国家标准《信息安全技术 信息安全控制》（征求意见稿）编制说明

一、工作简况

1.1 任务来源

根据国家标准化管理委员会 202X 年下达的国家标准制修订计划,《信息安全技术 信息安全控制》由北京赛西科技发展有限责任公司负责承办，计划号：202XXXXX-T-469。本标准由全国信息安全标准化技术委员会归口管理。

1.2 修订背景

GB/T 22081—2016《信息技术 安全技术 信息安全控制实践指南》等同采用 ISO/IEC 27002:2013,国际标准 ISO/IEC 27002:2013 已经完成修订并正式发布，新版国际标准为 ISO/IEC 27002:2022《信息安全、网络空间安全和隐私保护 信息安全控制》。本次修订等同采用 ISO/IEC 27002:2022，紧跟国际标准变化，在考虑组织信息安全风险环境下提出信息安全控制的选择、实现和管理，为组织实现信息安全控制提供指导，并为信息安全管理提供最佳实践。

1.3 起草过程

北京赛西科技发展有限责任公司负责组织起草，中国合格评定国家认可中心、中电长城网际系统应用有限公司、中国网络安全审查技术与认证中心、北京时代新威信息技术有限公司、北京江南天安科技有限公司、山东省标准化研究院、四川大学、杭州安恒信息技术股份有限公司、黑龙江省网络空间研究中心等单位共同参与了本标准的起草工作。具体起草过程如下：

（1）标准草案阶段

1） 2022 年 3 月，标准牵头单位联合原标准起草单位，成立标准编制组，并确定任务分工及翻译注意事项。

2） 2022 年 6 月，标准牵头单位汇总形成标准草案初稿，标准编制组根据各自分工校对相关内容。

3） 2022 年 7-10 月，标准编制组多次组织标准草案研讨会，针对有争议的翻译进行讨论，不断修改完善标准草案。

4） 2022 年 10 月 30 日，信安标委印发《关于 2022 年网络安全国家标准

项目立项的通知》（信安字〔2022〕26 号），国家标准《信息安全技术 信息安全控制》修订项目正式立项。

5） 2022 年 11 月 14 日至 11 月 30 日，在信安标委网站和微信公众号面向社会公开征集标准参编单位。

6） 2022 年 12 月 2 日，标准牵头单位组织召开项目启动会，研讨确定标准编制思路、工作计划、任务分工等。

7） 2022 年 12 月 7 日，将标准草案提交信安标委 WG7 全体会议进行审议，充分听取工作组成员单位意见，根据会议决议，同意标准修改完善后形成征求意见稿。

（2）标准征求意见稿阶段

1） 2022 年 12 月 8 日至 2023 年 2 月，根据工作组成员单位意见修改，并多次组织编制组内部研讨，修改完善后形成当前的征求意见稿版本。

2） 2023 年 3 月 2 日，秘书处组织召开标准征求意见稿专家审查会，与会专家听取了编制组的汇报，经质询和讨论，建议编制组根据本次会议意见修改完善后，发起公开征求意见。

二、标准编制原则、主要内容及其确定依据

2.1 标准编制原则

本标准的研制工作遵循以下原则：

（1）目的原则

翻译过程中，要符合中文的语言表达习惯。翻译行为所要达到的目的决定整个翻译行为的过程，即结果决定方法。

（2）连贯性原则

要做到表述通畅，具有可读性和可接受性，使标准读者能够容易理解。

（3）忠实性原则

本标准与国际标准之间应该存在语际连贯一致，在充分理解国际标准原文的基础上进行翻译，做到准确表达原意。

2.2 主要内容及其确定依据

本标准等同采用 ISO/IEC 27002:2022《信息安全、网络空间安全和隐私保护 信息安全控制》，对 GB/T 22081—2016《信息技术 安全技术 信息安全控制

实践指南》进行修订。

本标准提供了一套通用信息安全控制参考集，包括实施指南。

本标准适用于：

a）组织基于 GB/T 22080 实施信息安全管理体系（ISMS）；

b）组织基于国际公认最佳实践实施信息安全控制；

c）组织开发其自身的信息安全管理指南。

本标准适用于所有类型和规模的组织。组织在实施基于 GB/T 22080 信息安全管理体系的信息安全风险处置时，本标准可作为其确定和实施所需控制措施的参考；本标准还可作为组织在确定和实施普遍接受的信息安全控制措施时的指导文件。此外，本标准旨在用于制定特定于行业和组织的信息安全管理指南，同时考虑其具体的信息安全风险环境。除本文件包含的控制措施外，可通过风险评估来确定特定于组织或环境所需要的控制措施。

2.3 修订前后技术内容的对比

修订的主要内容包括调整现有控制项的结构，将列举的安全控制项从 114 个减少至 93 个，并删除一些未能反映最佳实践的控制项。同时，新增 11 个控制项，包括威胁情报、云服务使用的信息安全以及数据防泄露等。

三、试验验证的分析、综述报告，技术经济论证，预期的经济效益、社会效益和生态效益

3.1 试验验证的分析、综述报告

在标准研制过程中，将选取典型行业领域与应用场景，对标准内容的可操作性和适用性进行验证，充分征求工作组、业界专家、技术支撑单位等相关方意见。

3.2 技术经济论证

暂无。

3.3 预期的经济效益、社会效益和生态效益

本标准旨在用于实施信息安全管理体系(ISMS)时选择控制项的参考，或作为组织实施普遍接受的信息安全控制项的指南。

修订后的标准框架简单，易于读者对信息安全控制进行分类；同时增加了控制的属性，可用来实现特定主题的划分和选择，针对性更强，以帮助组织加强信息安全控制的实施，支撑信息安全策略；并且修订后的标准指导的安全控制内容

更加详细和具体，使组织更容易实现安全控制的落地。

四、与国际、国外同类标准技术内容的对比情况，或者与测试的国外样品、样机的有关数据对比情况

本标准与国际标准技术内容保持一致，等同采用 ISO/IEC 27002:2022《信息安全、网络空间安全和隐私保护 信息安全控制》。

五、以国际标准为基础的起草情况，以及是否合规引用或者采用国际国外标准，并说明未采用国际标准的原因

本标准等同采用国际标准 ISO/IEC 27002:2022《信息安全、网络空间安全和隐私保护 信息安全控制》，做了下列最小限度的编辑性改动：

——将属性表、控制、目的、指南和其他信息列为二级条；

——调整了参考文献中的文件清单。

六、与有关法律、行政法规及相关标准的关系

本标准与《网络安全法》《密码法》《数据安全法》《个人信息保护法》等有关法律、行政法规以及 GB/T 22080《信息技术 安全技术 信息安全管理体系 要求》等相关标准协调一致。

七、重大分歧意见的处理经过和依据

本标准编制过程中未出现重大分歧。

八、涉及专利的有关说明

本标准不涉及专利。

九、实施国家标准的要求，以及组织措施、技术措施、过渡期和实施日期的建议等措施建议

建议本标准作为推荐性国家标准发布实施。标准发布后，将在标准起草单位内率先开展应用，并通过标准宣贯、标准应用指南等方式，推进标准落地应用。同时，从标准发布到标准实施，建议过渡期设置为 6 个月。

十、其他应当说明的事项

本标准代替 GB/T 22081—2016《信息技术 安全技术 信息安全控制实践指南》。

《信息安全技术 信息安全控制》标准编制组

2023 年 3 月