国际
标准

ISO/IEC 27018

信息安全、网络安全与隐私保护-作为个人身份信息（PII）处理者的公共云中个人可识别信息（PII）的指南

第三版
2025-08

参考编号
ISO/IEC 27018:2025（英文）

受版权保护的文件

ISO 版权局 CP 401 · Ch. de
Blandonnet 8 CH-1214 Vernier, Geneva 电
话：+41 22 749 01 11 电子邮件：
copyright@iso.org 网站：
www.iso.org

瑞士出版

内容

页

前言

ISO（国际标准化组织)和国际电工委员会（IEC)构成了全球标准化的专业体系。作为ISO或IEC成员的国家机构通过各自组织设立的技术委员会参与国际标准的制定,这些技术委员会负责处理特定领域的技术活动。

ISO 和 IEC 技术委员会在共同感兴趣的领域开展合作。其他政府和非政府国际组织也与 ISO 和 IEC 保持联络,参与相关工作。

ISO/IEC 指令第 1 部分描述了本文件的制定程序及其后续维护的程序。尤其应注意不同类型文件所需的不同批准标准。本文件是根据 ISO/IEC 的编辑规则起草的。

IEC 指令,第 2 部分（请参阅www.iso.org/directives或www.iec.ch/members_experts/refdocs)。

ISO 和 IEC 提醒注意,本文件的实施可能涉及使用一项或多项专利。ISO 和 IEC 对任何已主张的专利权的证据、有效性或适用性不持任何立场。截至本文件发布之日,ISO 和 IEC 尚未收到实施本文件可能需要的一项或多项专利的通知。然而,实施者需注意,这可能并非最新信息,最新信息可从www.iso.org/patents和https://patents.iec.ch的专利数据库获取。ISO和 IEC 不负责识别任何或所有此类专利权。

本文件中使用的任何商品名称仅为方便用户而提供的信息,并不构成认可。

有关标准的自愿性质、与合格评定相关的 ISO 特定术语和表达的含义,以及有关 ISO 在技术性贸易壁垒 (TBT) 中遵守世界贸易组织 (WTO) 原则的信息,请参阅www.iso.org/iso/foreword.html。

在 IEC 中,请参阅www.iec.ch/understanding-standards。

本文件由 ISO/IEC JTC 1信息技术联合技术委员会、 SC 27信息安全、网络安全和隐私保护分委员会编写。

第三版取消并取代了第二版（ISO/IEC 27018:2019）,并进行了技术修订。

主要变化如下：

文本已与 ISO/IEC 27002:2022 保持一致；

增加了附件B。

有关本文档的任何反馈或问题,请直接联系用户所在国家的标准机构。这些机构的完整列表请访问www.iso.org/members.html。以及www.iec.ch/national-committees。

介绍

0.1 背景和上下文

根据与客户签订的合同处理个人身份信息 (PII) 的云服务提供商应以允许双方满足涵盖 PII 保护的适用法律和法规要求的方式运营其服务。云服务提供商与其客户之间的要求以及要求划分方式因法律管辖区以及云服务提供商与客户之间的合同条款而异。管理如何处理（即收集、使用、传输和处置）PII 的法律有时被称为数据保护法律；PII 有时被称为个人数据或个人信息。PII 处理者的义务因管辖区而异，这使得提供云计算服务的企业在跨国环境中运营面临挑战。

当公共云服务提供商为云服务客户并根据其指示处理 PII 时，它就是“PII 处理者”。与公共云 PII 处理者有合同关系的云服务客户可以是自然人（即“PII 主体”，在云中处理他或她自己的 PII），也可以是组织（即“PII 控制者”，处理与许多 PII 主体相关的 PII）。云服务客户可以授权与其关联的一个或多个云服务用户使用根据其与公共云 PII 处理者签订的合同向客户提供的服务。云服务客户对数据的处理和使用拥有权限。作为 PII 控制者的云服务客户可能比公共云 PII 处理者承担更广泛的 PII 保护义务。

