信息安全应急处理服务资质认证自评估表填写指南

填写要求：

1.当条款对应的需提供证明材料为制度或项目文档时，在“证明材料清单栏目”填写文档的完整名称。例如《XX 公司信息安全应急处理服务规范》、《XX 系统应急处理服务方案》、《安全事件管理程序》、《XX 安全事件处理报告》等，并概括地介绍制度或项目文档各章节的主要内容。

2.当条款对应的需提供证明材料为记录文档时，在“证明材料清单栏目”填写记录的完整名称。例如《应急响应工具包更新记录》、《XX 项目应急响应服务承诺书》、《XX 事件应急响应过程记录》等，并概括地介绍记录文档的主要内容。

3.当条款对应的需提供证明材料为某制度或文档的某章节内容时，在“证明材料清单栏目”填写文档的完整名称及对应的章节编号。例如《XX 安全事件处理报告》第 X 章 安全建议、《XX 突发事件应急预案》第 X 章 预案启动条件等，并对相关内容进行总结概括。

4.所有出现在“证明材料清单”栏目中的文档，都需提供相应的电子版文档或纸质文档的扫描件作为证明材料，并按照条款的序号建立文件夹整理归档，建立文件夹的格式为“序号-条款的考核内容”，例如“1-应急处理服务流程”、“27-安全事件检测规范”、“53-安全事件处理记录”等。

以下给出了一份填写样例，供申请组织进行参考。填报组织应按照填写样例的细粒度，进行相关信息的填报。当申请三级服务资质时，仅填写自评估表中与三级相关的条款（具体分两种情况：1、标明适用于三级的；2、未标明属于哪个级别的）；申请二级服务资质时，除填写标明适用于二级的条款之外，还应填写所有属于三级要求的条款；申请一级服务资质时，填写全部条款。

组织名称	XX 公司（全称）	申报级别	X 级
评估时间	XX 年 X 月 X 日-X 月 X 日	评估部门/人员	XX 部/XX

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
1.	服务技术要求	建立信息安全应急处理服务流程。	按照相关标准建立的信息安全应急处理服务流程，流程图中应包括每个阶段对应的职责、输入输出等。			提供 XX 公司应急响应流程（包含准备阶段、检测阶段、抑制阶段、根除阶段、恢复阶段、总结阶段），对每个阶段的目标、角色、内容、输出进行了详细说明。 1.准备阶段： 目标： 工作内容： 输出： ……
2.		制定信息安全应急处理服务规范并按照规范实施。	已制定的信息安全应急处理服务规范。			提供《XX 公司应急响应操作规范》，包含微软系统、Linux 系统、IIS、HP-UX 主机、SQL server 服务、DB2 数据库、oracle 数据等系统的应急响应检测规范，提供网站暗链、网站挂马、网站篡改、流量异常、网站钓鱼、病毒蠕虫、网站数据泄露、DDOS 等 8 类常见信息安全事件的应急处理操作规范。
3.	准备阶段	明确客户的应急需求。	应急服务内容，已完成项目中对客户应急需求进行调研分析的证明材料。			提供 XX 项目应急需求调研报告，客户对应急服务的需求包括…… 提供 XX 项目合同，合同名称：XX，签订时间：XX，合

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
						同服务期限：XX，合同金额：XX，服务内容：XX。
4.		了解客户应急预案的内容。	需对客户自身已建立的应急预案的内容进行了解与熟悉（客户应急预案的内容）。			提供甲方自身的应急预案，包含 XX、XX、XX、XX、XX 等内容。
5.		向客户提供应急处理服务流程。	应为客户提供本企业应急处理服务流程，使其了解应急处理服务的相关环节（应急处理服务流程图及各阶段工作说明）。			提供项目的应急响应服务方案，服务方案中第 X 节对应急响应流程（包含 XX 阶段、XX 阶段、XX 阶段、XX 阶段）的每个阶段的目标、角色、内容、输出进行了详细说明。
6.		**仅三级要求：**可提供本地 2 小时应急响应服务能力。	该级别服务提供商需具备本地 2 小时应急响应时间的能力（服务承诺书）。			提供《XX 项目应急响应服务承诺书》，承诺的应急响应服务时间为 XX。
7.		配备有处理网络或信息安全事件的工具包，包括常用的系统命令、工具软件等。	工具包及工具列表。			提供《应急响应技术指南及工具》清单，主要包含 WEB 应用弱点扫描器、数据库弱点扫描器、WEB 应用代码安全检测系统、基准安全分析器、XX 等。
8.		工具包应定期更新。	工具包更新记录。			提供《应急响应工具包更新记录》，记录的主要内容包含： 软件名称： 更新内容： 更新时间： 更新人：
9.		配备应急处理服务人员。	服务人员列表、专业资质证书。			提供《应急响应服务人员列表》，包含 XX、XX、XX、XX、XX 等信息。

