1. 测评机构和测评人员的职责

商用密码应用安全性评估工作是一项专业性很强的工作，需要专门的测评机构派出专业测评人员实施测评，测评结果作为密码应用安全性评估结论的重要依据。

测评机构是商用密码应用安全性评估的承担单位，应当按照有关法律法规和标准要求科学、公正地开展评估。承担商用密码应用安全性评估工作的测评机构，需要经过国家密码管理部门组织的试点培育，经评审后，纳入试点测评机构目录；在测评过程中，需要全面、客观地反映被测系统的密码应用安全状态，不得泄露被测评对象的工作秘密和重要数据，不得妨碍被测系统的正常运行。测评机构完成商用密码应用安全性评估工作后，应在 30 个工作日内将评估结果报国家密码管理部门备案。

从事商用密码应用安全性评估工作的测评人员应当通过国家密码管理部门（或其授权的机构）组织的考核，遵守国家有关法律法规，按照相关标准，为用户提供安全、客观、公正的评估服务，保证评估的质量和效果。

2. 网络与信息系统责任单位的职责

网络与信息系统责任单位即网络与信息系统建设、使用、管理单位，是商用密码应用安全性评估的责任单位，应当健全密码保障系统，并在规划、建设和运行阶段，组织开展商用密码应用安全性评估工作，并负主体责任。重要领域网络与信息系统的运营者，应按如下要求开展工作。

第一，系统规划阶段，网络与信息系统责任单位应当依据商用密码技术标准，制定商用密码应用建设方案（简称密码应用方案），组织专家或委托具有相关资质的测评机构进行评估。其中，使用财政性资金建设的网络与信息系统，商用密码应用安全性评估结果应作为项目立项的必备材料。

第二，系统建设完成后，网络与信息系统责任单位应当委托具有相关资质的测评机构进行商用密码应用安全性评估，评估结果作为项目建设验收的必备材料，评估通过后，方可投入运行。

第三，系统投入运行后，网络与信息系统责任单位应当委托具有相关资质的测评机构定期开展商用密码应用安全性评估。未通过评估的，网络与信息系统责任单位应当按要求进行整改并重新组织评估。其中，关键信息基础设施、网络安全等级保护第三级及以上信息系统每年至少评估一次。

第四，系统发生密码相关重大安全事件、重大调整或特殊紧急情况时，网络与