ICS 35.030
CCS L70

团　　体　　标　　准

CQAE*****—2025

数据安全运营能力评估规范

Specification for evaluation of Data Security Operation Capability

（报批稿）

202X-XX- XX 发布　　202X-XX- XX 实施

中国电子质量管理协会　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。

本文件由北京数企云服信息技术有限公司提出。

本文件由中国电子质量管理协会归口。

本文件起草单位：核电运行研究（上海）有限公司、内蒙古蒙壹购壹商贸有限公司、上海建工电子商务有限公司、上海互知光科技有限公司、河南许继仪表有限公司、招商局检测车辆技术研究院有限公司、浙江迈新科技股份有限公司、江苏省软件产品检测中心、深圳正元星捷信息科技有限公司、健康小屋大数据有限公司、国网思极检测技术（北京）有限公司、重庆安标检测研究院有限公司、四川省中认信安技术服务有限公司、国家工业信息安全发展研究中心、重庆信安网络安全等级测评有限公司、山西省信息产业技术研究院有限公司、山东金钟科技集团股份有限公司、河北华测信息技术有限公司、中国电力科学研究院有限公司、内蒙古电力（集团）有限责任公司内蒙古电力科学研究院分公司、西藏高驰信息安全技术有限责任公司、中国移动通信集团西藏有限公司、SGS通标标准技术服务（上海）有限公司、广西电网有限责任公司信息中心、国家高速列车青岛技术创新中心、中国民用航空总局第二研究所、中汽院（深圳）科技有限公司、中移物联网有限公司、杭州麟云科技有限公司、湖南浩基信息技术有限公司、湖南省电子信息产业研究院、吉林省赛宝信息服务有限公司、江西省网络安全研究院、临汾云时代技术有限公司、陕西卓信信息技术服务有限公司、深圳市天龙腾科技有限公司、新疆量子通信技术有限公司、重庆巽诺科技有限公司、云南电网有限责任公司信息中心、云上广济（贵州）信息技术有限公司、可安评估有限公司、鄂尔多斯市政务服务中心、北京亿安天下科技股份有限公司、上海天泰网络技术有限公司、交信（浙江）信息发展股份有限公司、国网山东省电力公司、北京金智达管理顾问有限公司、中国电子信息产业集团有限公司第六研究所、贵州省网络与信息安全测评认证中心、南京大数据集团有限公司、郑州郑大信息技术有限公司、江西省科技基础条件平台中心、中国电子质量管理协会软件与信息技术专业委员会、北京中标服检验技术研究院有限公司、广东优科检测技术有限公司、北京技考帮教育科技有限公司、北京数企云服信息技术有限公司、北京中电标研技术中心、北京北方华测认证服务有限公司、北京中达信成科技有限公司。

本文件主要起草人：刘祯、刘旭嘉、王潇耿、解鸿斌、侯超、陈可、周雨欣、刘刚、孔群景、杨锦业、张延国、张明媛、尧剑飞、倪世贤、吴超、周鹏、李军厚、金翅翔、张晖、王磊、吴真炜、聂文江、龚诗然、张伟、樊佩茹、江浩、张卓晖、王利斌、林亮成、李永刚、石发强、金文志、罗俊海、吴海林、吴徐龙、刘一廷、傅秋雨、荆艳飞、林峰、闫士华、高业尚、杨知、王云龙、李勇、刘妍蕾、郭亮亮、赵彬宏、王兵兵、王晓东、杨伟伟、刘敬仪、郑海燕、平措占堆、马腾、孟椿智、艾徐华、潘俊冰、杜杰伟、于金山、秦振华、杨长幸、刘春阳、张晨、刘利军、黄小芹、张辉、刘洋、邹远辉、李源、孟庆阳、万鹏、孙烨、刘洋、李青青、史强、张羿、宗鹏飞、张家林、刘涛、张梅、王俊彪、王小龙、武玉平、许德忠、李红明、庞海浪、朱敏、赵建飞、田江磊、杨威、陈剑飞、魏昌超、赵本金、刘朝晖、李红灯、邢凯龙、陈伟、耿琦、周源、付康、饶兰香、孙丹、胡敏、王蕾、王伟、张玉、张百川、张伟、陈通、石跃超、张宏波、马啟田、邹金林、刘道军、李美丽、胡蝶、温章义、马廉杰、谢黑尔扎提·努尔买买提、梁峰、邢献红、吴寒、陈以腊、蒋欣睿、姚固、陈中华。