维持 PII 控制者和 PII 处理者之间的区别依赖于公共云 PII 处理者除了云服务客户针对其处理的 PII 设定的目标以及实现云服务客户目标所需的操作之外没有其他数据处理目标。

注1：当公共云PII处理者正在处理云服务客户账户数据时，它可以充当PII控制者。本文件不涵盖此类活动。

本文件旨在与 ISO/IEC 27002 中的信息安全目标和控制措施结合使用，创建一套通用的安全类别和控制措施，供作为 PII 处理者的公共云计算服务提供商实施。本文件的目标如下：

使公共云 PII 处理器在相关事项上保持透明，以便云服务客户可以选择管理良好的基于云的 PII 处理服务；

协助云服务客户和公共云 PII 处理者签订合同协议；

为云服务客户提供行使审计和合规权利和责任的机制，以防托管在多方虚拟化服务器（云）环境中的单个云服务客户数据在技术上无法审计，并且可能增加现有物理和逻辑网络安全控制的风险。

注2 预计公共云服务提供商在充当 PII 时应遵守适用的义务处理器。

本文档可以为公共云服务提供商（特别是那些在跨国市场运营的服务提供商）提供通用的合规框架。

0.2 公共云计算服务的 PII 保护控制

本文件旨在供各组织在基于 ISO/IEC 27001 实施云计算信息安全管理体系的过程中，作为选择 PII 保护控制措施的参考，或作为作为公共云 PII 处理者的组织实施普遍接受的 PII 保护控制措施的指导文件。具体而言，本文件以 ISO/IEC 27002 为基础，并考虑了 PII 保护要求所产生的特定风险环境，这些要求可能适用于作为 PII 处理者的公共云计算服务提供商。

就公共云服务提供商作为 PII 处理者的 PII 保护要求而言，该组织正在保护其客户委托的信息资产。公共云 PII 处理者实施 ISO/IEC 27002 的控制措施既适合此目的，也十分必要。

本文件扩展了 ISO/IEC 27002 控制措施，以适应风险的分布式特性以及云服务客户与公有云 PII 处理者之间存在的合同关系。本文件通过以下两个方面扩展了 ISO/IEC 27002：

适用于部分现有 ISO/IEC 27002 的公共云 PII 保护的实施指南
控件，以及

附件 A中的一组附加控制措施和相关指南旨在满足现有 ISO/IEC 27002 控制措施未涉及的公共云 PII 保护要求，并按照 ISO/IEC 29100 的隐私原则进行组织。

本文件中的大部分控制措施和指南也适用于 PII 控制者。然而，在大多数情况下，PII 控制者仍需承担本文未规定的其他义务。

0.3 PII保护要求

组织必须明确其对 PII 保护的要求。主要有以下三个方面的需求。

a) 法律和合同要求：法律和合同要求是组织机构及其贸易伙伴、承包商和服务提供商必须遵守的义务之一，以及与其社会文化和运营环境相关的责任。需要注意的是，PII 处理者所做出的法律、法规和合同承诺可能会要求选择特定的控制措施，也可能要求制定实施这些控制措施的具体标准。这些要求可能因司法管辖区而异。

b) 风险：另一个来源是评估与 PII 相关的组织风险，同时考虑组织的整体业务战略和目标。通过风险评估，可以识别风险，评估其后果和可能性，并评估风险。ISO/IEC 27005 提供了信息安全风险管理指南，包括风险评估、风险接受、风险沟通、风险监控和风险审查方面的建议。ISO/IEC 29134 提供了隐私影响评估指南。

c) 公司政策：虽然公司政策涵盖的许多方面都源于法律和社会文化要求，但组织也可以自愿选择超越源自 a) 要求的标准。

0.4 在云计算环境中选择和实施控制

可以从本文档中选择控制措施（该文档引用了 ISO/IEC 27002 中的控制措施，从而为相关行业定义的行业或应用创建组合参考控制措施集）。如有需要，还可以从其他控制措施集中选择控制措施，或根据需要设计新的控制措施以满足特定需求。

