信文件。

8.5 根除阶段

8.5.1 根除方法的确定和认可

具体要求如下:

- 1) 服务提供方应协助服务对象检查所有受影响的系统, 在准确判断安全事件原因的基础上, 提出根除的方案建议;
- 2) 由于入侵者一般都会安装后门或使用其他的方法以便于在将来有机会侵入该被攻陷的系统, 因此在确定根除方法时, 需要了解攻击者是如何入侵的, 以及与这种入侵方法相同和类似的各种方法。
- 3) 服务提供方应明确告知服务对象所采取的根除措施可能带来的风险, 制定应变和回退措施, 并获得服务对象的书面授权。
- 4) 服务提供方应协助服务对象进行根除方法的具体实施。

8.5.2 根除实施

具体要求如下:

- 1) 服务提供方应使用可信的工具进行安全事件的根除处理, 不得使用受害系统已有的不可信文件;
- 2) 根除措施应包含但不限于以下几个方面:
 - a) 改变全部可能受到攻击的系统的口令;
 - b) 去除所有的入侵通路和入侵者做的修改;
 - c) 修补系统和网络漏洞;
 - d) 增强防护功能, 复查所有防护措施(如防火墙)的配置, 并依照不同的入侵行为进行调整, 对于受防护或者防护不够的系统增加新的防护措施;
 - e) 提高检测能力, 及时更新诸如 IDS 和其他入侵报告工具等的检测策略, 以保证将来对类似入侵进行检测;
 - f) 重新安装系统, 并对系统进行调整, 包括打补丁、修改系统错误等, 以保证系统不会出现新的漏洞。

8.6 恢复阶段

具体要求如下：

- 1) 服务提供方应告知服务对象一个或多个能从安全事件中恢复系统的方法，以及每种方法可能存在的风险。
- 2) 服务提供方应与服务对象共同制定系统恢复的方案，根据抑制和根除的情况，协助服务对象选择合理的恢复方法。恢复方案涉及到以下方面：
 - a) 如何获得访问受损设施或地理区域的授权；
 - b) 如何通知相关系统的内部和外部业务伙伴；
 - c) 如何获得安装所需的硬件部件；
 - d) 如何获得装载备份介质；
 - e) 如何恢复关键操作系统和应用软件；
 - f) 如何恢复系统数据；
 - g) 如何成功运行备用设备。
- 3) 如果涉及到涉密数据，确定恢复方法应遵守相关的保密要求。
- 4) 服务提供方应按照系统的初始化安全策略恢复系统。
- 5) 恢复系统时，应根据系统中各子系统的重要性，确定系统恢复的顺序。
- 6) 系统恢复过程应包含但不限于：
 - a) 利用正确的备份恢复用户数据和配置信息；
 - b) 开启系统和应用服务，将受到入侵或者怀疑存在漏洞而关闭的服务，修改后重新开放；
 - c) 将恢复后的系统连接到网络。
- 7) 对于不能彻底恢复配置和清除系统上的恶意文件，或不能肯定系统经过根除处理后是否已恢复正常时，应选择重建系统。
- 8) 服务提供方应协助服务对象验证恢复后的系统是否运行正常、对重建后的系统进行安全加固，并建立系统快照。

8.7 总结和报告阶段

具体要求如下：

- 1) 服务提供方应及时检查安全事件处理记录是否齐全，是否具备可追溯性，并对事件处理过程进行总结和分析。
- 2) 应急处理总结的具体工作包括但不限于：
 - a) 事件发生原因分析；
 - b) 事件现象总结；
 - c) 系统的损害程度评估；
 - d) 事件损失估计；
 - e) 形成总结报告；
 - f) 相关工具和文档（如记录、方案、报告等）归档。
- 3) 服务提供方应向服务对象提供完备的网络安全事件处理报告。

- 4) 服务提供方应向服务对象提供网络安全方面的建议和意见，必要时指导和协助服务对象实施。
- 5) 服务提供方应告知服务对象可能涉及法律诉讼方面的要求或影响。