数据安全运营能力评估规范

1 范围

本文件规定了组织数据安全运营的评估项目、能力要求、评估方法等。

本文件适用于组织对内开展数据安全运营能力评价，同时适用于组织、服务机构和第三方评估机构作为运营服务提供者的运营能力评价。

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/T1.1-2020 《标准化工作导则 第1部分：标准化文件的结构和起草规则》

GB/T 25069-2022 《信息安全技术 术语》

GB/T 43697-2024 《数据安全技术 数据分类分级规则》

YD/T 4246-2023 《电信网和互联网数据异常行为监测技术要求与测试方法》

在本标准中，**黑体字部分**表示较高等级中增加或增强的要求。

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据 data

任何以电子或者其他方式对信息的记录。

3.2

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.3

数据安全运营 data security operation

通过系统性、规范化的管理和技术措施，协调数据采集、传输、存储、处理、共享及销毁等数据处理活动及其处理者，确保数据的机密性、完整性、可用性以及合规性的持续性活动。

3.4

运营能力 operation capability

在业务活动全过程中，保障数据安全、流程规范及合规性要求，实现动态化资源整合、风险管控和效能优化的能力。

3.5

敏感数据 sensitive data

一旦泄露、非法提供或滥用,可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息,以及一旦泄露、非法提供或滥用，可能导致企业信誉、财产安全受到严重危害或企业竞争力下降的企业数据。

注:例如种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等个人信息，企业经营情况、企业网络结构、IP地址列表等企业数据。

[来源：YD/T 4246-2023，3.1.3]

3.6

威胁 threat

可能对系统或组织造成危害的不期望事件的潜在因素。

[来源:GB/T 25069-2022,3.6]

3.7

数据异常行为 abnormal behavior data

针对数据所进行的异常的、不符合管理要求的、与预期不符的访问和利用的行为，包括并不限于对数据超频次访问、越权访问、绕行访问、非常规时间访问等。

[来源：YD/T 4246-2023，3.1.6]

3.8

画像 profiling

针对某类对象,在多维度上构建其描述性标签属性,并利用这些标签属性,分析对象多方面的特征,抽象概括其全貌的过程。

3.9

预警 warning

针对即将或正在发生的网络安全事件或威胁,提前或及时发出的警示。

3.10

风险评估 risk assessment

风险识别、风险分析和风险评价的全过程。

[来源：GB/T 29246-2017，2.71，有修改]

4 评估原则

数据安全运营能力评估应遵循以下六项原则，涵盖法律约束、流程规范及技术要求，确保评估活动的合法性、客观性与可操作性。

a） 合法性原则：评估活动应严格遵循国家法律法规及行业规范要求；

b） 客观公正原则：评估人员应基于证据链完整性与方法一致性，对安全措施的有效性进行独立判定，避免利益冲突；
c） 完备性原则：评估范围应覆盖被评估对象所涉及的评估范围及其技术、管理、合规三个基本层面；
d） 可复现原则：评估过程应满足可重复验证性；
e） 最小影响原则：评估活动应避免对被评估对象所涉及的业务系统的干扰；
f） 保密性原则：评估机构应采取一定的控制措施，确保被评估对象的商业秘密不被泄露。

5 评估总要求

5.1 评估内容

数据安全运营是通过系统性、规范化的管理和技术措施，协调数据采集、传输、存储、处理、共享及销毁等数据处理活动及其处理者，确保数据的机密性、完整性、可用性以及合规性的持续性活动，是组织的数据安全团队与其他部门进行沟通、协作及价值输出的重要枢纽。

组织的数据安全运营能力是指组织能够在业务活动全过程中，通过数据、模型、工具等手段以及一系列的运营工作，保障数据安全、流程规范及合规性要求，实现数据安全赋能业务发展的整体目标。组织的数据安全运营能力要求包括运营基础要求、专业技术要求和运营优化要求三个方面，具体见图1。