注：公共云 PII 处理者提供的 PII 处理服务可视为云计算的一种应用，而非一个独立的领域。然而，本文档使用“公共云服务提供商专用”一词，因为这是 ISO/IEC JTC 1/SC 27 制定的其他信息安全管理系统标准中使用的常规术语。

控制措施的选择取决于组织基于风险接受标准、风险处理方案以及适用于组织自身以及通过合同协议适用于其客户和供应商的一般风险管理方法而做出的决策。此外，控制措施的选择还须遵守相关的国家和国际法规。如果组织/公共云提供商未选择本文档中指定的控制措施，则应提供理由。

此外，控制措施的选择和实施取决于公共云提供商在整个云计算参考架构（参见 ISO/IEC 22123-3)中扮演的实际角色。许多不同的组织可能参与在云计算环境中提供基础设施和应用服务。在某些情况下，所选的控制措施可能针对特定服务类别。

云计算参考架构。在其他情况下，在实施安全控制方面可以有共享角色。合同协议应明确所有参与提供或使用云服务的组织的 PII 保护责任，包括公共云 PII 处理者、其分包商和云服务客户。

本文档中的控制可被视为指导原则，适用于大多数组织。
本文档对这些要求进行了更详细的解释，并提供了实施指南。如果在设计公共云 PII 处理者的信息系统、服务和运营时考虑到 PII 的保护要求，则可以简化实施。这种考虑是通常被称为“隐私设计”的概念的一个要素（参见参考文献[64]和[65]）。

0.5 制定附加指南

本文件可作为制定 PII 保护指南的起点。本实践准则中的控制措施和指南可能并非全部适用。此外，可能需要本文件中未包含的其他控制措施和指南。在制定包含其他指南或控制措施的文档时，在适用的情况下交叉引用本文件中的条款会很有帮助，以便审计师和业务合作伙伴进行合规性检查。

0.6 生命周期考虑

PII 具有自然的生命周期，从创建和发起，到存储、处理、使用和传输，再到最终的销毁或废弃。PII 的风险在其生命周期内可能有所不同，但 PII 的保护在各个阶段都至关重要。

在管理现有和新的信息系统的整个生命周期时，预计将考虑 PII 保护要求。

信息安全、网络安全和隐私保护
公共云中个人身份信息 (PII) 处理者的保护指南

1 范围

本文档建立了普遍接受的控制目标、控制措施和指南，以根据 ISO/IEC 29100 中针对公共云计算环境的隐私原则实施保护个人身份信息 (PII) 的措施。

具体而言，本文档指定了基于 ISO/IEC 27002:2022 的指南，同时考虑到 PII 保护的监管要求，该要求可适用于公共云服务提供商的信息安全风险环境。

本文件适用于所有类型和规模的组织，包括公共和私营公司、政府实体和非营利组织，这些组织作为 PII 处理器通过与其他组织签订合同通过云计算提供信息处理服务。

本文档中的指南也适用于充当 PII 控制者的组织。

2 规范性引用文件

文中引用下列文件，其部分或全部内容构成本文件的要求。凡是注日期的引用文件，仅其版本适用于本文件。凡是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。

ISO/IEC 27000，信息技术　安全技术　信息安全管理系统
概述和词汇

ISO/IEC 27002:2022，信息安全、网络安全和隐私保护　信息安全控制

ISO/IEC 22123-1，信息技术 - 云计算 - 第 1 部分：词汇

3 术语和定义

就本文件而言，ISO/IEC 22123-1、ISO/IEC 27000、ISO/IEC 27002 以及以下给出的术语和定义适用。

ISO 和 IEC 在以下地址维护用于标准化的术语数据库：

ISO 在线浏览平台：https: //www.iso.org/obp

IEC Electropedia：网址：https: //www.electropedia.org/

3.1
数据泄露
安全漏洞导致传输、存储或以其他方式处理的受保护数据遭到意外或非法破坏、丢失、更改、未经授权的披露或访问

[来源：ISO/IEC 27040:2024，3.5.2]

