附件 2：ISO/IEC 27001:2022 与 GB/T 22080-2025 差异性分析报告

第一部分：按标准章节逐一比较

本部分以《ISO/IEC 27001:2022》整合 Amd 1:2024)的章节顺序为基准，与《GB/T 22080-2025》进行逐条比较。

条款号	ISO/IEC 27001:2022 标准内容	GB/T 22080-2025 标准内容	差异性比较结果
名称	信息安全 网络安全和隐私保护 信息安全管理体系 要求	网络安全技术 信息安全管理体系 要求	核心主题一致，但措辞和范围表述有差异
前言	描述国际标准的制修订程序、版本历史及版权声明。	包含与中国标准制定相关的信息，如与 2016 版的技术变化、起草单位等。明确指出纳入了 ISO/IEC 27001:2022/Amd 1:2024 的内容。	编辑性差异：内容因发布机构和受众不同而完全不同，但均不构成技术要求。
引言	阐述 ISMS 的概述、目的及与其他管理体系标准的兼容性。	内容与 ISO/IEC 27001:2022 引言的技术性内容一致。	完全一致
1	规定 ISMS 的建立、实施、维护和持续改进的要求。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
2	引用 ISO/IEC 27000 等国际标准。	引用中国国家标准（GB/T），如 GB/T 29246 (IDT ISO/IEC 27000)。	编辑性差异：引用标准编号不同，但技术内容通过等同采用（IDT）关系保持一致。
3	采用 ISO/IEC 27000 界定的术语和定义。	采用 ISO/IEC 27000 界定的术语和定义。	完全一致
4.1	明确要求“组织应确定气候变化是否是一个相关事项”。	条款内容与 ISO/IEC 27001:2022（含 Amd 1:2024） 完全相同。	完全一致
4.2	在注释中说明“相关方可能提出与气候变化相关的要求”。	条款及注释内容与 ISO/IEC 27001:2022（含 Amd 1:2024） 完	完全一致

条款号	ISO/IEC 27001:2022 标准内容	GB/T 22080—2025 标准内容	差异性比较结果
		全相同。	
4.3	规定确定范围的边界和适用性。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
4.4	要求组织建立、实施、维护和持续改进 ISMS。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
5.1	最高管理层应通过 a)—h)活动证实其领导与承诺。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
5.2	最高管理层应建立信息安全方针，该方针应满足 a)—d ）要求，并执行 e)—g ）活动。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
5.3	最高管理层应确保信息安全相关角色的责任和权限得到分配和沟通。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
6.1	规划时应考虑风险和机遇，并定义和应用风险评估与处置过程。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
6.2	组织应建立信息安全目标，并在规划时确定如何实现。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
6.3	当确定需要对 ISMS 进行变更时，应进行规划。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
7.1	组织应确定并提供所需资源。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
7.2	组织应确定、确保并保留人员能力的证据。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
7.3	人员应意识到信息安全方针、其贡献及不符合的后果。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
7.4	组织应确定内部和外部的沟通需求。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
7.5	组织应控制 ISMS 所需的文件化信息。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
8.1	组织应规划、实施和控制所需过	条款内容与 ISO/IEC 27001:2022	完全一致

条款号	ISO/IEC 27001:2022 标准内容	GB/T 22080-2025 标准内容	差异性比较结果
	程。	完全相同。	
8.2	组织应按计划执行信息安全风险评估。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
8.3	组织应实现信息安全风险处置计划。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
9.1	组织应监视、测量、分析和评价信息安全绩效和 ISMS 有效性。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
9.2	组织应按计划的时间间隔进行内部审核。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
9.3	最高管理层应按计划评审 ISMS。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
10.1	组织应持续改进 ISMS。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
10.2	发生不符合时，组织应采取措施并保留文件化信息。	条款内容与 ISO/IEC 27001:2022 完全相同。	完全一致
附录 A	包含 93 项控制措施，分为组织、人员、物理、技术 4 类。	控制项的数量、编号、标题、分类及具体内容与 ISO/IEC 27001:2022 完全相同。	完全一致

第二部分：主要差异说明

1. 《GB/T 22080-2025》的名称使用“网络安全技术”作为引导词，使其更好地融入中国的网络安全治理框架，术语更符合国内的使用习惯。两个名称都准确反映了标准的核心内容——为“信息安全管理体系”设定“要求”，并未改变标准本身的技术内容。
2. 技术内容的完全等同性:《ISO/IEC 27001:2022》(在整合 Amd 1:2024 后)与《GB/T 22080-2025》在所有技术性条款、要求及规范性附录上实现了完全一致。从第 4 章到第 10 章，以及附录 A 的所有内容，两者不存在任何技术性分歧。

3. 核心差异在于非技术层面：两者之间的主要差异仅限于前言内容和规范性引用文件的编号，这些是属于标准编辑、发布和本土化层面的差异，不影响标准的核心要求和使用。GB/T 22080-2025 在发布形式上提供了更优的整合性。
4. 结论：可以认定《ISO/IEC 27001:2022》（整合 Amd 1:2024 后）与《GB/T 22080-2025》在技术内容上完全等同。组织依据任何一个标准建立和实施信息安全管理体系，均能满足另一个标准的要求。差异仅存在于编辑性和标准的呈现方式上。