ICS 35.020
L 70

团　　体　　标　　准

X/XXXXX XXX-XXXX

电子政务系统商密应用安全性评估中数据安全测评规范

The specification of data security assessment for commercial cryptography application security evaluation in E-governance systems

（征求意见稿）

2023 - XX - XX 发布　　2023- XX - XX 实施

广东省网络空间安全协会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广东省网络空间安全协会提出并归口。

本文件起草单位：华南师范大学、数字广东网络建设有限公司、工业和信息化部电子第五研究所、深圳奥联信息安全技术有限公司、广州竞远安全技术股份有限公司、广东申腾信息技术有限公司、华南农业大学、北京海泰方圆科技股份有限公司。

本文件主要起草人：郑伟平、陈静、高锐、战鹏、王正临、黄琼、陈世胜、龚征、但波、王学进、刘洪军、姚莹、蔡合、陈浩东、肖媚燕、付庆龙。

引　言

随着互联网的普及应用，网络安全已成为国家安全战略重要组成部分。如何确保信息网络的设施安全、运行安全和数据安全，备受社会各方关注。国家也先后出台了《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国数据安全法》和《个人信息保护法》等相关法律法规，相关行业主管部门在此基础上，陆续推出了《商用密码应用安全性评估管理办法》、《商用密码应用安全性评估量化评估规则》，指导商用密码应用安全性评估机构、信息系统责任单位开展商用密码应用安全性评估工作。由于广东省电子政务系统，存储并运行着大量个人信息、政务数据等重要敏感数据，因此在针对电子政务系统开展密码应用安全性评估的过程中，规范化数据应用和数据安全保护工作，能有效强化广东省电子政务系统数据的安全保密管理，提升电子政务系统重要数据在传输、存储过程中的机密性、完整性。

本标准提出电子政务系统商密应用安全性评估中数据安全测评指标与要求，为密码管理行业标准《信息系统密码应用测评要求》、国家标准《信息安全技术 信息系统密码应用基本要求》在电子政务系统商密应用安全性评估提供技术支撑，指导商密应用安全性评估中数据安全评估的开展。

电子政务系统商密应用安全性评估中数据安全测评规范

1 范围

本文件规定了电子政务系统商用密码应用安全性评估中数据安全的检测要求与评估方法。

本文件适用于规范监管部门、第三方评估机构在电子政务系统商用密码应用安全性评估中数据安全监督、管理与测评，为电子政务数据安全保护工作提供支撑与参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 39786-2021信息安全技术 信息系统密码应用基本要求

GB/T 信息安全技术 网络数据分类分级要求（征求意见稿）

GM/Z 4001 密码术语

GM/T 0028 密码模块安全技术要求

GM/T 0039 密码模块安全检测要求

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

3 术语和定义

GB/T 25069 信息安全技术 术语

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 40692-2021 政务信息系统

GM/Z 4001 密码术语

上述标准定义和范围界定的以及下列术语和定义适用于本文件。

3.1

电子政务系统 e-governance system

电子政务系统是由政务部门建设、运行或使用的,用于直接支持政务部门工作或履行其职能的各类信息系统。

3.2

密码测评 cryptographic evaluation

按照有关法律法规和标准规范，对网络与信息系统使用商用密码技术、产品和服务的合规性、正确性、有效性进行检测分析和评估验证的活动。

3.3

电子政务数据 e-governance data

由政务部门或为政务部门采集、存储、加工、使用、处理等的信息资源。

注: 政务信息资源包括:政务部门依法采集的信息资源;政务部门在履行职能过程中产生和生成的信息资源;政务部门投资建设和外购服务获取的信息资源;政务部门依法授权管理的信息资源。

3.4

收集 acquisition

通过电子政务系统采集、人工填写、交易购买、共享交换等方式获取数据的行为。

3.5

存储 storage

电子政务数据以某种格式记录在计算机内部或外部存储介质上的行为。

3.6

使用加工 processing

通过对电子政务数据进行数据挖掘、分析、加工等活动，获取目的结果的行为。

3.7

传输 transmission

电子政务数据从一个系统、设备、平台、企业传送到另一个系统、设备、平台、企业的通信过程。

3.8

提供 provide

电子政务数据处理者向其他数据处理者提供数据，或将电子政务数据处理权由一个处理者向另一个处理者转移，且双方分别对数据拥有独立处理权的过程。

3.9

公开 public disclosure

将电子政务数据向社会或不特定人群公开发布的行为。

3.10

销毁 destruction

将电子政务数据进行彻底删除，使其无法复原的过程。

3.11

数据全生命周期 data life cycle

数据收集、存储、使用加工、传输、提供、公开等各环节数据处理活动。

3.12

数据处理者 data processor

对电子政务数据进行收集、存储、使用加工、传输、提供、公开等数据处理活动的组织。

4 缩略语

下列缩略语适用于本文件。

a) IP：互联网协议（Internet Protocol）。

b) MAC：媒体访问控制（Medium Access Control）。

c) IMSI：国际移动用户识别码（International Mobile Subscriber Identification Number）。

d) IMSI：国际移动设备识别码（International Mobile Equipment Identity）。

5 电子政务系统商密应用安全性评估中数据安全总体框架

5.1 概述

电子政务系统通过密码技术保障数据的机密性、完整性、真实性和敏感性，建立建全分类分级、组织保障、人员管理和安全评估，提升数据采集、数据传输、数据存储、数据处理、数据交换、数据清除等数据生命周期中的安全保障能力。电子政务系统商密应用安全性评估中数据安全总体框架如图 1 所示。

