商用密码应用安全性评估“十问十答”

密码为保护信息安全而生，是网络安全的核心要件，是数字经济基础支撑。下面，我们就来介绍一下日常工作生活中融入的商用密码应用及其安全性评估。

一、什么是商用密码，为什么要使用商用密码？

密码分为核心密码、普通密码和商用密码，我们日常工作生活中接触到的多是商用密码。工作中，网上办公、缴税纳税等过程都有商用密码在起作用。生活中，第二代居民身份证就通过商用密码技术保证认证一致，购买火车票、网络购物等在线支付全过程都有商用密码的保护。

商用密码，是指对不涉及国家秘密内容的信息进行加密保护或安全认证所使用的密码技术和密码产品。其中，商用密码技术，是保障信息安全的核心技术。从功能上看，主要包括加密保护技术和安全认证技术；从内容上看，主要包括密码算法、密钥管理和密码协议。商用密码产品，是指采用密码技术对不涉及国家秘密内容的信息进行加密保护或安全认证的产品，即承载密码技术、实现密码功能的实体。按照形态划分，商用密码产品分为六类，即软件、芯片、模块、板卡、整机、系统；按照功能划分，商用密码产品分为七类，即密码算法类、数据加解密类、认证鉴别类、证书管理类、密钥管理类、密码防伪类和综合类。

密码是网络信任体系的重要基石，是目前世界上公认的，保障网络与信息安全最有效、最可靠、最经济的关键核心技术。《网络

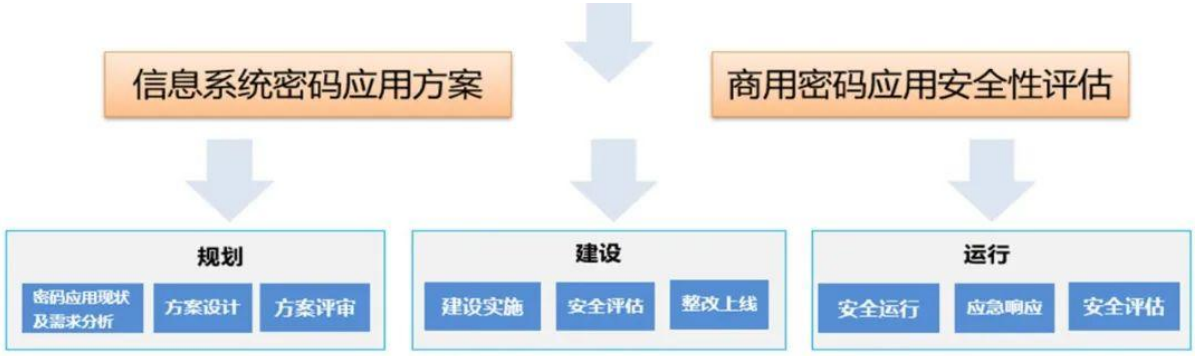
安全法》《密码法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等法律法规均不同程度地提到要使用商用密码。在信息互联时代，密码除传统加密外，主要体现在身份认证、权限管理、访问控制等。数字经济时代，密码的作用不断扩展到数据流通、数据共享等新维度，密码技术自身也需要持续革新。

二、商用密码应用安全性评估（简称“密评”）是什么，哪些单位需要开展密评工作

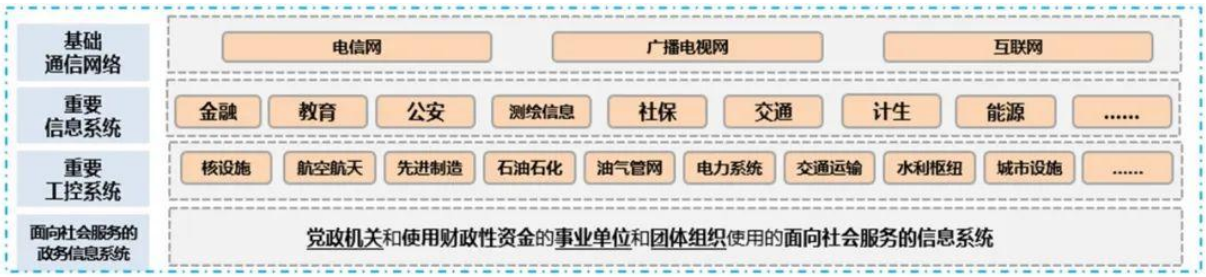
“密评”是指

络和信息系统中，

估。



国家网络安全和密码相关法律法规明确要求非涉密的关键信息基础设施、等保三级及以上系统、国家政务等重要信息系统要开展密评工作。并且，密评管理办法也明确规定：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，需要每年至少评估一次。