3.2

个人身份信息

个人身份信息

信息 a) 可用于建立信息与该信息所涉及的自然人之间的联系，或 b) 是或可以直接或间接地与自然人联系

注1：定义中的“自然人”是指PII主体(3.4)。为确定PII主体是否可识别，应考虑持有数据的隐私利益相关者或任何其他方可合理使用的所有手段，以建立PII集合与自然人之间的联系。

注2：本定义用于定义本文档中使用的术语“PII”。公共云PII处理器(3.5)通常无法明确知道其处理的信息是否属于任何指定类别，除非云服务客户明确说明。

[来源：ISO/IEC 29100:2024，3.7，已修改 - 已添加条目注释 2。]

3.3

PII 控制器

决定处理个人身份信息 (PII)的目的和方式的隐私利益相关者 (或隐私利益相关者) (3.2)，除将数据用于个人目的的自然人外

注 1：PII 控制者有时会指示其他人 [例如PII 处理者(3.5)]代表其处理 PII，但处理的责任仍由 PII 控制者承担。

[来源：ISO/IEC 29100:2024，3.8]

3.4

主要 PII

与个人身份信息 (PII) (3.2)相关的自然人

注 1：根据司法管辖区和特定的 PII 保护和隐私立法，同义词“数据主体”也可以用来代替术语“PII 主体”。

[来源：ISO/IEC 29100:2024，3.9，已修改 - 已添加条目注释 1。]

3.5

PII 处理器

代表PII 控制者(3.3)并按照其指示处理个人身份信息 (PII) (3.2)的隐私利益相关者

[来源：ISO/IEC 29100:2024，3.10]

3.6

PII 处理

PII 处理

对个人身份信息 (PII)执行的操作或一组操作(3.2)

注1：PII 处理操作的示例包括但不限于 PII 的收集、存储、更改、检索、查阅、披露、匿名化、假名化、传播或以其他方式提供、删除或销毁。

[来源：ISO/IEC 29100:2024，3.21，已修改 - “PII 处理”已添加为首选术语。]

3.7

公共云服务提供商

根据公共云模型提供云服务的一方

4 概述

4.1 本文件的结构

本文件遵循 ISO/IEC 27002:2022 中用于描述控制措施的结构。在这方面，本文件重复了早期版本（ISO/IEC 27018:2019）中采用的相同策略，即镜像 ISO/IEC 27002:2013,1 中的控制措施。

附件 B对本文档和上一版本（ISO/IEC 27018:2019）中的两种控制布局进行了比较。

具体而言，本文档在镜像 ISO/IEC 27002:2022 中的控制措施时使用了以下规则。如果某项控制措施的控制布局（如4.2 中所述）的各个要素相同，则仅提供对 ISO/IEC 27002:2022 中相应控制措施的引用。对于那些在公共云 PII 保护方面需要额外指导和相关信息的控制措施，分别在“公共云 PII 保护实施指南”和“公共云 PII 保护的其他信息”标题下提供了额外指导。此类指南也被称为“公共云服务提供商特定的实施指南”。除此之外，适用于云计算服务提供商 PII 保护的额外控制措施和相关实施指南在附件A 中描述。最后，本文档中的条款编号与 ISO/IEC 27002:2022 中的相应条款编号保持一致。

表 1中的控制措施分为四个主题，分别对应于第 5 条中列出的控制措施至8如下：

- 主题“提供针对公共云服务提供商的实施指南”对应于控制“公共云PII保护实施指南”；
- 主题“提供针对公共云服务提供商的特定实施指南和其他信息”对应于控制“公共云 PII 保护实施指南和其他用于公共云 PII 保护的信息”；
- 主题“未提供针对公共云服务提供商的额外实施指南或其他信息”对应于控制“没有针对公共云 PII 保护的具体指南或其他信息”；
- 主题“提供针对公共云服务提供商的实施指南，并交叉引用附件A 中的控制措施”对应于控制措施“公共云 PII 保护实施指南和交叉引用附件A 中的控制措施”。

