第 5 章

网络安全同行评估技术和方法

同行评估通常采用的方法主要包括现场巡视、现场观察、文档审阅和人员访谈等。对于网络安全领域，还可考虑采用配置核查、安全测试和沙盘推演等方式进行补充，或者以等级测评、实战演习等报告成果作为同行评估的输入。

5.1 同行评估技术和方法

同行评估通常采用的方法主要包括现场观察、文档审阅和人员访谈等。对于网络安全领域，还可考虑采用配置核查、安全测试和沙盘推演等方式进行补充，或者以等级测评、实战演习等报告成果作为同行评估的输入。在工作方式上，也可以采用创新工坊、挑战会等形式。评估方应该本着审慎的原则，在开展现场评估时，一般不安排涉及网络和系统的配置核查和安全测试等风险评估内容，避免执行系统数据变更操作；确有必要时，应与受评方对口人进行协商，明确具体操作步骤并制订风险控制措施，由受评方对口人进行风险分析和把握，根据受评方的有关操作规程和评估项需求对受评网络和系统进行核查操作。如有近期类似的测试报告，应尽可能采用，作为现场观察的输入。

1. 现场观察及应用简述

评估人员通过观察工作被如何执行、执行得如何、其后果如何，并询问工作是否可以被进一步提高或改善，然后确定一组事实，每一个事实都是一个偏差或未被做好的事，并且给出判断的理由，即这样做将会如何，最后编制形成观察报告。

评估人员进行现场观察之前，应准备好评估作业指导书、评估结果记录表格等。开展现场观察时，应根据受评方的实际情况，在受评方对口人的陪同下，到系统运行现场通过实地观察相关人员的操作行为、技术设施和物理环境状况，判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况，评估其是否符合相应评估项的安全要求。

针对不同等级系统的具体评估对象，在评估实施时有不同的强度要求。总体而言，在进行现场观察时，应参照评估作业指导书选定的评估项基本要求，判断实地观察到的情况与制度和文档中说明的情况是否一致，核查相关设备、设施的有效性和位置的正确性，与系统设计方案的一致性。

现场观察完成后，应做好现场观察评估结果记录，以评估项为单元，准确描述每一个事实偏差，并与受评方对口人沟通确认，写入观察报告。

2. 文档审阅及应用简述

文档审阅是指评估人员通过对受评方支撑网络与信息系统安全建设与运维的安全管理制度、工作记录等文档的核查，获取证据以证明受评方网络与信息系统的安全保护要求是否全面，安全保护规定是否得到执行，是否有更有效的实践可以应用。

评估人员在开始文档审阅之前，应根据自己承担的评估任务需要，取得受评方对口人的支持，准备好待审阅的主要文档，例如受评方网络安全策略、安全方针文件、安全管理制度、安全管理的执行过程文档、系统设计方案、网络设备的技术资料、系统和产品的实际配置说明、网络安全设备或软件的安全性测试报告、系统的各种运行记录文档、机房建设相关资料、机房出入记录等过程记录文档。

在文档审阅中，侧重进行以下几个核查工作：

（1）核查该任务评估作业指导书需评估的有关制度、策略、操作规程等文档是否齐备。

（2）核查是否有完整的制度执行情况记录，如机房出入登记记录、电子记录、关键设备使用登记记录等。

（3）核查安全策略以及技术相关文档是否明确说明了相关技术要求的实现方式。

（4）对上述文档进行审核与分析，核查其完整性和这些文档之间的内部一致性。

针对不同等级系统的具体评估对象，在评估实施时有不同强度要求。总体而言，在进行文档审阅时，应参照评估作业指导书选定的评估项基本要求，检查文档是否齐备且完整，并且所有文档之间是否保持一致性。要求有执行过程记录的，过程记录文档的记录内容应与相应的管理制度和文档保持一致。与实际情况保持一致，安全管理过程应与系统设计方案保持一致且能够有效地对系统进行管理。