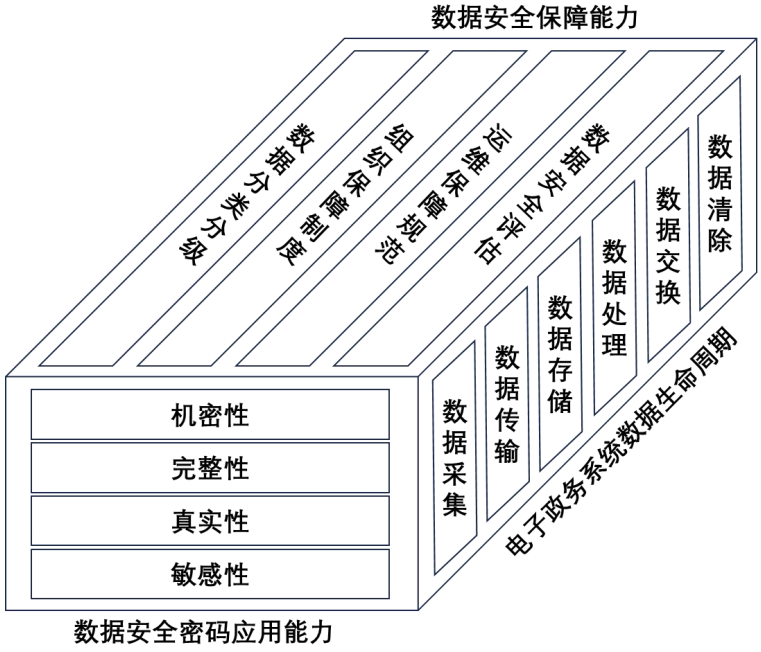

图1 电子政务系统商密应用安全性评估中数据安全总体框架

5.2 数据安全保障能力

5.2.1 概述

实施电子政务系统的数据分类分级管理，建立组织保障制度和运维保障规范，通过数据安全评估提升数据安全的保障能力。

5.2.2 电子政务系统数据分类

参照系统运行场景和商用密码应用性安全评估规则，将电子政务数据分为四种类型，包括鉴别类数据、主体类数据、业务类数据、系统类数据。电子政务系统数据分类说明如表 1 所示。

表 1 电子政务系统数据分类说明

数据分类	参考说明
鉴别类数据	用于电子政务系统用户鉴别身份的数据，一旦遭到未经授权的查看或未经授权的变更，会对电子政务系统的使用主体的数据造成危害。包括但不限于： 1）电子政务系统常规使用的身份鉴别数据，如：账号、卡号、USBKEY、口令等数据。 2）电子政务系统使用生物特征的身份鉴别数据，如：弱隐私（如人脸、声纹、步态、耳纹、眼纹、笔迹等。）、强隐私（指纹、虹膜等）的个人生物特征样本数据与特征值数据。 3）电子政务系统辅助用于身份鉴别的数据，如动态口令、短信验证码、口令提示问题等。
主体类数据	用于电子政务系统可识别特定个人、组织的主体身份数据，一旦遭到未经授权的查看或未经授权的变更，会对个人、组织主体造成危害。包括但不限于： 1）基本数据 指个人基本情况数据，如个人姓名、性别、国籍、民族、婚姻状况、证件类型、证件号码、证件生效日期、证件到期日期、家庭住址等。 组织基础概况数据，如法定代表人姓名、企业名称、

	统一社会信用代码、经营许可证、经营范围、行业分类、经济类型、人员规模、注册资本、企业地址等。 2）通讯数据 指个人、组织各类通信联系方式数据，如手机、固定电话、电子邮箱地址、微信号、联系人、通讯地址等。 3）关系数据 指个人、组织各类关系的记录数据，如个人与个人的关系数据（子或女、父母、兄弟姐妹、配偶等）个人与组织的关系数据（法定代表人、财务负责人、业务经办人、一般雇员、高管等）。组织与组织的关系数据（如集团关系、家族企业、互持股情况等）。 4）位置数据 指能用于标记个人地理空间或网络空间位置的数据，如定位信息、IMEI/IMSI、IP地址、MAC地址、地理位置等。 5）政治面貌数据 指个人政治、宗教信仰等数据，如党员、团员、党派、宗教信仰等。
业务类数据	电子政务系统业务过程种生成的数据，一旦遭到未经授权的查看或未经授权的变更，会对个人、组织主体造成危害。包括但不限于：教育、财产、卫生、司法、交通、招投标等。
系统类数据	电子政务系统运行过程种生成的数据，一旦遭到未经授权的查看或未经授权的变更，会对电子政务系统运行造成危害。包括但不限于：系统规划数据、软件程序数据、运行日志数据、安全管理数据等。