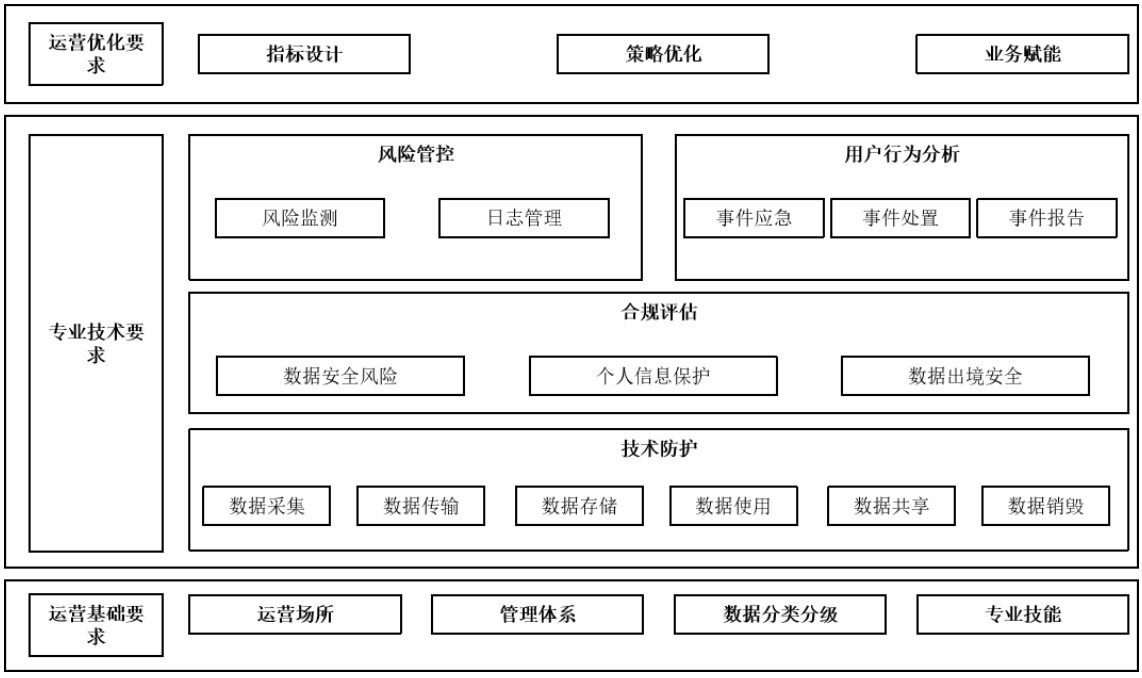

图 1 数据安全运营能力架构图

5.2 评估等级

数据安全运营能力等级共分为三级。三个级别的能力要求为从低到高、递进包含的关系，即高等级的能力要求应包括所有低等级能力要求。具体见表1。

表1 能力等级

能力等级	等级要求
一级	在这一等级，组织具备基本的数据安全运营基础设施、专业技术及管理措施、运营指标和策略。组织应： a） 具备开展运营工作的场地及团队人员； b） 初步识别敏感数据、常见数据安全风险； c） 具备基础的数据安全技术措施； d） 能够对数据安全事件进行响应、处置、报告； e） 具备简易的运营指标，能够对运营策略进行管理、展示。
二级	在一级的基础上，组织具备较为完备的数据安全运营基础设施、专业技术、合规、管理措施、运营指标和策略。组织应： a） 具备功能分区合理的运营工作场所，团队人员具备数据安全运营相关专业技能； b） 建立数据分类分级规则，具备分类分级工具、风险监测平台等自动化工具； c） 对部分数据处理活动或生命周期环节实施数据安全技术防护，并结合实施效果部署数据安全运营工作； d） 基于合规评估结果部署数据安全运营工作； e） 建立数据安全事件处置流程，具备安全编排与自动化响应平台； f） 具备体系化的运营指标，具备工单系统，能够对运营策略、工作进行自动化调度、管理，并对业务数据安全工作产生积极影响。
三级	在一级、二级的基础上，组织具备智能化的数据安全运营基础设施及其他技术、管理工具。组织制定了完善的运营指标和策略，能够通过智能化工具进行持续优化。组织应： 组织应： a） 部署智能化的运营平台工具，团队人员在数据安全运营领域具备较高的专业技能水平； b） 具备智能化的分类分级工具、风险监测平台，支持数据分类分级运营、数据安全风险预警与运营等相关工作； c） 基于数据全生命周期实施数据安全技术防护，并结合实施效果部署数据安全运营工作； d） 实现合规评估与数据安全运营的一体化； e） 接入外部威胁预警信息平台，实现数据安全事件的处置； f） 实现运营团队与业务部门有效协作，能够量化、规划数据安全运营对组织业务的贡献及运营资源投入。

5.3 评估方法

数据安全运营能力通过文档查验、人员访谈、配置核查三种方法进行评估。

a）文档查验是指评估人员查阅数据安全相关文件资料，例如组织数据安全管理制度、业务技术资料和其他相关文件，用以评估数据安全治理相关制度文件是否符合标准要求；

b）人员访谈是指评估人员通过与评估对象相关人员进行交流、讨论、询问等活动，以评估数据安全保障措施是否有效；

c）配置核查是指评估人员检查承载数据的应用、系统、网络设备的安全配置，以评估以确认其符合预定义的安全策略、技术标准及法律法规要求。

6 运营基础要求

6.1 概述

运营基础要求是指组织建立数据安全运营所必需的场所、管理体系，结合数据分类分级结果，明确开展运营工作的重点领域，并通过专业团队、人员技能构建运营能力底座的基础性要求。