三、不做密评或测试结果不合格会有哪些影响呢？

相关影响已经有文件加以明确：

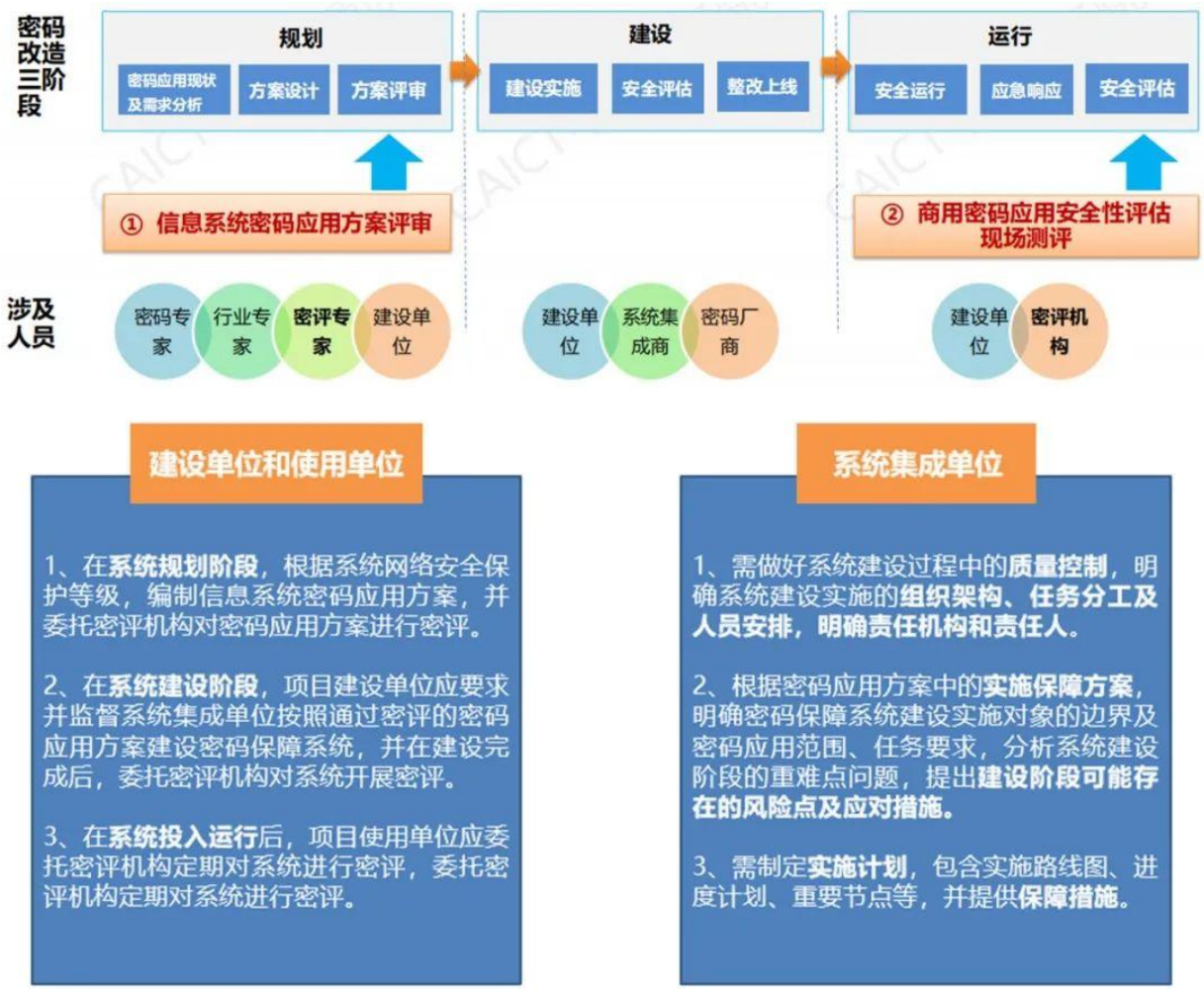
●**首先，是《密码法》第三十七条第一款指出：**关键信息基础设施的运营者未按照要求使用商用密码，或者未按照要求开展密评的，由密码管理部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，将处十万元以上一百万元以下罚款。