9 安全培训服务要求

9.1 概述

安全培训服务是指针对电信网和互联网的安全管理、建设、运行维护等与网络和信息安全相关的岗位人员所开展的，以提高安全意识、安全素质和安全技能为目的教育培训活动。

安全培训服务流程一般包括培训需求分析、培训计划制定、培训前准备、培训实施、培训效果评价等 5 个环节，每个阶段都应输出相应的文档/记录，安全培训服务流程如图 2 所示。如果培训需求相对比较明确，在培训需求分析阶段可以不用编制单独的培训需求分析报告。



图2 安全培训服务流程

9.2 培训需求分析

9.2.1 需求分析的目的及内容

在培训需求分析阶段应明确培训的目的、培训的对象、培训要求等方面内容。安全培训需求分析应考虑以下几方面的需求：

- 1) 政策法规需求：为了满足国家政策、法规对于网络安全保障的要求，首先应熟悉了解国家和主管部门所制定的法律和规章制度；
- 2) 管理需求：主要是通过培训加深员工对企业相关安全规章制度、策略的了解，以便规范和指导安全相关工作；
- 3) 岗位需求：主要是通过培训提高安全相关岗位任职人员的岗位技能，包括管理能力和技术能力，例如对相关的安全管理制度与规定的了解、对于相关设备的操作维护能力、安全攻防技术等；
- 4) 安全意识教育：即企业对员工的需求，员工需要具有安全意识和安全责任，能够及时发现安全隐患，主动维护企业信息资源等各方面安全，并自觉规范其安全行为。

9.2.2 培训需求分析方法

针对不同内容，需求分析可以采用但不限于以下方法：

- 1) 访谈法：通过与被访谈人进行面对面的交谈来获取培训需求信息。可与问卷调查法相结合使用。访谈法应首先确定访谈目标、访谈对象和访谈方式。
- 2) 问卷调查法：以标准化的问卷形式来获取调查对象的实际情况。当需要进行培训需求分析的人较多，且时间较为紧急时采用此方法。

3) 观察法：通过现场观察，获取信息数据，发现问题。观察法应明确观察所需要的信息和观察对象，确保观察对象对要进行观察的员工所进行的工作有深刻的了解，熟知相关行为准则，以及观察期间不干扰被观察者的正常工作，注意观察的隐蔽性。

4) 关键事件法：通过考察工作过程和活动情况来发现潜在的培训需求。关键事件法的实施应确保已制定重大事件记录的指导原则并建立记录媒介，如工作日志等，并对记录进行定期分析或审计。

5) 绩效分析法：通过与绩效标准的对比和绩效考核来获取差距，进而找出原因和相应的培训内容需求。绩效分析法应首先明确以规定的标准作为考核基线，明确关键业绩指标，找出未达到理想业绩水平的原因，确定通过培训能否达到业绩水平。

6) 经验判断法：指一些具有一定的通用性或规律性，可凭经验加以判断的培训需求。经验判断法要求判断者具有丰富的经验。

7) 专项测评：通过高度专业化、深层次的测评方法，获取更加具体而系统的信息。专项测评需要有大量的专业知识作支撑。

8) 胜任能力分析法：通过对员工所具备的知识、技能、态度和价值观等确定其是否能够胜任某一工作。胜任能力分析法应明确职位任职者应具备的知识、技能、态度和价值观，以及被评估者目前的能力水平。

9.2.3 培训需求分析报告

在制定培训需求调查计划并实施调查后，应对调查信息进行归类、整理、分析和总结，撰写培训需求分析报告。培训需求分析报告应包含以下几点内容：

- 1) 需求分析实施背景，即产生培训需求的原因或培训动议；
- 2) 开展需求分析的目的和性质，此活动前是否有过类似的分析，如果有的话，应明确以往的分析中存在哪些缺陷与失误；
- 3) 概述需求分析的方法和过程；
- 4) 阐明分析结果；
- 5) 解释、评论分析结果并提供参考意见；
- 6) 附录，包括收集和分析资料用的图标、问卷、部分原始资料等；
- 7) 报告提要，提要应对报告要点进行概述，简明扼要。