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
10.		对在应急处理服务过程中可能会采取的操作、处理等行为，获得用户的书面授权。	用户出具的书面授权书。			提供项目的书面授权书，其中对 XX、XX、XX 等应急处理操作进行了书面授权。
11.		**仅二级/一级要求：**在客户应急需求基础上制定应急服务方案。	应急服务方案（模板和实际服务项目方案）。			提供项目应急响应服务方案，包含 XX、XX、XX、XX、XX 等章节内容。 提供 XX 公司的《应急响应服务方案模板》，包含 XX、XX、XX、XX、XX 等章节内容。
12.		**仅二级/一级要求：**应急服务方案应涉及客户应急预案的启动与执行。	应急服务方案中应涵盖客户自身建立的应急预案内容。			提供《XX 突发事件应急预案》，针对 X 种场景（包括 XX、XX、XX 等），预案的启动条件为……、处置过程为……、预期结果为……、处置要求为……
13.		**仅二级/一级要求：**若客户未建立应急预案，可协助客户建立。	协助客户建立的应急预案。			提供甲方自身的应急预案，包含 XX、XX、XX、XX、XX 等章节内容。
14.		**仅二级要求：**可提供本地 1 小时、外地 8 小时应急响应服务能力。	该级别服务提供者应具备本地 1 小时、外地 8 小时提供应急处理服务的能力（服务承诺书、合同条款等）。			提供《XX 项目应急响应服务承诺书》，承诺的应急响应服务时间为 XX。
15.		**仅二级/一级要求：**网络与信息安全事件工具包中应配备专业技术检测设备。	工具包及工具列表。			提供《应急响应技术指南及工具》清单，主要包含 WEB 应用弱点扫描器、数据库弱点扫描器、WEB 应用代码安全检测系统、基准安全分析器、XX 等。
16.		**仅二级/一级要求：**对工具包实行制度化管理。	工具包管理制度及执行记录。			提供《工具管理制度》，包含 XX、XX、XX、XX、XX 等章节内容。 提供《应急响应工具包更新记录》，记录的主要内容包含：

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
						软件名称： 更新内容： 更新时间： 更新人：
17.		**仅一级要求：**建立有体系化的应急处理服务流程。	应急服务流程应纳入公司的相关体系管理范围（相关体系文件及实施记录）。			提供 XX 公司《信息安全应急处理流程》，包含 XX、XX、XX、XX、XX 等章节内容。 提供 XX 公司《XX 管理体系文件》，其中 XX 文件对应急服务流程进行了规定。
18.		**仅一级要求：**可提供本地 7X24 小时、外地 4 小时应急响应服务能力。	该级别服务提供者应具备本地 7X24 小时、外地 4 小时提供应急处理服务的能力（签订的服务级别协议）。			提供《XX 项目应急响应服务承诺书》，承诺的应急响应服务时间为 XX。
19.		**仅一级要求：**与客户之间建立安全保密的信息传输渠道。	与客户传输信息时采用可信及保密传输渠道的证明材料。			对于电子类的文档，与客户通过加密邮件的方式进行传输。
20.		**仅一级要求：**具有自主开发专业检测工具的能力。	该级别服务提供商需具备自主开发专业安全检测工具的能力，如有自主知识产权的工具产品（自主知识产权书、商用产品检测证书、安全产品认证证书等）。			提供 XX 公司 XX 产品安全测评证书： 证书号：XX，满足级别：XX，有效期至 XX。
21.	检测阶段	确定检测对象及范围。	确定检测对象及范围的过程记录。			提供项目《安全事件检测方案》，包含 XX、XX、XX、XX 等章节的内容。
22.		对发生异常的系统进行信息的收集与分析，判断是否真正发生了安全事件。	收集信息的过程及判断依据（过程记录）。			提供项目《安全事件检测过程记录》，包含 XX、XX、XX、XX 等章节的内容，对异常信息的收集与分析过程为….