5.2.3 电子政务系统数据分级

依据国家相关法律法规，电子政务系统数据安全遭受破坏，对国家安全、公众权益、个人权益、组织权益等影响，主要考虑以下情况：

a) 影响对象为国家安全的情况，一般指数据的安全性遭到破坏后，可能对国家政权稳固、领土主权、民族团结、社会经济、市场稳定等造成影响。

b) 影响对象为公众权益的情况，一般指数据的安全性遭到破坏后，可能对生产经营、教学科研、医疗卫生、公共交通等社会秩序和公众的政治权利、人身自由、经济活动等造成影响。

c) 影响对象为个人权益的情况，一般指数据的安全性遭到破坏后，可能对敏感个人信息和其他受法律保护的个人权益造成影响。

d) 影响对象为组织合法权益的情况，一般指数据的安全性遭到破坏后，可能对某单位或企业的生产运营、声誉形象、公信力等造成影响。

影响程度包括严重损害、一般损害、轻微损害和无损害，影响程度说明如表2所示。

表 2 影响程度说明

影响程度	参考说明
严重损害	1）可能导致危及国家安全的重大事件，发生危害国家利益或造成重大损失的情况。 2）可能导致严重危害社会秩序和公共利益，引发公众广泛诉讼等事件，或者导致市场秩序遭到严重破坏等情况。 3）可能导致监管部门重要/关键业务无法正常开展的情况。 4）可能导致重大个人信息安全风险、侵犯个人隐私等严重危害个人权益的事件。 5）可能导致电子政务系统各项业务对外无法正常开展的情况。
一般损害	1）可能导致危害社会秩序和公共利益，引发公众广泛诉讼等事件，或者导致市场秩序遭到严重破坏

	等情况。 2）可能导致监管部门业务无法正常开展的情况。 3）可能导致个人信息安全风险、侵犯个人隐私等危害个人权益的事件。 4）可能导致电子政务系统各项业务对外无法正常开展的情况。
轻微损害	1）可能导致监管部门部分业务临时性中断等情况。 2）可能导致个别的组织、个人在电子政务或其他领域中的业务中断等情况。 3）可能导致电子政务系统内部业务临时性中断等情况。 4)可能导致超出个人客户授权加工、处理、使用数据等情况，对个人权益造成部分或潜在影响。
无损害	对组织权益和个人隐私等不造成影响，或仅造成微弱影响但不会影响国家安全、公众权益、市场秩序或者电子政务系统各项业务正常开展。

电子政务系统数据安全分级规则如表3所示。

表 3 电子政务系统数据安全分级规则

参考安全级别	影响范围		数据特征
	对象	程度	
5	国家安全	严重损害/一般损害/轻微损害	• 数据通常主要用于国家监管机构、大型或特大型机构，电子政务系统中重要核心节点类关键业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 数据安全性遭到破坏后，对国家安全造成影响，或对公众权益造成严重影响。
	公众权益	严重损害	
4	公众权益	一般损害	• 数据主要用于电子政务系统中重要核心节点的重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 数据安全性遭到破坏后，对公众权益造成一般影响，或对个人权益或组织权益造成严重影响，但不影响国家安全。
	个人权益	严重损害	
	组织权益	严重损害	
3	公众权益	轻微损害	• 数据用于电子政务系统关键或重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 数据的安全性遭到破坏后，对公众权益造成轻微影响，或对个人权益或组织权益造成一般影响，但不影响国家安全。
	个人权益	一般损害	
	组织权益	一般损害	
2	个人权益	轻微损害	• 数据用于电子政务系统一般业务使用，一般针对受限对象公开，通常为内部管理且不宜广泛公开的数据。 • 数据的安全性遭到破坏后，对个人权益或组织造成轻微影响，但不影响国家安全、公众权益。
	组织权益	轻微损害	
1	国家安全	无损害	• 数据一般可被公开或可被公众获知、使用。 • 个人或组织主体主动公开的信息数据。 • 数据的安全性遭到破坏后，可能对个人权益或组织权益不造成影响，或仅造成微弱影响但不影响国家安全、公众权益。
	公众权益	无损害	
	个人权益	无损害	
	组织权益	无损害	

5.2.4 电子政务系统数据安全的组织保障

组织保障，是电子政务系统数据安全保障能力的重要组成部分，明确数据安全的组织管理、制度管理、人员管理、第三方机构管理，保障电子政务系统数据安全的实施。

5.2.5 电子政务系统数据安全的运维保障

运维保障，是电子政务系统数据安全的运营支撑部分，明确访问控制、安全监测、安全审计、应急处置等过程中的密码应用要求，保障电子政务系统数据安全的运行。

5.2.6 电子政务系统数据安全的安全评估

安全评估，是电子政务系统数据安全的检查评估部分，明确数据采集、数据传输、数据存储、数据处理、数据交换和数据清除的密码应用的评估流程与评估原则，保障电子政务系统数据安全的可靠性。