9.3 培训计划

9.3.1 培训计划考虑因素

制定培训计划前应考虑以下几点重要因素：

- 1) 目标：根据实际需求分析，明确培训的目标；
- 2) 预算：预算的确定、分配方式，以及预算与计划可能存在的冲突；
- 3) 培训类型：外部老师的内部培训或参加外部企业组织的培训；
- 4) 培训方式：如讲授法、演示法、研讨法、视听法、案例研究法和模拟教学法等，各种方法可配合使用；
- 5) 培训时间：如长期培训还是短期培训，分阶段实施还是集中培训，具体培训时间安排等；

- 6) 培训级别：主要可分为公司级别和部门级别。
- 7) 培训计划是否能加深员工对培训的了解，并增加员工对培训计划的兴趣和承诺；
- 8) 培训计划是否获得管理者的参与、支持与协助；
- 9) 计划时间是否可能影响组织的运作；
- 10) 培训计划成本是否符合组织的资源限制。

9.3.2 培训计划制定

培训计划制定应包含以下内容：

- 1) 确立培训目标：由培训需求分析给出培训的总体目标；
- 2) 培训目标分类：当培训需求包含多种类型时，应将培训目标进行分类，确定每类培训的目标；
- 3) 设计培训计划大纲及期限：为培训计划确定基本结构、项目和时间阶段的安排；
- 4) 明确各培训项目信息：包括具体时间、培训类型、培训名称、培训方式、参与人员范围、重点参加人员等；
- 5) 制定控制措施：通常采取登记、例会汇报、流动检查等手段监督培训计划的进展；
- 6) 决定评估方法：可采用命题作业、书面测验、受训人培训报告等方式综合评价受训人的培训效果；
- 7) 培训预算规划：根据以上制定内容所涉及的经费进行估算；
- 8) 与部门及领导讨论：讨论培训计划，并获取相应部门及领导的支持，并根据讨论结果修改培训计划；
- 9) 培训计划确认：培训服务供需双方应当对培训计划进行确认。在制定培训计划后，应及时通知相关人员做好培训准备工作。

9.4 培训准备工作

培训前的准备工作包括确定培训内容、编写培训讲义、准备培训环境等。培训前的准备工作是保证培训效果的一个关键环节，因此培训服务双方在培训内容实施前应当对培训准备工作进行确认。

9.4.1 确定培训内容

培训内容设计应符合培训需求，以达到培训目的为基本要求，综合考虑市场、组织机构、培训人和受训人等实际情况，选择适当的培训类型和培训方式，以求获得最佳的培训效果。

培训内容的确定应至少满足以下几点要求：

- 1) 明确培训基准：包括标准、制度、规范等，且应及时获取最新版作为培训的指导文件；
- 2) 培训内容具有针对性：培训内容应针对需求，以解决需求为培训目的，围绕培训目的设计培训内容；
- 3) 培训内容具有实用性：培训内容应与当前实际情况和需求相关结合，合理设计培训内容，而不是简单沿用以往培训内容。

根据培训需求及培训类型的不同，安全培训内容应包括但不限于以下部分或全部内容：

- 1) 通信网络安全的相关政策、法规要求：包括国家颁布的法律法规、工信部制定的通信网络安全规章制度、管理办法等。

2) 通信网络安全防护标准：工信部颁布的通信网络安全防护系列行业标准。

3) 网络安全基础知识：包括基本概念、模型、访问控制、密码技术、数据保护、入侵检测、安全审计、冗余备份、应急响应等。

4) 安全攻防技术：包括基本的主机扫描、端口扫描、漏洞扫描、配置核查方法，以及网络渗透测试基础。

5) 网络安全管理：结合通信网络安全防护标准要求，以及 ISO27000 标准对于信息安全管理的要求，结合运营商安全管理规定，培训安全管理的基本要求。

6) 岗位技能培训：与安全相关岗位人员的岗位技能培训，例如：针对安全管理人员进行安全管理的政策法规及标准的培训；针对安全运行维护人员进行安全配置基线要求及配置方法的培训；针对应急响应人员进行应急响应预案的培训等。