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
23.		与客户共同确定应急处理方案。	提供应急处理方案（模板及实际项目的应急处理方案）。			提供项目应急响应服务方案，包含 XX、XX、XX、XX、XX 等章节内容。 提供 XX 公司的《应急响应服务方案模板》，包含 XX、XX、XX、XX、XX 等章节内容。
24.		应急处理方案应明确检测范围与检测行为规范，其检测范围应仅限于客户已授权的与安全事件相关的数据，对客户的机密性数据信息未经授权不得访问。	应急处理方案的内容中应明确规定检测范围及检测行为规范（模板及实际项目的应急处理方案）。			提供 XX 公司《安全工程实施规范》，XX 章节对应急响应服务项目现场实施的安全保密、文档管理、离场结束安全管理等进行了要求。
25.		与客户充分沟通，并预测应急处理方案可能造成的影响。	应急处理方案涉及的风险阐述（风险识别与风险控制措施）。			提供项目应急响应服务方案，其中 X 章节对应急响应服务过程中的风险进行了描述，主要风险包括……
26.		检测工作应在客户的监督与配合下完成。	应急处理工作流程或其他文档中约定的工作配合/监督机制，相关过程记录。			应急响应服务项目的检测工作均由项目甲方人员监督配合下完成。
27.		**仅二级/一级要求：**建立有针对常规应用系统、安全设备、常见网络与信息安全事件的检测技术规范。	提供相应的检测技术规范列表及各规范内容（范本或应用本），如针对 windows、Aix、Unix、Linux、oracle、Firewalls、Router 等。			提供 XX 公司《应急响应操作规范》，其中包含 XX 系统、XX 系统的应急响应操作规范。
28.		**仅二级/一级要求：**协助客户确定安全事件等级。	信息收集的过程及确定安全事件等级的证明材料。			提供 XX 项目《XX 事件应急响应过程记录》，事件定级为 XX。
29.		**仅二级/一级要求：**应急处理方案应包含对安全事件的抑制、根除和恢复的详细处理步骤。	应急方案应涵盖该内容。			提供 XX 项目应急响应服务方案，其中 X 章节对安全事件的抑制、根除和恢复的详细步骤进行描述，主要包括……