5.3 数据安全密码应用能力

5.3.1 概述

商用密码技术是电子政务数据安全的重要技术能力，重点实现数据的机密性、完整性、真实性、敏感性，降低数据破坏、泄露的风险。

5.3.2 机密性

使用商用密码技术，对电子政务系统中安全级别三级以上的数据，可采用基于对称密码算、非对称算法的加解密，实现数据的机密性。

5.3.3 完整性

使用商用密码技术，对电子政务系统中安全级别三级以上的数据，可采用基于对称密码算法或密码杂凑算法的消息鉴别码机制，公钥密码算法的数字签名机制，实现数据的完整性。

5.3.4 真实性

使用商用密码技术，对电子政务系统中安全级别三级以上的数据，可采用基于对称密码算法或密码杂凑算法的消息鉴别码机制，公钥密码算法的数字签名机制，实现数据的真实性。

5.3.5 敏感性

使用商用密码技术，对电子政务系统中安全级别二级以上的数据，可采用格式保留加密或差分隐私算法等脱敏技术，有效降低数据的敏感性。

6 电子政务系统商密应用安全性评估中数据生命周期安全防护要求

6.1 数据采集密码应用安全要求

数据采集，指电子政务系统内部新产生数据，以及外部收集数据的阶段。数据采集存在数据源伪造、特权账户滥用、数据泄露、数据篡改、恶意数据注入等安全风险，应基于商用密码技术保障数据来源的真实性，保障采集安全级别3级以上数据的机密性与完整性。

基于商用密码技术的数据采集安全要求如下：

a) 应使用商用密码的电子签名技术，对数据采集的来源的真实性实施保护。
b) 应采用商用密码技术对鉴别类数据的采集时，实施机密性和完整性保护。如口令、生物特征数据等。
c) 应采用商用密码技术对安全级别3级以上的主体类数据采集时，实施机密性和完整性保护。如证件号、手机、定位等数据。
d) 应采用商用密码技术对安全级别3级以上的业务类数据采集时，实施机密性和完整性保护。如电子单证、标书等数据。
e) 应采用商用密码技术对采集数据的应用软件程序，实施完整性保护。
f) 应采用商用密码技术对采集数据过程产生的日志数据，实施完整性保护。

6.2 数据传输密码应用安全要求

数据传输，指电子政务系统将数据从客户端传输到系统，或将数据从系统传输到系统的阶段。数据传输存在数据篡改、 伪造及窃取等安全风险，应基于商用密码技术保障数据在传输过程中的机密性、完整性、真实性。

基于商用密码技术的数据传输安全要求如下：

a) 应采用商用密码技术对安全级别2级以上的数据在公共网络传输时，保障通道安全。
b) 应采用商用密码技术对传输数据的主体身份，实施真实性保护。
c) 应采用商用密码技术对鉴别类数据的传输时，实施机密性和完整性保护。如口令、生物特征数据等。
d) 应采用商用密码技术对安全级别3级以上的主体类数据传输时，实施机密性和完整性保护。如证件号、手机、定位等数据。
e) 应采用商用密码技术对安全级别3级以上的业务类数据传输时，实施机密性和完整性保护。如电子单证、标书等数据。
f) 应采用商用密码技术对数据传输过程产生的日志数据，实施完整性保护。

6.3 数据存储密码应用安全要求

数据存储，指电子政务系统数据以任何数字格式进行存储的阶段。数据存储存在数据泄露、数据篡改等安全风险，应基于密码技术保障数据存储过程中的机密性、完整性。

基于商用密码技术的数据存储安全要求如下：

a) 应采用商用密码技术对鉴别类数据的存储时，实施机密性和完整性保护。如口令、生物特征数据等。
b) 应采用商用密码技术对安全级别3级以上的主体类数据存储时，实施机密性和完整性保护。如证件号、手机、定位等数据。
c) 应采用商用密码技术对安全级别3级以上的业务类数据存储时，实施机密性和完整性保护。如电子单证、标书等数据。
d) 应采用商用密码技术对数据存储过程产生的日志数据，实施完整性保护。

6.4 数据处理密码应用安全要求

数据处理，指电子政务系统在业务或服务的过程中，对数据进行计算、分析、可视化等操作的阶段。数据处理存在越权访问、数据篡改等安全风险，应基于密码技术保障数据处理的完整性、真实性、敏感性。

基于商用密码技术的数据处理安全要求如下：

a) 应采用商用密码技术对数据处理的主体身份，实施真实性保护。
b) 应采用商用密码技术对数据处理的软件程序数据，实施完整性保护。
c) 应采用商用密码技术对鉴别类数据进行可视化时，实施机密性保护，有且只有数据的提供方有明文的可视化能力。如修改口令时可查看口令的明文。
d) 应采用商用密码技术对生物特征数据进行可视化时，实施敏感性保护。如通过遮蔽、偏转等方式降低展示数据的安全级别。
e) 应采用商用密码技术对安全级别3级以上的主体类数据展示时，实施敏感性保护。如通过遮蔽、格式保留加密等方式降低展示数据的安全级别。
f) 应采用商用密码技术对安全级别3级以上的业务类数据展示时，实施敏感性保护。如通过差分等方式降低展示数据的安全级别。
g) 应采用商用密码技术对数据处理过程产生的日志数据，实施完整性保护。