文档审阅完成后，应做好文档审阅评估结果记录，以评估项为单元，准确描述每一个事实偏差，并与对口人沟通确认，写入观察报告。

3. 人员访谈及应用简述

人员访谈是指评估员通过与受评方对口人进行交流、讨论等活动，获取事实证据以证明网络与信息系统的安全保护措施、管理体系及其运行有效性以及是否追求卓越。

在访谈开始前，评估人员应准备好现场评估工作计划、评估作业指导书以及评估

结果记录表格等。访谈评估时，评估员与受评方对口人进行交流、讨论等活动，获取相关证据，了解有关信息。评估员应侧重识别和发现受评方的实践与评估项的要求存在的事实偏差以及偏差原因、相关补偿措施和潜在风险等。在访谈范围上，不同评估任务有不同的要求，一般应基本覆盖所有的安全相关人员类型，在分类基础上抽样。具体可参照 3.5 节介绍的同行评估典型任务作业指导书要点。访谈完成后，应做好访谈评估结果记录，以评估项为单元，准确描述每一个事实偏差，并与对口人沟通确认，写入观察报告。

4. 配置核查及应用简述

配置核查是指评估人员通过对受评网络和系统进行观察、查验、分析等活动，获取证据以证明受评网络和系统安全保护措施是否有效。

评估人员在进行配置核查之前，应准备好评估作业指导书、评估结果记录表格等。在配置核查中，应侧重进行以下工作：

（1）根据评估结果记录表格内容，利用上机验证的方式核查应用系统、主机系统、数据库系统以及各设备的配置是否正确，是否与文档、相关设备和部件安全配置要求保持一致，对文档审阅的内容进行核实（包括日志审计等）。

（2）如果系统在输入无效命令时不能完成其功能，应测试其是否对无效命令进行错误处理。

（3）针对网络连接，应对连接规则进行验证。

针对不同等级系统的具体评估对象，在开展配置核查时有不同强度要求。总体而言，在进行配置核查时，应参照评估作业指导书选定的评估项基本要求，评估其实施的正确性和有效性，核查配置的完整性和准确性，测试网络连接规则的一致性，测试系统是否符合可用性和可靠性的要求。

配置核查完成后，应做好配置核查评估结果记录，以评估项为单元，准确描述每一个事实偏差，并与对口人沟通确认，写入观察报告。

配置核查也可能影响受评方网络与信息系统正常运行。在进行现场评估时，如果需要对设备和系统的安全策略配置和安全功能进行核查验证，部分配置核查内容会涉及对设备的操作，可能对系统的运行造成一定的影响，甚至存在误操作的可能。因此，如确有必要进行此类配置核查，评估方需要相应地拟定风险控制措施，并与受评方对口人事先协商一致。

5. 安全测试及应用简述

安全测试是指评估人员使用预定的方法/工具使受评网络和系统产生特定的行为，通过查看、分析这些行为的结果，获取证据以证明受评方网络与信息系统安全保护措施是否有效。

评估人员在进行安全测试前，应准备好评估作业指导书、评估结果记录表格等。在进行安全测试时，应在受评方对口人陪同下，按照事先编制和沟通确认的安全测试风险防范要求进行如下工作：

（1）根据评估作业指导书，利用技术工具对系统进行测试，包括基于网络探测和基于主机审计的漏洞扫描、渗透性测试、功能测试、性能测试、入侵检测和协议分析等。

（2）备份测试结果。

针对不同等级系统的具体评估对象，在评估实施时有不同的强度要求。总体而言，在进行安全测试时，应参照评估作业指导书选定的评估项基本要求，针对服务器、数据库管理系统、网络设备、安全设备、应用系统等进行漏洞扫描，针对应用系统完整性和保密性要求进行协议分析，渗透测试应包括基于一般脆弱性的内部和外部渗透攻击，针对物理设施进行有效性测试。