●**《国家政务信息化项目建设管理办法》第二十八条第三款也有提到：**对于不符合密码应用和网络安全要求，或者存在重大安全隐患的政务信息系统，不安排运行维护经费，项目建设单位不得新建、改建、扩建政务信息系统。

此外，全国各地方也在不断将密码应用要求纳入行业管理规范、工作计划。如川办发〔2021〕49号《四川省省级政务信息化项目管理办法》，以及近两年印发的《广东省政务信息化项目建设管理办法》《河北省省级政务信息化项目建设管理办法》《河南省政务云管理办法》《江西省政务信息化项目建设管理办法》《吉林省政务信息化项目建设管理办法》《广西政务信息化项目建设管理办法》，均提到了要按要求采用密码技术和定期开展密评。

四、密评在密码应用部署过程中所处的位置，全过程涉及的参与方有哪些？

项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。



五、密评主要由哪些机构开展？

从事密评活动的机构（简称“密评机构”），应当经国家密码管理部门认定，依法取得商用密码检测机构资质。

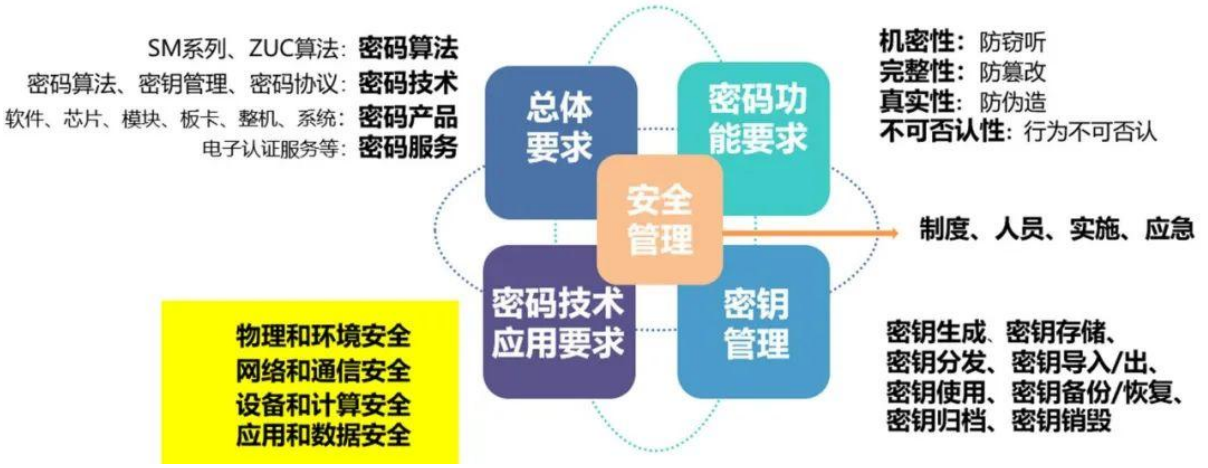
密评机构应具备商用密码相关测评工具，技术人员具备专业的测评实施能力，依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等标准规范，为用户提供信息系统商用密码应用安全性评估相关的咨询服务以及测评评估服务。

六、开展密评工作主要参考哪些标准规范？

参考的标准主要分为两类：

●第一类是基本要求

就是我们通常说的“信息系统密码应用基本要求”，主要依据国家标准 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，此标准于 2021 年 10 月 1 日正式实施。



●第二类是评估方法

目前主要参考的文件是 2021 年发布的 GM/T 0115-2021《信息系统密码应用测评要求》、GM/T 0116-2021《信息系统密码应用测评过程指南》，中国密码学会密评联委会修订形成的《信息系统密码应用高风险判定指引》《商用密码应用安全性评估量化评估规则》。