6.5 数据交换密码应用安全要求

数据交换，指电子政务系统将数据以任何数字格式在组织与组织或个人之间进行传递的阶段，数据交换存在数据泄露、数据篡改等安全风险，应基于密码技术保障数据交换的机密性、完整性、真实性、敏感性。

基于商用密码技术的数据交换安全要求如下：

a) 应确保数据交换的各方具有相同的商用密码能力保护数据安全，可实施数据交换。
b) 应采用商用密码技术改变数据的敏感性，降低安全级别，可实施数据交换。
c) 应采用商用密码技术对数据交换的主体身份，实施真实性保护。
d) 应采用商用密码技术对数据交换方的密钥及密钥协商数据，实施机密性和完整性保护。
e) 应采用商用密码技术对鉴别类数据交换，实施机密性和完整性保护。
f) 应采用商用密码技术对安全级别3级以上的主体类数据交换时，实施机密性和完整性保护。
g) 应采用商用密码技术对安全级别3级以上的业务类数据交换时，实施机密性和完整性保护。
h) 应采用商用密码技术对数据交换过程产生的日志数据，实施完整性保护。

6.6 数据清除密码应用安全要求

数据清除，指电子政务系统通过相应操作对存储介质上的数据进行删除。数据清除存在因数据恢复而泄露的安全风险，应基于密码技术保障数据的机密性。

基于商用密码技术的数据清除安全要求如下：

a) 应确保清除数据在商用密码技术的保护下，可实施数据清除。
b) 应采用商用密码技术对数据清除的主体身份，实施真实性保护。
c) 应采用商用密码技术对鉴别类数据多次密文覆盖后，可实施数据清除。
d) 应采用商用密码技术对安全级别2级以上的主体类数据多次密文覆盖后，可实施数据清除。
e) 应采用商用密码技术对安全级别2级以上的业务类数据多次密文覆盖后，可实施数据清除。
f) 应采用商用密码技术对数据清除过程产生的日志数据，实施完整性保护。
g) 应对数据清除相关的密钥数据进行销毁，保障密钥数据不可恢复。

7 电子政务系统密码应用中数据安全管理要求

7.1 管理制度

管理制度要求包括：

a) 应制定电子政务系统密码应用中数据安全管理工作的总体方针和安全策略，阐明电子政务系统密码应用中数据安全工作的总体目标、范围、原则和安全框架等；
b) 应对电子政务系统密码应用管理活动中的数据安全管理内容建立管理制度；
c) 应对数据安全管理人员或操作人员执行的日常管理操作建立操作规程并对执行记录进行妥善保存；
d) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系；
e) 应指定或授权专门的部门或人员负责电子政务系统密码应用中数据安全管理制度的制定；
f) 应明确电子政务系统密码应用中数据安全管理制度的发布流程并进行版本控制；
g) 应定期对电子政务系统密码应用中数据安全管理制度的合理性和适用性进行认证和审定，对存在不足或需要改进的安全管理制度进行修订。

7.2 人员管理

人员管理要求包括：

a) 电子政务系统相关人员应了解并遵守数据安全相关法律法规；
b) 应根据实际情况设置密码应用中数据安全管理、审计和操作岗位，明确岗位在电子政务系统中的职责；
c) 应在人员录用、调离等过程中，对涉及数据安全工作的操作和管理人员身份、背景、专业资质、涉密情况等开展审查；
d) 应对涉及数据安全工作的操作和管理人员进行专门培训，确保其具体岗位所需专业技能；

e） 应定期对涉及数据安全工作的操作和管理人员进行考核；
f） 应涉及数据安全工作的操作和管理人员建立保密制度，签订保密合同，承担保密义务；
g） 应根据人员角色（包括内部人员、外部合作人员、运维人员等），加强对数据的访问控制；
h） 将能获知重要数据和核心数据内容的人员确定为关键岗位人员，明确数据处理行为规范和安全保护责任，签署责任书。

7.3 权限管理

权限管理要求包括：
a） 应制定电子政务系统权限管理与审批制度，根据实际情况建立多级审核工作机制和流程，并根据岗位、人员变动情况及时更新审核事项涉及部门和人员；
b） 应分别设置数据安全管理、审计和操作人员的权限，严格控制超级管理员权限账号数量，加强数据安全访问控制；
c） 应对数据处理平台或系统账号的分配、开通、使用、注销等进行严格管理，并按照业务需求、安全保护策略及最小授权原则合理分配数据处理权限；
d） 应定期对权限分配情况进行复核，严禁非授权访问数据。