安全测试完成后，应做好安全测试评估结果记录、测试完成后的电子输出记录、备份的测试结果文件等，以评估项为单元，准确描述每一个事实偏差，并与对口人沟通确认，写入观察报告。

安全测试可能影响受评方网络与信息系统正常运行。在进行现场评估时，如果使用一些技术测试工具进行漏洞测试、性能测试甚至渗透测试等，可能会对系统的负载造成一定的影响，其中漏洞测试和渗透测试可能对系统数据造成一定破坏。因此，必须慎重选择和确定安全测试的必要性、测试内容、测试工具、测试作业步骤和风险控制与应急处置措施。在同行评估中，建议尽可能不重新实施安全测试，而要利用已有的最新安全测试结果。

6. 沙盘推演及应用简述

沙盘推演是核能行业同行评估中采用的评估方法之一。在核电工程建设领域，利用沙盘推演方法，可以通过对项目场景的实战化演练，在现实方案、进度和资源配置的基础上，梳理和完善实施方案，深入剖析风险与挑战，借助行业专家经验，以多视角识

别风险并开展逐级分析，提出解决方案或建议，进而促进项目风险管控。

近年来，沙盘推演在网络安全领域也逐步得到应用。应用沙盘推演，通常是利用实战攻防演习的成果，在攻击路线、攻击手段等方面的有效性已被证实的基础上，对无法进行实战演习的关键信息基础设施系统或特定场景，评估真实网络攻击或潜在网络安全风险可能对受评方的网络安全产生的实际影响，包括经济损失、声誉损失和可能的社会影响等，同时对攻防过程中受评方的应急响应有效性进行全过程评估。

评估方如果认为需要组织沙盘推演，应与受评方共同进行推演方案的策划和准备，基本思路是：在现场评估进入到一定深度和中后期阶段，汇总收集各评估领域初步发现和识别的主要业绩偏差（待改进项），从中选定受评方重要的网络信息系统或关键信息基础设施系统作为推演攻击目标，识别其中风险较大或防守薄弱的攻击场景和攻击切入点，拟定推演攻击思路、路径、方式、方法和具体手段，形成不同组合的推演攻击方案。推演攻击方案应针对已评估发现的受评方网络安全防护短板弱项和风险隐患点，应具有理论和现实的可行性。在推演攻击时，评估队首先讲解攻击方案及其可行性，包括技术可行性、攻击可能投入的时间、人力和物力等，然后受评方进行提问和质询，并报告防守方案、应对措施和应急处置方案等，双方就不同组合的推演攻击方案和防守措施等进行对峙抗辩，就其中的风险、隐患、潜在后果以及防护措施等进行交流探讨。评估方的领队和队长以及受评方主管部门和分管领导作为评估专家组成员认真旁听、客观分析、科学研判，在推演攻击的过程中，本着“有则改之、无则加勉”的原则，全面、深入和系统地发现和研判受评方潜在的网络安全风险短板弱项，积极研判评估推演攻击成功后可能对受评方业务连续性产生的影响，包括可能造成的经济损失、声誉损失和社会影响等，为最后确定重要的待改进项、编制总体评估报告和完善应急处置响应措施等形成双方的共识。在沙盘推演结束后，应做好沙盘推演结果记录，进一步验证、确认和补充修订已发现的待改进项，尽可能提出相应的改进意见和建议。

7. 创新工坊及应用简述

创新工坊是一种基于创新设计思维，左右脑思考相结合，面向产品设计、服务创新和解决复杂问题，以积极、开放和创新的心态，按照一定的研讨框架和问题清单，规范、高效地探索和寻求创新解决方案的一套团队学习和创新的头脑风暴流程、工具和方法论。

在同行评估工作过程中，为了快速和精准地抓住关键问题或薄弱环节，提高评估作业指导书的编制质量和效率，积极调动全体评估员以及受评方对口人在评估工作中的积极性和创造性，切实达成“同行互评、互学互促”以有效提升评估工作效果的目标，在同行评估的入场培训、评估作业指导书编制、网络安全领导力研讨、总体评估中寻求待改进项的解决方案建议等场景或环节中，均可以考虑采用创新工坊的评估形式。