7) 针对具体设备的操作培训：根据培训需求，培训内容也可以是针对某个具体设备的操作培训，例如防火墙、IDS 等设备的安全配置方法；

8) 安全测试工具的使用：针对常用安全测试工具使用方法的培训，例如脆弱性扫描、配置核查或者渗透测试工具的使用方法及技巧的培训。

总之，培训内容的选择要求根据运营商的实际需求，考虑时间、成本及其它条件，选择合适的培训内容，避免大而不全、或者虚而不实，力求实效。

针对确定的培训内容应当形成相应的培训讲义。培训讲义应准确反映培训内容，便于培训学员学习、理解。

9.4.2 准备培训环境

针对不同的培训内容需要，培训服务商应在培训前搭建相应的培训环境。培训环境包括方便用于培训的培训场地，也包括用于培训的试验环境、演示设备及培训中需要使用的相关工具、材料等，包括但不限于：

- 1) 带有投影设备的培训教室；
- 2) 网络试验环境；
- 3) 安全攻防试验环境；
- 4) 安全攻防测试工具；
- 5) 操作培训使用的样机；
- 6) 计算机等辅助设备。

有些培训环境可能需要被服务单位协助准备，双方应沟通确认。

9.5 培训实施

培训的实施应按照双方确认的培训计划进行，包括培训的内容、培训的人员、培训的地点、时间、培训方式、进度等都应当按照计划进行实施。如果在实施过程中需要对培训的内容、时间、进度、方式、培训老师等进行调整，需要双方协商达成一致，并且进行记录。

培训过程中应当填写培训记录。培训记录内容一般包括培训的时间、地点、培训内容、参加人员等信息，并且要求参加人员填写培训签到表。培训记录应当保存归档。

9.6 培训效果评价

9.6.1 培训评估分类

培训评估应贯穿于整个培训过程，可分为以下三类：

- 1) 训前评估：包括培训需求确认的科学性、培训对象当前的信息、培训计划的合理性、培训资源的合理配置、培训效果测定方式的有效性等。
- 2) 训中评估：包括培训计划的有效实施、培训执行情况的反馈和调整、培训进度与中间效果等。
- 3) 训后评估：包括培训目标达成情况、培训效果效益综合情况、受训人业绩改善等。

9.6.2 培训效果评估方法

应从以下 4 个层面对培训效果进行评估。其中前面两种方法用于对短期培训效果进行评价，后两种方式用于对组织中长期培训效果的评价。

- 1) 反映评估：在课程刚结束时实施，通过问卷调查了解受训人对培训项目的主观感觉和满意程度。
- 2) 学习评估：一般在课程刚结束时实施，主要通过测评、考核等方式评价受训人通过培训对所学知识深度与广度的掌握程度。
- 3) 行为评估：用于在组织中对中长期的培训效果进行评价，主要通过主管、同事、客户等周围人员的评价和评估人的观察来评估受训人在工作中行为的改善程度。
- 4) 结果评估：用于在组织中对中长期的培训效果进行评价，主要通过培训后引起的个人业绩、组织业务结果的变化情况对培训效果进行评估。

9.6.3 培训评估的实施

依据培训评估的分类和评估层次，培训评估应按照以下步骤实施：

- 1) 确定评估计划，结合培训需求分析和培训计划，明确评估目的和评估对象，评估对象应包括培训课程、培训方式、培训人和受训人等；
- 2) 收集整个培训周期中的相关数据；
- 3) 制定培训评估计划，结合培训计划中设计的评估方法，明确评估层次及评估衡量方法；
- 4) 分析评估资料，得出评估结论；
- 5) 撰写评估报告，报告中应说明已获得的培训效果，以及培训项目的不足之处，如内容不适当、授课方式不适当、受训人本身缺乏积极性等，为以后的培训设计和调整提供参考依据；
- 6) 沟通培训结果：包括与培训主管、管理层、受训人员和受训人领导的沟通。