7.4 建设运行

建设运行要求包括：
a） 应依据数据安全相关标准和需求，在系统密码应用方案中涵盖数据安全管理方案；
b） 电子政务系统在运行过程中，应严格执行既定的数据安全管理制度，应开展数据安全性评估，评估的内容包括数据管理能力、数据安全防护能力等情况，分析数据被未经授权的访问、控制、处理或数据被泄露、窃取、篡改、滥用等风险，形成相应的数据安全评估报告，并根据评估结果进行整改。

7.5 日志留存

日志留存要求包括：
a） 应对电子政务系统数据收集、存储、使用加工、传输、提供、公开、销毁、出境、转移、委托处理等环节实施日志留存管理；
b） 日志记录信息应包括执行时间、操作账号、处理方式、授权情况、登录信息等，并保证日志记录完整、准确；
c） 日志的留存时间应不低于 6 个月；
d） 应对日志操作进行权限控制，设置日志审计员加强日志访问和处理管理。

7.6 安全审计

安全审计要求包括：
a） 应建立电子政务系统数据安全审计相关制度，明确审计目的、审计对象、审计操作规程、审计频度、审计内容、审计报告要素等；
b） 应明确数据安全审计工作涉及部门和人员的权限、责任以及相关权限的授予规程；
c） 应明确数据安全审计的内容，包括内部权限控制、数据流动跟踪情况、数据安全事件、数据安全防护措施有效性等；
d） 应在使用审计系统开展数据安全审计的过程中准确记录对数据的操作时间、操作地点、操作人、操作方式、操作的数据内容等信息，以及审计发现的相关安全事件；
e） 应记录并形成数据安全审计报告，并制定计划整改审计发现的问题。

7.7 应急处置

应急处置要求包括：

a) 应根据实际情况建设电子政务数据安全风险监测预警能力，重点面向操作系统、交换机、数据服务器、网络边界、应用软件、数据库、政务云平台等开展数据安全风险监测，根据电子政务数据特征及面临的典型风险进行针对性监测分析，排查安全隐患，采取必要措施防范数据安全风险；

b) 应将可能造成较大及以上安全事件的或涉及重要数据和核心数据的安全风险向有关部门报告，报告内容包括风险所处系统、风险类型、风险级别、风险后果影响等；

c) 应制定数据安全事件应急预案，定期组织开展应急演练并保存演练记录；

d) 应在数据安全事件发生后，按照应急预案开展应急处置，涉及重要数据和核心数据的安全事件，应第一时间向有关部门报告。对可能损害用户合法权益的数据安全风险或事件，应告知用户，并提供减轻危害的措施；

e) 事件处置完成后，应在规定期限内形成总结报告，每年向有关部门报告数据安全事件处置情况。总结报告内容包括事件原因、事件后果、影响范围、事件责任、处置过程和结果、工作经验等。

8 电子政务商密应用安全性评估中数据安全测评规范

8.1 评估总体原则

8.1.1 总体框架

电子政务系统商密应用安全性评估中数据安全评估主要利用人员访谈、文件审查、配置检查及测试验证等多种方法评估开展商密应用安全性评估后的电子政务系统在各类数据处理活动及数据承载系统平台的保障措施合规情况，从通用性管理与全生命周期管理两方面出发，针对各个指标项明确评估涉及的重要管理措施、重点技术措施及判断标准，明确被评估事项合规性保障基线，以提升数据安全管理及相关技术保障措施能力水平。评估框架如图 2 所示。