表 1　ISO/IEC 27002:2022 中针对公共云服务提供商的具体指南和其他用于实施控制的信息的位置

ISO/IEC 27002:2022 控制标识符	ISO/IEC 27002:2022 控制名称	主题
第 5 条 – 组织控制		
5.1	信息安全政策	特定于公共云服务提供商 实施指导及其他 提供信息。c
5.2	信息安全角色和职责	特定于公共云服务提供商 提供了实施指导。b
5.3	职责分离	没有针对公共云服务提供商的额外实施指南 或提供其他信息。d
5.4	管理职责	没有针对公共云服务提供商的额外实施指南d 或提供其他信息。
5.5	与当局联系	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.6	与特殊利益团体的联系	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.7	威胁情报	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.8	项目管理中的信息安全	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.9	信息和其他相关资产的清单	没有针对公共云服务提供商的额外实施指南d 或提供其他信息。
5.10	信息和其他相关资产的可接受使用	没有针对公共云服务提供商的额外实施指南d 或提供其他信息。
5.11	资产返还	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.12	信息分类	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.13	信息标签	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d

ISO/IEC 27002:2022 中引入了新的控制措施。

b本控制措施可作为“公共云 PII 保护实施指南”适用。

c本控制措施适用为“公共云 PII 保护实施指南及公共云 PII 保护的其他信息”。

d此控制适用于“没有针对公共云 PII 保护的具体指导或其他信息”。

e此控制措施可作为“公共云 PII 保护实施指南和对附件A中控制措施的交叉引用”适用。

表 1 （续）

ISO/IEC 27002:2022 控制标识符	ISO/IEC 27002:2022 控制名称	主题
5.14	信息传递	特定于公共云服务提供商 提供了实施指导。 b
5.15	访问控制	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.16	身份管理	特定于公共云服务提供商 提供了实施指导。 b
5.17	身份验证信息	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.18	访问权限	没有针对公共云服务提供商的额外实施指南d 或提供其他信息。
5.19	供应商关系中的信息安全	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.20	解决供应商协议中的信息安全问题	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.21	管理ICT供应链中的信息安全	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.22	供应商服务的监控、审查和变更管理	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.23	使用云服务的信息安全	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.24	信息安全事件管理规划和准备	没有针对公共云服务提供商的额外实施指南d 或提供其他信息。
5.25	信息安全评估与决策 事件	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.26	信息安全事件响应	特定于公共云服务提供商 提供了实施指南，以及对附件A中控制措施的交叉引用。e
5.27	从信息安全事件中吸取教训	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.28	证据收集	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d

ISO/IEC 27002:2022 中引入了新的控制措施。

b本控制措施可作为“公共云 PII 保护实施指南”适用。

c本控制措施适用为“公共云 PII 保护实施指南及公共云 PII 保护的其他信息”。

d此控制适用于“没有针对公共云 PII 保护的具体指导或其他信息”。

e此控制措施可作为“公共云 PII 保护实施指南和对附件A中控制措施的交叉引用”适用。

表 1 （续）

ISO/IEC 27002:2022 控制标识符	ISO/IEC 27002:2022 控制名称	主题
5.29	中断期间的信息安全	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
上午5:30	ICT 为业务连续性做好了准备	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.31	法律、法规、监管和合同要求	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.32	知识产权	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.33	记录保护	没有针对公共云服务提供商的额外实施指南d 或提供其他信息。
5.34	隐私和 PII 保护	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.35	信息安全独立审查	特定于公共云服务提供商提供了实施指导。 b
5.36	遵守信息安全政策、规则和标准	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
5.37	记录的操作程序	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
第 6 条 – 人员控制		
6.1	筛查	没有针对公共云服务提供商的额外实施指南d 或提供其他信息。
6.2	雇佣条款和条件	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
6.3	信息安全意识、教育和培训	特定于公共云服务提供商实施指导及其他提供信息。c
6.4	纪律处分程序	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
6.5	终止或变更雇佣关系后的责任	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d