9.6.4 培训评估报告

培训评估报告应包括但不限于以下几点内容：

- 1) 培训简要说明；
- 2) 阐述评估实施方法和过程；
- 3) 评估结果；
- 4) 分析评估结果及建议；
- 5) 附录。

10 符合性评测服务要求

10.1 概述

符合性评测是指针对电信网和互联网的网络单元进行检查,评价其是否符合相关安全防护标准的规定要求。

符合性评测应依据相应的网络安全防护测评要求,对被测网络单元的网络安全、设备安全、业务应用安全、物理环境安全和管理安全等几个方面进行检查。

符合性测评服务过程包括测评准备工作、测评方案制定、测评实施、证据保存与确认和测评报告 5 个环节。

10.2 测评准备工作

具体要求如下:

- 1) 应通过系统调研,明确测评的范围。调研内容应包括业务系统及功能、网络架构及支撑环境、系统边界、主要的设备及软件、数据和信息、安全防护级别、已经采取的安全措施、相关的人员和管理制度等。
- 2) 应通过调研分析确定测评所适用的网络安全防护标准及防护级别。
- 3) 上述调研内容完成后,应形成需求分析报告并且得到双方的确认。
- 4) 测评方应事先准备好测评所用的测评工具。
- 5) 测评双方应签订测评服务合同,明确双方的责任和义务。

10.3 测评方案制定

具体要求如下:

- 1) 测评服务方应确定相应的测评标准,在此基础上编制符合性测评方案;
- 2) 测评方案应包含测评依据、测评方法、使用的测评工具以及测评内容;
- 3) 测评方案中应对测评工作可能带来的安全风险进行分析,制定相应的风险处置预案并且得到委托方的认可;
- 4) 测评方案应明确测评服务的工作计划,包括测评项目团队及人员安排、测评时间进度安排、需要协调的事项等;
- 5) 测评方案应得到双方的确认。

10.4 测评实施

具体要求如下:

- 1) 测评方应按照相应的网络安全防护测试标准、所确认的测试方案进行测试;
- 2) 针对不同的测评内容,符合性评测应采用人员访谈、查阅资料、现场检查和技术检查等测评方法,对被测网络系统、网络设备、业务应用、配套物理环境设施、相关人员及管理制度是否满足相应安全防护标准要求进行检查;
- 3) 测评人员应严格遵守被测单位的安全管理制度要求;

- 4) 测评工作不应影响被测网络系统的正常运行，不对系统业务带来影响；
- 5) 测评过程中应注意收集及保存获得的证据。

10.5 安全证据确认与保存

具体要求如下：

- 1) 应对测评过程中收集的安全证据进行确认和保存；
- 2) 应确保测评过程中的各种现场记录可复现，并作为产生歧义后解决问题的依据；
- 3) 测评过程中应及时将评估结果向被评估方进行反馈和确认；
- 4) 在报告及总结阶段，应对测评过程中的各种现场记录进行再次确认；
- 5) 对项目实施过程中收集到的资料，测评方应严格遵守知识产权条款，按照保密协议要求保护被评估方利益和商业、技术秘密：包括针对项目所开发的软件程序、安全服务文档，被评估方提供的所有业务、技术资料。

10.6 测评报告要求

具体要求如下：

- 1) 测评报告应详尽、准确地反映测评结果；
 - 2) 对于测评中发现的问题或不符合项，在测评报告中应给出合理的安全处置建议；
 - 3) 测评单位应具有文档控制程序，对于测评过程中形成的相关文档，应规定其标识、存储、保护、检索、保存期限以及处置所需的控制；
 - 4) 测评报告的发放应得到审核和批准；
 - 5) 测评报告的分发应按照保密协议要求得到严格的控制，除非得到被测评单位的许可，测评单位不应将测试报告及测试结果透露给其它组织或个人；
 - 6) 测评报告及测评结果应得到被评测方的确认。
-