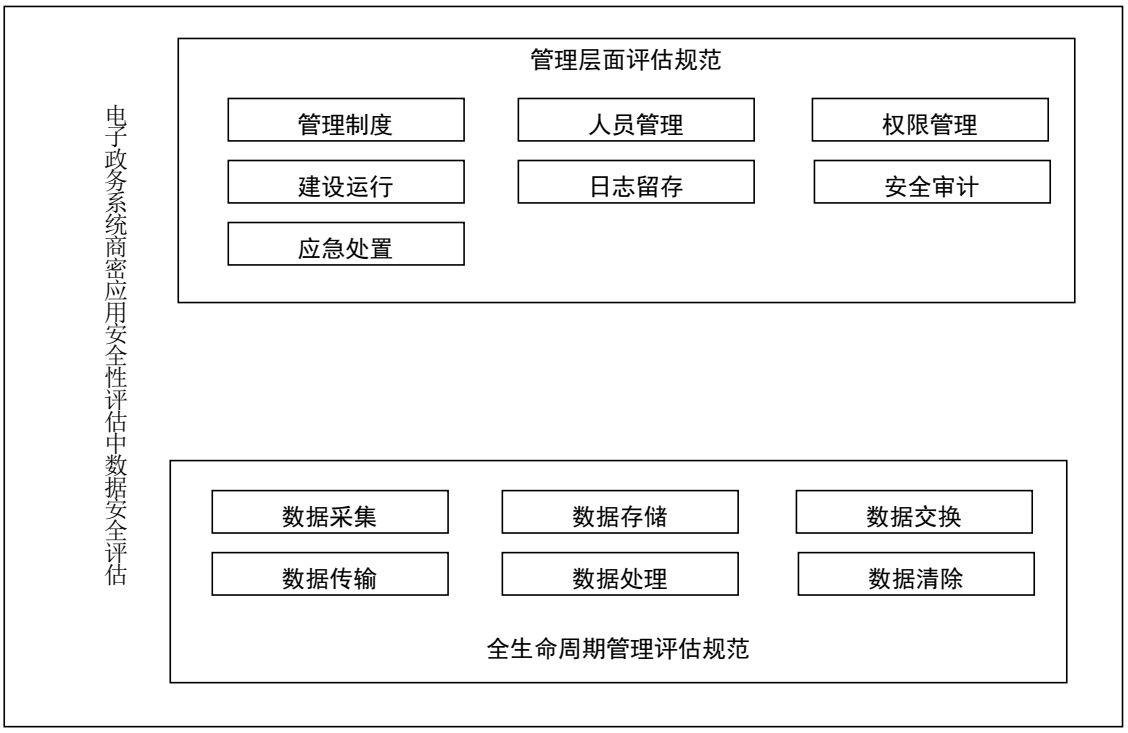

图2 数据安全评估总体框架

8.1.2 评估原则

标准性原则：指遵循电子政务系统相关标准开展数据安全评估工作。

客观公正原则：指评估人员在评估活动中应充分收集证据，对评估对象实施的安全措施的有效性和可靠性做出客观公正的判断。

可重复和可再现原则：指在相同的环境下，对同一评估对象，不同的评估人员依照同样的要求，使用同样的方法，对每个评估实施过程的重复执行都应得到同样的评估结果。

可控性原则：在评估过程中，应保障参与评估的人员、使用的技术和工具、评估过程都是可控的。

完备性原则：严格按照被评估对象所涉及的评估范围进行全面的评估。

最小影响原则：从相关管理层面和工具技术层面，将评估工作对数据和承载数据的应用、系统、网络正常运行的可能影响降低到最低限度，不会对被评估对象涉及的应用、系统、网络运行产生显著影响。

保密原则：指评估人员开展数据安全评估工作前，需要与被评估单位就数据安全保密责任义务进行认定与划分，包括不限于保密协议签署等，应对评估中获取的相关信息、评估过程文档等严格保密，以保障被评估方的数据安全。

8.2 评估启动条件

满足下列情形之一的，开展商密应用安全性评估评后的电子政务系统应及时启动数据安全评估：

a) 业务运营阶段，在数据承载环境发生较大变化时开展评估：如数据采集渠道变更、数据存储系统升级改造、数据处理技术变更等；
b) 应在开展数据重要操作（如开放数据对外接口、数据共享、数据转移、数据加工、数据出境等）前对涉及到的数据相关管理措施、技术措施开展评估；
c) 行业主管部门要求单位进行数据安全评估的；
d) 满足国家法律法规有关情形时，应开展数据安全评估。

8.3 评估流程

8.3.1 评估准备阶段

8.3.1.1 组建评估团队

应组建适当的评估团队，包括评估管理单位、责任单位和开发运营单位，评估人员需具备数据安全评估相关能力，以支撑整个评估过程的推进及有效开展。当被评估组织委托安全服务机构开展数据安全评估时，应与被委托单位共同组建评估团队。

8.3.1.2 确定评估范围

应根据数据评估对象进行评估范围界定，确定数据涉及的生命周期阶段，以及各阶段所涉及的应用、系统、平台范围。

数据评估对象可以为具有收集、使用用户个人信息功能的业务，涉及存储用户个人信息和核心网络数据的业务支撑系统等，例如，评估范围可界定为行业热点业务、业务支撑网运营管理系统、大数据分析系统等。

8.3.1.3 评估对象调研

评估团队应对被评估单位的数据安全相关工作进行充分调研，调研内容包括被评估单位数据安全管理相关制度和流程、数据安全设备部署情况等，从而为后续数据安全评估实施奠定基础。

8.3.2 评估实施阶段

评估组织实施阶段，对标数据安全基线要求，采用包括人员访谈、文件审查、配置检查及测试验证等方式对管理措施和技术措施进行评估，对不合规项逐项提出针对性整改建议。数据安全评估团队评估实践过程中，应当对评估佐证材料进行收集、整理，做好评估过程记录。

评估实践过程通常可包括数据安全初评实践、数据安全复评实践两部分：

a)数据安全初评实践：指数据安全评估团队在完成评估准备阶段后，对评估对象的初步评估。数据安全评估团队应根据初步评估结果，结合评估对象实际情况，对评估不合规项逐项提出针对性整改建议，给出评估对象初评结论。

b)数据安全整改复核：指数据安全评估团队在评估对象完成整改或达到整改期限后， 对评估对象的整改复核评估。数据安全评估团队应根据初步评估结果及整改建议， 检查评估对象整改措施有效性、合规性，确定评估对象是否完成整改，给出评估对象复评结论。