在开展创新工坊之前，评估方的领队或队长应与受评方负责人充分沟通，围绕评估工作的预定目标，识别和确定研讨主题，通过对该主题的初步研讨，进一步识别主要问题或问题的主要方面，确定问题研讨和分析模板，确定研讨团队成员和分组名单，确定创新教练、速记员和创意提炼师，准备场地环境和设备设施，准备问题导入材料等相关 PPT 文件。在创新工坊进行过程中，教练应在问题背景导入基础上直击问题清单，有序规范地调动团队每个成员进行创新思考和互动研讨，通过涂鸦思考、创意提炼、观点累加、去伪存真、分类归类、优先排序和总结展示等方式，共同探寻、筛选和提炼问题的解决方案。在创新工坊结束后，将相关解决方案的行动清单分解落实到每个评估员或受评方对口人，并且将这些研讨成果融入评估作业指导书编制、各评估子领域和领域事实偏差发现、问题根本原因分析和改进措施拟定等具体评估工作之中。

8. 挑战会及其应用

挑战会是同行评估中经常使用的一种沟通事实、确认偏差和达成共识的会议形式。挑战会可以是评估队内部成员之间的挑战，也可以是评估员与受评方对口人之间的挑战，旨在以事实为依据，以严谨的逻辑分析为主线，对评估队成员和受评方对口人提出的观点或意见进行交流和辩论，达到去伪存真、去粗取精等目的。

采用挑战会这种说法和会议形式，归根到底就是倡导同行评估中的各项工作成果都要“经得起挑战”。一方面，要求评估队成员在开展评估工作的全过程中充分发挥自己的专业和经验优势，以网络安全业绩目标为导向，以评估准则的基本要求为参考，着力发现受评方具体的事实偏差，坚持实事求是而非凭借个人印象，有理有据地如实、准确记录事实偏差和分析问题，得出的评估结论和评估建议经得起评估队成员和受评方对口人的质疑和挑战；另一方面，挑战会也是倡导一种严格、审慎、细致和务实的评估工作作风以及积极、开放和创新的工作氛围。

5.2 同行评估常用文件编制要点

5.2.1 编制和审阅先期文件包

编制和审阅先期文件包(AIP)是评估准备阶段最基础的工作。先期文件包由评估方提出需求,受评方具体负责编制并在入场前提交评估队。其目的是让评估队在开始现场评估之前,尽可能全面而概要地了解受评方业务和网络总体情况,为评估员编制现场评估任务作业指导书提供基本输入。先期文件包一般包括以下内容。

1. 受评方基本情况

受评方基本情况主要包括受评方企业性质、发展目标、核心业务、地域范围、管理架构、组织结构、制度体系、安全生产概况、内外部接口(如上级单位、业务或行业主管部门、下属单位、主要合作单位、主要供应商或客户)等信息。受评方可以列出其外部门户网站,以此为基础补充其他必要的信息或已有的相关信息。

2. 受评方网络安全总体情况

受评方网络安全总体情况主要包括受评方网络与信息系统总体架构、技术体系、运维和监测体系、管理体系和监督体系的基本构成和运行概况,等级保护定级、测评和检查发现的问题及其整改计划与执行进展概况。

3. 网络安全评估领域基本情况

网络安全评估领域基本情况主要是从网络安全领导力、安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全建设管理、安全运维管理、安全监测防护和安全管理保障 9 个待评估领域简述受评方相应领域的网络安全防护实施基本情况和关注事项。

4. 管理层对本次评估的期望

管理层对本次评估的期望主要是简述受评方管理层网络安全关注问题以及对本次评估的期望。

5. 附表附件

附表附件主要包括：受评方网络结构总图和分区分域说明，受评方内部网络对外连接出口示意图及其简述，受评方网络安全等级保护定级（和拟定级）清单，重要或关键业务或信息系统功能、边界、组件部署、服务对象、用户分布和安全防护简介，受评估方网络安全防护良好实践简介，等等。