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
30.		**仅二级/一级要求：**应急处理方案应包含实施方案失败的应变和回退措施。	应急方案应涵盖该内容。			提供 XX 项目应急响应服务方案，其中 X 章节对实施方案失败的应变和回退措施进行描述，主要包括……
31.		**仅一级要求：**建立有完善的检测技术规范及具有对高技术入侵的检测技术能力。	相关技术检测规范，技术人员检测高技术入侵的能力展示。			提供 XX 应急响应技术检测规范，包含 XX、XX、XX、XX、XX 等章节内容。 提供技术入侵检测的模拟环境设备清单，主要包括 XX、XX 设备。
32.		**仅一级要求：**具有挖掘系统设备及业务系统安全漏洞的能力。	提供相关漏洞的证明，包括漏洞平台的发布、漏洞库编号等。			提供中国国家信息安全漏洞库信息安全漏洞提交证明 X 份，漏洞编号分别为： CNNVD-XXXX-XX，……
33.		**仅一级要求：**对确认的安全事件启动安全事件管理程序。	提供安全事件管理程序及事件启动条件（安全事件管理程序文件）。			提供 XX 公司《信息安全事件管理程序》，包含 XX、XX、XX、XX、XX 等章节内容。
34.		**仅一级要求：**应急处理方案中应对可能造成的影响进行分析，包括社会影响。	应急处理方案中对社会影响进行分析的证明材料。			提供 XX 项目应急响应服务方案，其中 X 章节对可能造成的影响进行分析，主要内容为……
35.	抑制阶段	与客户充分沟通，使其了解所面临的首要问题及抑制处理的目的。	沟通的内容及结果。			提供 XX 项目《应急响应服务沟通记录》，主要内容为……
36.		在采取抑制措施之前，应告知客户可能存在的风险。	应急处理抑制阶段涉及的风险阐述及告知记录。			提供 XX 项目《应急响应服务风险告知记录》，主要风险为……
37.		严格执行抑制处理方案中规定的内容，如有必要更改，须获得客户的授权。	应急抑制处理方案的变更管理（变更管理涉及的文档）。			提供 XX 公司《系统变更管理办法》，包含 XX、XX、XX、XX、XX 等章节内容。
38.		抑制措施应能够限制受攻击的范围，抑制潜在的或进一步的攻击和破坏行为。	抑制措施的内容。			提供项目的《抑制处理方案》，主要抑制措施为……

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
39.		**仅一级要求：**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。	抑制过程中用到的可信工具列表、工具简介。			提供 XX 公司《主要网络安全事件处理工具清单》，清单中主要包含 XX、XX、XX 等工具，工具均为正规厂商生产的商用产品，均已获得相关销售许可。
40.	根除阶段	协助客户检查所有受影响的系统，提出根除的方案建议，并协助客户进行具体实施。	根除建议（方案）的内容。			提供 XX 项目的《根除方案》，主要根除措施为……
41.		应明确告知客户所采取的根除措施可能带来的风险。	应急处理根除阶段涉及的风险阐述及告知记录。			提供 XX 项目《应急响应服务风险告知记录》，根除阶段主要风险为……
42.		找出导致网络或信息安全事件发生的原因，并予以彻底消除。	安全事件得到根除的证明材料。			提供 XX 项目的《事件根除记录》，主要内容为……
43.		**仅一级要求：**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。	根除过程中用到的可信工具列表、工具简介。			提供 XX 公司《主要网络安全事件处理工具清单》，清单中主要包含 XX、XX、XX 等工具，工具均为正规厂商生产的商用产品，均已获得相关销售许可。
44.	恢复阶段	告知客户网络或信息安全事件的恢复方法及可能存在的风险。	应急处理恢复阶段涉及的风险阐述及告知记录。			提供 XX 项目《应急响应服务风险告知记录》，恢复阶段主要风险为……
45.		**（如需重建系统时适用该条款）**对于不能彻底恢复配置和彻底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可恢复正常时，应选择重建系统。	重建系统的相关过程记录。			提供 XX 项目的《重建系统过程记录》，主要内容为……
46.		**（如需重建系统时适用该条款）**应协助客户按照系统的初始化安全策略恢复系统。	重建系统过程中按照初始化安全策略恢复系统的相关过程记录。			提供 XX 项目的《重建系统过程记录》，其中“协助客户按照系统的初始化安全策略恢复系统”的主要步骤和方法为……