6.2 运营场所

6.2.1 一级要求

一级能力要求包括：

a) 组织应具备开展数据安全运营的场所；
b) 组织的数据安全运营场所应能够满足基本的物理环境安全要求；
c) 涉及第三方安全服务的，组织的数据安全运营场所应能够对第三方安全服务进行整合。

6.2.2 二级要求

二级能力要求包括：

a) 满足 6.2.1 的全部要求；
b) **组织应掌握数据安全运营场所内核心资源的配置控制权；**
c) **组织应基于业务场景与风险等级，对数据安全运营场所进行功能分区设计，应至少具备日常运营区、应急指挥区，各功能区应实现物理隔离。**

6.2.3 三级要求

三级能力要求包括：

a) 满足 6.2.1 和 6.2.2 的全部要求；
b) 组织应规划数据安全运营场所内的硬件设施、软性服务，降低第三方服务中断或数据泄露风险。

6.3 管理体系

6.3.1 一级要求

一级能力要求包括：

a) 组织应具备数据安全管理的组织架构、工作流程和管理制度；
b) 组织应具备负责数据安全运营工作的团队或人员，并明确其职责、权限。

6.3.2 二级要求

二级能力要求包括：

a) 满足 6.3.1 的全部要求；
b) **组织应制定数据安全运营的管理制度、规范手册，明确运营工作的基础操作流程；**
c) **组织的数据安全运营团队或人员应定期开展数据安全培训与文化建设；**
d) 涉及与外部机构开展数据合作的，组织应与外部机构签订协议，明确数据合作中的数据处理目的、双方权利、安全责任义务及事件协作与报告机制，并结合数据合作情况，定期对外部机构的安全资质进行审核，在合作期间持续监控评估三方的安全能力。

6.3.3 三级要求

三级能力要求包括：

a) 满足 6.3.1 和 6.3.2 的全部要求；
b) **组织应定期对数据安全运营的管理制度、规范手册进行审核、维护更新；**
c) **组织的数据安全运营团队或人员应定期评估运营工作情况，开展数据安全运营检查、问题整改与跟踪。**

6.4 数据分类分级

6.4.1 一级要求

一级能力要求包括：

a) 组织应能够依据国家法律法规及行业规范要求，将数据划分为核心数据、重要数据、一般数据；
b) 组织应能够识别国家核心数据、重要数据对应的合规义务，如涉及国家核心数据、重要数据，应按有关部门规定开展风险评估、数据目录报送等工作；
c) 组织应能够识别一般数据中较为敏感的数据，明确组织一般数据的类别、级别，并识别各级数据在数据处理活动中的相关方及其安全责任；
d) 组织应具备数据资产清单，定期开展数据资产清单的更新、维护；
e) 组织应明确数据的类别、级别发生变更的情形及相应的变更流程、记录要求。

6.4.2 二级要求

二级能力要求包括：

a) 满足 6.4.1 的全部要求；
b) **组织应具备数据分类分级保护的管理制度、规范手册，明确不同级别数据的安全保护要求和技术措施，并定期对管理制度、规范手册进行更新、维护；**
c) 组织应具备数据识别、数据分类分级的自动化工具，对组织数据资产进行识别、分类分级管理。
d) 组织应能够将数据分类分级结果应用于合规评估、事件响应等数据安全运营工作。