具体评估方法包括但不限于以下方法：

——文档审查。文档审查是指评估人员查阅数据安全相关文件资料，如单位数据安全管理制度、业务技术资料和其他相关文件，用以评估数据安全管理相关制度文件是否符合标准要求的一种方法。通常在评估准备阶段以及数据安全管理类基线评估部分使用该方法，单位需要事先完整准备上述文档以供评估人员查阅。

——人员访谈。人员访谈是指评估人员通过与被评估单位相关人员进行交流、讨论、询问等活动，以评估数据安全保障措施是否有效的一种方法。通常在评估过程中深入单位实地调研时使 用，单位需要安排熟悉数据流转过程，以及承载数据的应用、系统、网络情况的人员参加访谈。

——配置检查。配置检查是指单位相关人员演示、评估人员查看承载数据的应用、系统、网络，包括数据采集界面、数据展示界面、数据存储界面、数据操作日志记录等，以评估数据安全保障措施是否有效的一种方法。通常在评估过程中深入现场调研时使用，被测单位需要安排相关人员进行现场演示，评估人员根据配置检查情况进行查验。如系统存在高度保密性、可用性的要求，评估可通过事后提供日志列表或测试环境等方式进行。

——测评验证。测评验证是指评估人员通过实际测试承载数据的应用、系统、网络，查看、分析被测试响应输出结果，以评估数据安全保障措施是否有效的一种方法。通常是评估人员针对数据全生命周期涉及的相关技术指标进行验证时使用，评估人员需要事先进行业务注册、准备验证工具等以完成相关评估指标。

8.3.3 评估总结阶段

评估总结阶段包括召开专家评审会，对评估实施过程及评估意见、评估整改落实情况进行核验，确认评估评估对象是否已经配套数据安全管理措施和数据安全技术措施，满足数据安全基线要求，并撰写形成评估报告。

8.4 评估报告规范要求

数据安全评估报告应当包括以下组成部分：

a) 概述，包括被评估单位数据安全管理情况、被评估业务或系统平台具体功能及数据安全情况；

b) 数据安全评估流程，包括评估工作情况概述、评估人员组成、评估实施流程等；

c) 数据安全评估矩阵，根据通用性管理评估规范及全生命周期管理评估规范，梳理总结出合规性评测矩阵表；针对每一项评估指标，综合运用多种评估方法，收集佐证材料；对佐证材料进行研判评估，得出数据安全保障措施合规或完善程度有关结论；

d) 问题分析，根据评估结论梳理评估指标项中不合规项，指出存在问题；

e) 整改建议，依据存在问题逐项提出有针对性整改建议；

f) 整改落实情况，如涉及整改，需体现整改方案及整改措施、结果；

g） 复核结果及签字（建议盖章）。

附 录 A
（资料性）
电子政务数据分类方法参考示例

参照 5.2.2 系统运行场景和商用密码应用性安全评估规则，将电子政务数据分为四种类型，包括鉴别类数据，主体类数据、业务类数据、系统类数据。以民政电子政务数据为例给出分类示例如表 A。

表A 民政电子政务数据分类示例

数据分类名称	示例数据	备注
鉴别类数据	如：普通用户、管理员用户等登录口令	
主体类数据	如：姓名、性别、身份证号、电子邮箱、手机号等	
业务类数据	收入情况、患病情况、医疗救助日期、救助金额、支出费用总计、受理数量、审核状态、救助类型、同步状态、同步时间、审批意见等	
系统类数据	用户访问记录、业务操作日志、系统运行日志等	

附 录 B
（资料性）
电子政务数据分级方法参考示例

参照 5.2.3 电子政务系统数据分级，将电子政务数据影响分为四种类型，包括严重损害、一般损害、轻微损害和无损害四种程度。通过综合影响范围，设置五级参考安全级别。根据上述原则，基于疫情防控数据我们给出相应电子政务数据分级参考示例如表 B.1。

表B.1 疫情防控数据分级示例

待操作数据项或数据集合	数据量	安全级别	保护手段	保护方式
仅1列手机号或身份证号	1-50行	1级	可不加密	可公开
	50行以上	2级	密码技术	完整性
姓名、身份证号、手机号任2列	1行以上	3级	密码技术	机密性、完整性
多字段数据（含个人信息、敏感个人信息）	1行以上	3 级	密码技术	仅对敏感个人信息实现机密性、完整性保护

另外，由于个人信息属于涉及法律法规有专门管理要求的数据类别，应按照有关规定或标准对个人信息、敏感个人信息进行识别和分类。个人信息分类示例如表 B.2

表B.2 个人信息分类示例

分类	数据项	保护方式	备注
个人信息	身高	可不加密	可公开
	体重	可不加密	可公开
	生日	可不加密	可公开
	性别	可不加密	可公开
	民族	可不加密	可公开
	国籍	可不加密	可公开
敏感个人信息	姓名	密码技术	机密性、完整性
	身份证件号码	密码技术	机密性、完整性
	手机号码	密码技术	机密性、完整性
	电子邮箱	密码技术	机密性、完整性
	银行帐号	密码技术	机密性、完整性