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
47.		**（如需重建系统时适用该条款）**应协助客户验证恢复后的系统是否运行正常，并确认与原有系统配置保持一致。	重建系统过程中关于确认系统配置与原有系统配置是否一致的相关过程记录。			提供 XX 项目的《重建系统过程记录》，其中“协助客户验证恢复后的系统是否运行正常，并确认与原有系统配置保持一致”的主要步骤和方法为……
48.		**（如需重建系统时适用该条款）**在帮助用户重建系统前需进行全面的数据备份，备份的数据要确保是没有被攻击者改变过的数据。	重建系统过程中关于数据备份的相关过程记录。			提供 XX 项目的《重建系统过程记录》，其中关于数据备份的主要步骤和方法为……
49.		**（不需重建系统时适用该条款）**应建立重建系统的应急工作流程及规范，并开展重建系统的应急演练工作。	重建系统的应急工作流程及规范，重建系统的应急演练记录。			提供《重建系统应急工作流程及规范》，包含 XX、XX、XX、XX、XX 等章节内容。 提供《重建系统应急演练记录》。
50.		**仅二级/一级要求：**与客户共同制定系统恢复方案，根据实际情况协助客户选择合理的恢复方法。	形成的系统恢复方案及内容。			提供 XX 项目的《XX 系统恢复方案》，主要内容为……
51.		**仅二级/一级要求：（如需重建系统时适用该条款）**帮助客户为重建后的系统建立系统快照。	重建系统过程中关于建立系统快照的相关过程记录。			提供 XX 项目的《重建系统过程记录》，其中“帮助客户为重建后的系统建立系统快照”的主要步骤和方法为……
52.		**仅一级要求：（如需重建系统时适用该条款）**帮助客户对重建后的系统进行全面的安全加固。	重建系统过程中对系统进行安全加固的相关过程记录。			提供 XX 项目的《重建系统过程记录》，其中“帮助客户对重建后的系统进行全面的安全加固”的主要步骤和方法为……
53.	总结阶段	应保存完整的网络或信息安全事件处理记录，并对事件处理过程进行总结和分析。	网络安全事件处理过程的记录、总结与分析文档。			提供 XX 项目的安全事件处理过程记录，主要包括 XX、XX、XX、XX、XX 等。

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
54.		提供网络或信息安全事件处理报告。	已完成项目的网络安全事件处理报告（报告模板及实际报告）。			提供 XX 项目的安全事件处理报告，主要包括 XX、XX、XX、XX、XX 等章节。
55.		提供网络或信息安全方面的建议和意见，必要时指导和协助客户实施。	已完成项目中向客户提供的网络安全建议。			提供 XX 项目的安全事件处理报告，在 X 章节提供了相关网络安全建议，主要内容为……
56.		**仅二级/一级要求：**网络与信息安全事件处理记录应具备可追溯性。	已完成项目的网络安全事件处理过程记录、总结与分析文档。			提供 XX 项目的安全事件处理过程记录，主要包括 XX、XX、XX、XX、XX 等。（描述记录如何体现可追溯性）
57.		**仅二级/一级要求：**提供详实的网络与信息安全事件处理报告，完整展现应急处理服务的整个过程。	已完成项目的网络安全事件处理报告（报告模板及实际报告）。			提供 XX 项目的安全事件处理报告，主要包括 XX、XX、XX、XX、XX 等章节。
58.		**仅一级要求：**对网络与信息安全事件进行总结和分析后，针对典型案例存入事件知识库。	知识库的案例表。			提供 XX 公司应急响应案例文档，主要包含 XX、XX、XX 等项目案例。
59.		**仅一级要求：**提供关闭安全事件的管理程序。	安全事件的关闭程序（安全事件关闭涉及的文档）。			提供 XX 公司《安全事件关闭程序》，包含 XX、XX、XX、XX、XX 等章节内容。
60.		**仅一级要求：**告知客户所发生事件可能涉及到的法律诉讼方面的法律要求或影响。	应急处理中涉及到司法相关告知的相关文档。			提供 XX 项目的安全事件处理报告，在 X 章节告知了所发生事件可能涉及到的法律诉讼方面的法律要求或影响，主要内容为……
61.	**上一年度提出的观察项整改情况（如有）**					
62.		**XXXX（描述前一年度观察项）**				提供观察项整改措施、以及整改措施在新项目中的落实情况

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
63.						
64.	上一年度提出的不符合项整改情况（如有）					
65.		XXXX（描述前一年度不符合项）				提供不符合项整改措施，以及整改措施在新项目中的落实情况
66.						

自评估结论：

经自主评估，本单位的信息安全应急处理服务满足《信息安全服务 规范》___级要求，申请第三方审核。

本单位郑重承诺，《信息安全服务资质认证自评估表-公共管理》与本自评估表中所提供全部信息真实可信，且均可提供相应证明材料。