6.4.3 三级要求

三级能力要求包括：

a) 满足 6.4.1 和 6.4.2 的全部要求；
b) **组织应部署数据分类分级的智能化工具，提升对非结构化数据资产识别能力的深度、精度。**

6.5 专业技能

6.5.1 一级要求

一级能力要求包括：

a) 组织应具备负责数据安全运营的专业团队或人员；
b) 组织数据安全运营的专业团队或人员应掌握使用组织安全设备的理论知识、实践操作经验。

6.5.2 二级要求

二级能力要求包括：

a) 满足 6.5.1 的全部要求；
b) 组织数据安全运营的专业团队或人员应具备常见的网络数据安全事件处置、威胁或漏洞分析能力；
c) 组织数据安全运营的专业团队或人员应能够依据国家法律法规及行业规范要求，在组织发生数据安全事件时，及时开展事件响应与处置，并在事件结束后对组织的数据安全运营的管理制度、规范手册进行更新、维护；
d) 组织数据安全运营的专业团队或人员应具备跨部门协同和资源调度的能力，能够根据组织的数据安全运营的管理制度、规范手册，调整资源分配优先级；
e) 组织数据安全运营的专业团队或人员应能够具备数据安全培训与文化建设的能力，能够分析组织高频发生的风险场景，设计数据安全培训课程，并组织相关部门、人员参与培训；
f) 组织数据安全运营的专业团队或人员应定期参与数据安全运营相关培训；
g) 组织数据安全运营的专业团队或人员应定期参与数据安全运营相关演练，演练结果应纳入组织的人员绩效考核；
h) 组织数据安全运营的专业团队应具备一定比例的高等级成员，高等级成员应对国际、国内的网络或数据安全现行标准有一定的理解，且熟悉组织所在的行业法规、标准。

6.5.3 三级要求

三级能力要求包括：

a) 满足 6.5.1 和 6.5.2 的全部要求；
b) 组织数据安全运营的专业团队中的高等级成员应具备高级技术专业职称，对国际、国内的网络或数据安全标准有深刻地理解，并能够将自身的经验与知识输入到团队建设中；
c) 组织数据安全运营的专业团队应具备一定比例的业务安全架构师，业务安全架构师应具备数据安全相关技术培训经历和 TOGAF 架构设计经验；
d) 组织数据安全运营的专业团队应定期参与由外部专业机构组织开展的能力评估或技能认证。

7 专业技术要求

7.1 概述

专业技术要求是指建立组织数据安全运营所需的技术防护体系，结合合规评估，推动完善组织的数据安全风险监测、识别、处置、治理机制和事件应急处置流程，从而串联组织组织各项运营工作的专业性要求

7.2 技术防护

7.2.1 一级要求

一级能力要求包括：

a) 涉及开展数据采集活动的，组织应具备数据采集安全相关的技术工具，支持采集日志记录，确保采集活动及数据的安全性、合规性、可追溯性；
b) 涉及开展数据传输活动的，组织应具备数据传输安全相关的技术工具，支持传输数据加密、校验码，确保传输活动及数据的安全性、合规性；
c) 涉及开展数据存储活动的，组织应具备数据存储安全相关的技术工具，能够对数据存储系统、存储介质及逻辑存储空间等进行安全管理，具备备份与恢复的功能；确保存储活动、存储及备份数据的安全性、合规性、可用性；
d) 涉及开展数据使用活动的，组织应具备数据使用安全相关的技术工具，实现数据在加工、分析等环节的日志记录、权限管理和访问控制，确保使用活动及数据的安全性、合规性；
e) 涉及开展数据共享活动的，组织应具备数据共享安全相关的技术工具，确保共享活动及数据的安全性、合规性；
f) 涉及开展数据销毁活动的，组织应具备数据销毁安全相关的技术工具，确保销毁活动及数据的安全性、合规性。

7.2.2 二级要求

二级能力要求包括：

a) 满足 7.2.1 的全部要求；
b) **涉及开展数据传输活动的，组织的数据传输安全相关技术工具应支持签名验签；涉及对核心数据、重要数据及其他敏感数据传输的，应能够依据国家法律法规及行业规范要求，采用加密、去标识化、匿名化、传输通道加密等技术；**
c) **涉及开展数据存储活动的，组织的数据存储安全相关的技术工具应能够满足不同数据的加密存储要求，组织应定期对存储系统的安全配置进行扫描；**
d) **涉及开展数据使用活动的，组织的数据使用安全相关技术工具应能够支持静态脱敏、动态脱敏，并能够对敏感数据的脱敏操作进行日志记录和定期审计；**
e) **涉及开展数据共享活动的，组织的数据共享安全相关的技术工具应能够满足不同数据的共享安全要求，支持对数据共享活动及相关接口的安全管控、监控审计；涉及对核心数据、重要数据及其他敏感数据共享的，应能够依据国家法律法规及行业规范要求，采用数据加密、隐私计算、安全共享交换区域、数据水印等技术；**
f) **涉及开展数据销毁活动的，组织应定期抽样检查销毁活动的有效性。**