密评量化评估满分 100 分，得分大于等于 60 分且没有高风险项为基本合格。

七、密评的服务内容主要有哪些？

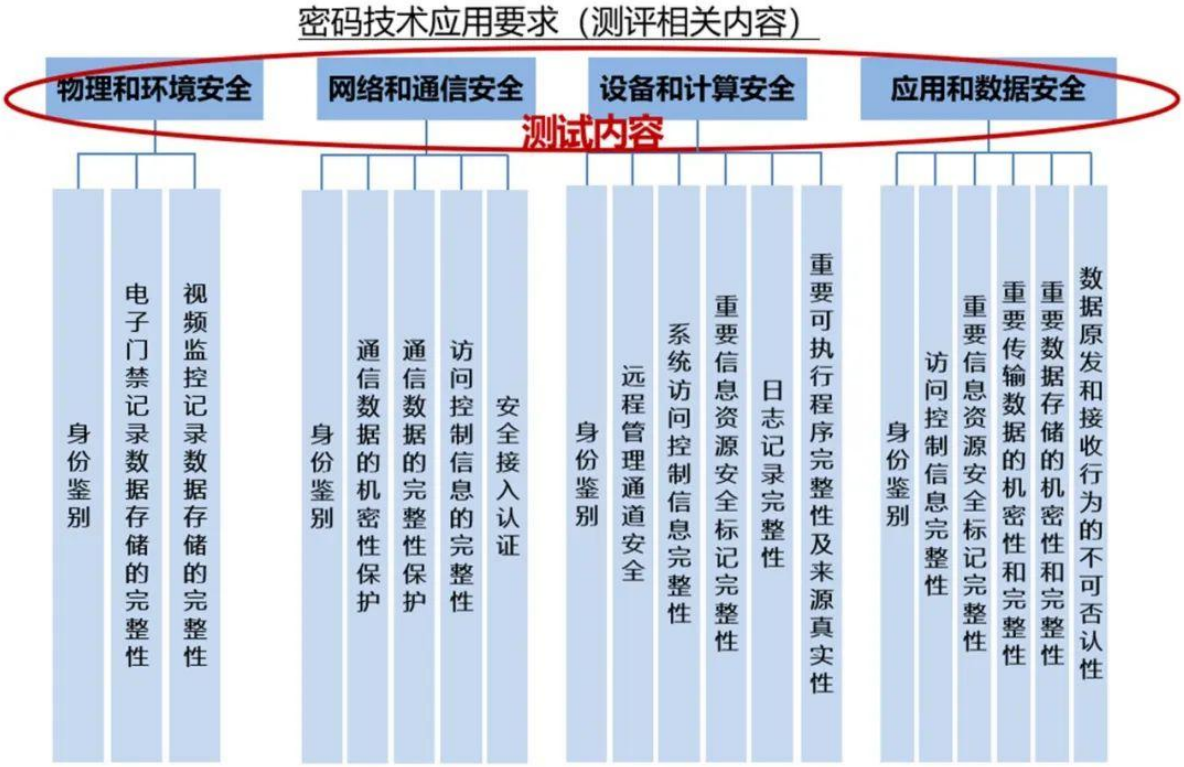
密评工作主要包括两部分内容：一是信息系统规划阶段的密码应用方案评审或评估，这一环节主要用于保证建设方案的安全性；二是信息系统建设完成后针对该系统开展现场测试。

●方案评审或评估阶段

主要针对新建或改造信息系统，密码应用改造方案一般由用户单位组织编写，用户单位编写密码应用建设方案/改造方案后，应组织对方案进行评审或评估。

●系统评估阶段

主要依据国标GB/T39786-2021《**信息安全技术 信息系统密码应用基本要求**》，从物理和环境、网络和通信、设备和计算、应用和数据、安全管理等方面开展评估。



八、密评过程主要包括哪些环节？

密评过程（见下图）分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动；测评双方之间的沟通与洽谈贯穿整个密码应用安全性评估过程。其中，测评对

象包括安全人员、管理员、密码产品、网络设备、服务器、数据库、安全设备、操作系统、应用系统、业务系统、技术文档、管理制度文档等；测评工具涉及协议分析工具、端口扫描工具、渗透测试工具、算法和随机性检测工具、密码应用检测工具、密码安全协议检测工具等。

九、密评过程中有哪些常见问题？

用户单位在密码实际应用改造过程中，会遇到诸多问题，如租用外部机房如何满足物理和环境安全项的要求、自建 CA 的合规性、云平台和云上应用的测评等问题，通用解答可参见 2021 年底已发布的《商用密码应用安全性评估 FAQ》（https://ht.cacrnet.org.cn/upload/file/20211217/1639751669666037.pdf），针对具体问题还需要结合用户单位实际情况进行详细解答。

十、取得密评报告后应如何去管理部门备案？

按照《密码法》确定的属地管理原则，应由运营者所在地的密码管理部门作为备案部门，由省级密码管理部门作为一般备案部门，国家密码管理局作为特殊备案部门。自密评报告出具之日起30日内，填写《网络与信息系统密评备案信息表》，并按备案表要求，附上密评合同和密评报告，邮寄到所属地密码管理局。