编制先期文件包，实际上是受评方开展内部自评估的一个工作过程，是整个同行评估及其价值体现的重要组成部分。受评方应尽可能地参考以上框架进行认真准备，以便为评估员高质量准备现场评估任务作业指导书并在有限的时间内有效完成现场评估工作奠定坚实基础。

评估队在收到先期文件包之后，评估队队长和协调员应分配和跟踪研阅任务。评估员应认真、全面研阅先期文件包，结合自己的网络安全防护经验、自己负责评估的领域以及相应领域的业绩目标与评估准则，进一步与受评方对口人进行核实或补充了解有关信息，编制“阅研先期文件包后发现的关注问题清单”，起草现场评估任务作业指导书要点，为现场快速、精准开展评估做好充分准备。

由于先期文件包事先需要经互联网邮件等方式发送给评估队和评估员，因此，受评方在准备先期文件包时，应注意避免在内容中出现敏感信息，并通过文件加密等方式进行传递。

5.2.2　评估发现和准确描述事实

1. 通过观察进行评估发现

同行评估是以业绩目标为基准的评价过程，观察是评估发现的一项重要手段。观察是指观察工作被如何执行、执行得如何、其结果如何，并进一步询问这项工作是否可以被做得更好。这里所指的观察，泛指现场观察、文档查阅、人员访谈等常见的同行评估方法。对于网络安全运行维护评估，现场观察是一种获得事实的重要手段，对于网

络安全建设项目评估，可找到一些具体的开展现场观察的工作场景，并将现场观察与文档查阅、人员访谈等有效结合起来。这样，更有利于进行评估发现。

2. 评估发现的目的是识别偏差事实

同行评估是以事实为基础的评价过程，事实是评估的根基，是进行逻辑分析得出评估结论的基础。评估期间，评估员通过客观的观察得到事实，并准确、如实地描述事实。每一事实都是一个偏差或者未被做好的事，应给出判断其错误或不够卓越的理由，即这样做会如何(So What)。在对事实描述的过程中，评估员应不添加任何关于印象的词汇，仅是对客观事实的描述。在观察的同时，还应关注以下问题："与卓越标准相比，还有更好的做法吗?"这也是体现同行评估"聚焦管理、追求卓越"特点和价值的具体评估要点。

在观察过程中，评估发现依赖于整个评估活动中评估方和受评方开放坦诚的态度。因此评估员要每天将发现的问题及时告知受评方对口人，不应使其感到"意外"或"吃惊"。这将确保受评方对口人理解评估员的发现；如果受评方对口人认为评估员掌握的事实不充分，这还有助于评估员补充进一步的事实，确保双方对发现的问题理解一致。受评方对口人应积极配合观察，不要试图改变评估员发现的问题，一切从实际出发。

3. 规范有序地进行评估发现以获得有价值的偏差事实

评估员应以评估任务作业指导书为指导，根据选定的具体评估对象和评估项基本要求，选择合适的工作场景进行现场观察。观察的对象可以是工作开始前的准备或正在进行的现场作业，也可以是工作结束后的相关文件或受访者的表达，还可以是工作记录和相关的资料等。

观察有 4 个主要步骤：准备；实施观察；确认事实；编制观察报告。

(1) 准备。依照制订的评估计划，和对口人沟通，明确准备观察什么；观察的活动。例如，准备观察一项具体工作的过程，如域控系统维护操作，包括新增用户、用户授权修改、安全配置变更等；又如，准备观察一项具体工作的结果，如网络设备配置变更记录、网络安全设备安全策略变更记录等。接下来，选择被观察的活动，并清楚观察的预期结果(实际上就是评估项基本要求的期望结果)。要让被观察的人员明白，要对他们进行观察。协商好见面的时间、地点，并提前准备好所需要的文件资料等，弄清观察涉