7.2.3 三级要求

三级能力要求包括：

a) 满足 7.2.1 和 7.2.2 的全部要求；
b) **涉及开展数据采集活动的，组织应具备对数据采集来源进行统一管理的技术工具；**
c) **涉及开展数据传输活动的，组织应具备基于数据类型和级别的加密模块；**
d) **涉及开展数据存储活动的，组织应具备对存储介质进行统一管理的技术工具；**
e) **涉及开展数据使用活动的，组织的数据使用安全相关技术工具应支持对数据使用量、使用频次、导出下载量等进行记录；组织应制定判断数据异常行为的规则，并对数据的违规使用行为进行识别、预警；**
f) **涉及开展数据共享活动的，组织的数据共享安全相关的技术工具应支持基于接口调用的风险画像，展示数据共享活动及相关接口的安全风险状态。**

7.3 合规评估

7.3.1 一级要求

一级能力要求包括：

a) 组织应制定数据安全合规评估的管理制度、规范手册，明确数据安全运营团队或人员的职责、评估实施场景、方式、流程、频率及结果报告的要求；
b) 组织应能够对数据安全合规评估所发现的风险或问题进行改进，持续跟踪改进措施的效果。

7.3.2 二级要求

二级能力要求包括：

a) 满足 7.3.1 的全部要求；
b) 组织应建立合规评估和检查清单，能够依据国家法律法规及行业规范要求，对数据安全风险、个人信息保护、数据出境安全进行合规评估、检查和报告；
    1) 数据安全风险相关评估应重点关注数据处理活动中是否对数据主体构成风险，组织运营团队应基于风险等级，制定差异化的监控策略；
    2) 个人信息保护相关评估应重点关注处理个人信息的过程中是否对个人信息主体合法权益造成不利影响，组织运营团队应结合数据分类分级标准和结果，定期复核脱敏、加密等技术措施的有效性；
    3) 数据出境安全相关评估应重点关注数据出境活动是否对国家安全、公共利益、个人或者组织合法权益构成风险。
c) 组织的数据安全运营团队或人员应能够结合数据安全合规评估结果，对运营资源进行分配。

7.3.3 三级要求

三级能力要求包括：

a) 满足 7.3.1 和 7.3.2 的全部要求；
b) 组织的数据安全合规评估工作规划应与数据安全运营工作规划有效对接，从而明确安全资源投入；
c) 组织宜部署数据安全合规管理平台或其他技术工具，能够自动检测合规风险问题，并将合规风险问题推送至数据安全运营工单系统，从而实现评估与运营的一体化。

7.4 风险管控

7.4.1 一级要求

一级能力要求包括：

a) 组织应制定数据安全风险管控的管理制度、规范手册，明确数据安全风险的类别和级别，并将风险类别、级别与运营工作流程进行映射、匹配；
b) 组织应制定日志的管理制度、规范手册，明确日志记录的范围、格式、保存时间、存储备份、日志访问及使用权限等要求；

c） 组织应部署日志管理平台，日志管理平台应支持将异常登录、批量导出等日志事件推送至数据安全运营工单系统。

7.4.2 二级要求

二级能力要求包括：

a） 满足 7.4.1 的全部要求；
b） 组织的数据安全运营团队或人员应针对高频发生的风险场景，定期开展风险评估或检查工作；
c） 组织应具备数据安全风险监测相关技术工具，支持对特权账号、数据异常行为、数据流向等的识别、监测、画像；
d） 组织应能够获取国家监管部门发布的风险警示信息。

7.4.3 三级要求

三级能力要求包括：

a） 满足 7.4.1 和 7.4.2 的全部要求；
b） **组织应建立风险知识库，定期整合历史的数据安全事件数据和处置经验；**
c） **组织应接入国家级、行业级威胁情报平台，持续提升威胁识别的准确性；**
d） 组织应参与、联合同业、合作伙伴，定期开展风险事件的联合演练。

7.5 事件处置

7.5.1 一级要求

一级能力要求包括：

a） 组织应制定数据安全事件处置的管理制度、规范手册，依据国家法律法规及行业规范要求，明确数据安全事件的类别、级别、处置流程、处置分工、处置时效、演练等要求，制定事件应急预案，并与运营工作流程进行映射、匹配；
b） 组织应具备网络流量监控、入侵检测与防御等技术工具。

7.5.2 二级要求

二级能力要求包括：

a） 满足 7.5.1 的全部要求；
b） **组织应部署数据安全事件应急响应相关技术工具，支持联动防火墙、终端监测与响应等安全设备，自动执行相关处置操作；**
c） 组织的数据安全运营团队或人员应定期开展数据安全事件应急演练，并将演练结果更新、维护至风险知识库；
d） 组织应及时将数据安全事件处置进度同步至组织相关部门；
e） 组织应依据国家法律法规及行业规范要求,对事件情况与处置进展报告至国家有关部门。

7.5.3 三级要求

三级能力要求包括：

a) 满足 7.5.1 和 7.5.2 的全部要求；
b) 组织应能够实现数据安全事件的智能化分析，基于历史事件数据，推荐事件处置方案；
c) 组织应实现主动开展事件自查与预防，同行业的组织发生数据安全事件时，及时开展内部安全自查。

8 运营优化要求

8.1 概述

运营优化要求是指通过构建组织的数据安全运营指标，对数据安全状态进行量化，使安全策略动态适配组织的数据安全运营和业务发展目标，实现数据安全运营的价值输出。

8.2 指标设计

8.2.1 一级要求

一级能力要求包括：

a) 组织应制定基本的安全性能指标，并与组织的运营工作流程进行映射、匹配；
b) 组织的数据安全运营团队或人员应能够监测安全设备运行情况，及时识别设备异常；
c) 组织的数据安全运营团队或人员应定期跟踪高危漏洞修复进度，通过运营工单系统进行进度管理；
d) 组织的数据安全运营团队或人员应根据工单处理时长，形成高耗时任务清单，持续优化运营流程；
e) 组织的数据安全运营团队或人员应制定工单与资源调度的优先级，建立工单分级响应机制；
f) 组织的数据安全运营团队或人员应定期组织运营会议，识别故障高发节点，提出设备升级、运营流程优化等相关建议。

8.2.2 二级要求

二级能力要求包括：

a) 满足 8.2.1 的全部要求；
b) **组织的数据安全运营团队或人员应将运营场景及指标与业务场景进行融合，构建“风险-业务”双维度指标，并明确指标阈值，指标显示异常时应启动专项排查；**
c) **组织的数据安全运营团队或人员应分析工单流转、处置的效率，持续优化协作流程；**
d) 组织应部署自动化的工单系统，支持自动识别工单类型，进行工单派发。

8.2.3 三级要求

三级能力要求包括：

a) 满足 8.2.1 和 8.2.2 的全部要求；
b) **组织的数据安全运营团队或人员应定期结合内外部环节变化，制定新增指标，废除不再适用的指标；**
c) **组织的数据安全运营团队或人员应定期对数据安全运营指标及其状态进行展示；**

d) 组织应构建全面的安全漏洞管理体系，实现漏洞的全生命周期管理；
e) 组织应依据国家法律法规及行业规范要求，定期或发生重大安全事件时，委托第三方机构对组织的漏洞管理体系进行全面审查和评估；
f) 组织应建立将数据安全指标与数据安全运营团队或人员绩效评价指标进行映射、关联。

8.3 策略优化

8.3.1 一级要求

一级能力要求包括：

a) 组织的数据安全运营团队或人员应制定数据安全运营策略，定期评估数据安全运营策略的匹配程度；
b) 组织的数据安全运营团队或人员应制定数据安全运营相关技术工具的配置基线手册，定期进行更新、维护。

8.3.2 二级要求

二级能力要求包括：

a) 满足 8.3.1 的全部要求；
b) **组织的数据安全运营团队或人员应制定数据安全运营策略和流程操作手册，结合运营指标结果，定期对手册内的流程、指标或阈值进行更新、维护；**
c) **组织的数据安全运营团队或人员应构建“技术-业务”双维度优化机制，定期收集安全设备运行信息和 IT、业务部门反馈的信息，对数据安全运营策略进行优化；**
d) 组织的数据安全运营团队或人员应部署策略自优化引擎，基于运营指标分析结果，自动部署、优化运营策略。

8.3.3 三级要求

三级能力要求包括：

a) 满足 8.3.1 和 8.3.2 的全部要求；
b) 组织应部署数据安全运营平台或其他技术工具，支持整合组织内部分散的安全设备或工具；
c) 组织应实现数据安全策略的动态自适应调整，能够根据最新的威胁、风险评估结果，自动调整安全策略。

8.4 业务赋能

8.4.1 一级要求

一级能力要求包括：

a) 组织应制定业务安全需求的对接流程，明确各业务部门与数据安全运营团队或人员的协作机制；
b) 组织的数据安全运营团队或人员应制定业务安全需求评估规范，明确业务需求中基础的安全要求。

8.4.2 二级要求

二级能力要求包括：

a) 满足 8.4.1 的全部要求；
b) **组织的数据安全运营团队或人员应参与业务项目的全流程，需求阶段及时识别数据安全风险点，开发和上线阶段开展代码扫描、渗透测试等安全检查与测试；**
c) 组织的数据安全运营团队或人员应提供数据安全内部咨询服务，定期汇总来自业务部门或人员的安全问题；
d) 组织的数据安全运营团队或人员应针对关键业务中的高发安全风险问题，提供专项培训或在相关业务系统、终端中嵌入风险提示；
e) 组织应部署自动化的风险监测平台，实时监控业务安全风险，检测到风险行为时，应能够通过弹窗等显著方式，向业务部门或人员提示风险，自动生成工单同步至数据安全运营工单系统。

8.4.3 三级要求

三级能力要求包括：

a) 满足 8.4.1 和 8.4.2 的全部要求；
b) **组织的数据安全运营团队或人员应对安全运营投入进行投入产出分析，量化数据安全运营投入对业务的影响，辅助组织的决策与规划工作；**
c) 组织的数据安全运营团队或人员应能够将工单、意见反馈、投诉、威胁情报等内外部数据、信息转化为安全赋能业务的行动方案或具体任务；
d) 组织的数据安全运营团队或人员应将安全战略与业务规划进行融合，制定安全赋能业务的行动方案或具体任务；
e) 组织应定期评估自身的数据安全运营能力，将自身数据安全运营实践经验进行总结，并在行业内进行最佳实践分享。

附 录 A
（资料性附录）
数据安全运营能力评估项

表 A.1 数据安全运营能力评估项目表

序号	评估项	评估要求类型	一级要求	二级要求	三级要求
6.2	运营场所	基础要求	6.2.1 a)~c）	6.2.2 a)	6.2.3 a) 6.2.3 b)
		高等级增强或增加要求	×	**6.2.2 b)** **6.2.2 c)**	**N/A**
6.3	管理体系	基础要求	6.3.1 a)、b)	6.3.2 a) 6.3.2 d)	6.3.3 a)
		高等级增强或增加要求	×	**6.3.2 b)** **6.3.2 c)**	**6.3.3 b)** **6.3.3 c)**
6.4	数据分类分级	基础要求	6.4.1 a)~e)	6.4.2 a) 6.4.2 c) 6.4.2 d)	6.4.3 a)
		高等级增强或增加要求	×	**6.4.2 b)**	**6.4.3 b)**
6.5	专业技能	基础要求	6.5.1 a)、b)	6.5.2 a) 6.5.2 c)~h）	6.5.3 a) 6.5.3 d)
		高等级增强或增加要求	×	**6.5.2 b)**	**6.5.3 b)** **6.5.3 c)**
7.2	技术防护	基础要求	7.2.1 a)~f）	7.2.2 a)	7.2.3 a)
		高等级增强或增加要求	×	**7.2.2 b)~f)**	**7.2.3 b)~f)**
7.3	合规评估	基础要求	7.3.1 a)、b)	7.3.2 a)~c）	7.3.3 a)~c）
		高等级增强或增加要求	×	**N/A**	**N/A**
7.4	风险管控	基础要求	7.4.1 a)~c）	7.4.2 a)~d）	7.4.3 a)、d）
		高等级增强或增加要求	×	**N/A**	**7.4.3 b)、c)**
7.5	事件处置	基础要求	7.5.1 a)、b)	7.5.2 a) 7.5.2 c)~e）	7.5.3 a)~c）
		高等级增强或增加要求	×	**7.5.2 b)**	**N/A**
8.2	指标设计	基础要求	8.2.1 a)~f)	8.2.2 a)、d）	8.2.3 a) 8.2.3 d)~f)
		高等级增强或增加要求	×	**8.2.2 b)、c)**	**8.2.3 b)、c)**
8.3	策略优化	基础要求	8.3.1 a)、b)	8.3.2 a)、d）	8.3.3 a)~c）
		高等级增强或增加要求	×	**8.3.2 b)、c)**	**N/A**
8.4	业务赋能	基础要求	8.4.1 a)、b)	8.4.2 a) 8.4.2 c)~e)	8.4.3 a) 8.4.3 c)~e）
		高等级增强或增加要求	×	**8.4.2 b)**	**8.4.3 b)**

参考文献

[1]GB/T 28458-2020 《信息安全技术 网络安全漏洞标识与描述规范》
[2]GB/T 37027-2018 《信息安全技术 网络攻击定义及描述规范》
[3]GB/T 40685-2021 《信息技术服务 数据资产 管理要求》
[4]GB/T 43697-2024 《数据安全技术 数据分类分级规则》
[5]GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》
[6]GB/T 45577-2025 《数据安全技术 数据安全风险评估方法》
[7]YD/T 4246-2023 《电信网和互联网数据异常行为监测技术要求与测试方法》