ISO/IEC 27002:2022 中引入了新的控制措施。

b本控制措施可作为“公共云 PII 保护实施指南”适用。

c本控制措施作为“公共云 PII 保护实施指南及公共云 PII 保护的其他信息”适用。

d此控制适用于“没有针对公共云 PII 保护的具体指导或其他信息”。

e此控制措施可作为“公共云 PII 保护实施指南和对附件A中控制措施的交叉引用”适用。

表 1 （续）

ISO/IEC 27002:2022 控制标识符	ISO/IEC 27002:2022 控制名称	主题
6.6	保密或不披露协议	特定于公共云服务提供商 提供了实施指南，以及对附件A中控制措施的交叉引用。e
6.7	远程工作	没有提供针对公共云服务提供商的额外实施指南或其他信息。d
6.8	信息安全事件报告	没有提供针对公共云服务提供商的额外实施指南或其他信息。d
第 7 条 – 物理控制		
7.1	物理安全边界	没有针对公共云服务提供商的额外实施指南d 或提供其他信息。
7.2	实体入口	没有提供针对公共云服务提供商的额外实施指南或其他信息。d
7.3	确保办公室、房间和设施的安全	没有提供针对公共云服务提供商的额外实施指南或其他信息。d
7.4	物理安全监控	没有提供针对公共云服务提供商的额外实施指南或其他信息。d
7.5	防范物理和环境威胁	没有提供针对公共云服务提供商的额外实施指南或其他信息。d
7.6	在安全区域工作	没有提供针对公共云服务提供商的额外实施指南或其他信息。d
7.7	清理桌面和屏幕	没有针对公共云服务提供商的额外实施指南d 或提供其他信息。
7.8	设备选址和保护	没有提供针对公共云服务提供商的额外实施指南或其他信息。d
7.9	场外资产安全	没有提供针对公共云服务提供商的额外实施指南或其他信息。d
7.10	存储介质	没有提供针对公共云服务提供商的额外实施指南或其他信息。d
7.11	支持实用程序	没有提供针对公共云服务提供商的额外实施指南或其他信息。d

ISO/IEC 27002:2022 中引入了新的控制措施。

b本控制措施可作为“公共云 PII 保护实施指南”适用。

c本控制措施作为“公共云 PII 保护实施指南及公共云 PII 保护的其他信息”适用。

d此控制适用于“没有针对公共云 PII 保护的具体指导或其他信息”。

e此控制措施可作为“公共云 PII 保护实施指南和对附件A中控制措施的交叉引用”适用。

表 1 （续）

ISO/IEC 27002:2022 控制标识符	ISO/IEC 27002:2022 控制名称	主题
7.12	布线安全	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
7.13	设备维护	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
7.14	安全处置或再利用设备	特定于公共云服务提供商提供了实施指南，以及对附件A中控制措施的交叉引用。e
第 8 条 – 技术控制		
8.1	用户端点设备	没有针对公共云服务提供商的额外实施指南d 或提供其他信息。
8.2	特权访问权限	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.3	信息访问限制	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.4	访问源代码	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.5	安全身份验证	特定于公共云服务提供商提供了实施指导。 b
8.6	容量管理	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.7	防范恶意软件	没有针对公共云服务提供商的额外实施指南d 或提供其他信息。
8.8	技术漏洞管理	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.9	配置管理	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.10	信息删除	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.11	数据屏蔽	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d

ISO/IEC 27002:2022 中引入了新的控制措施。

b本控制措施可作为“公共云 PII 保护实施指南”适用。

c本控制措施作为“公共云 PII 保护实施指南及公共云 PII 保护的其他信息”适用。

d此控制适用于“没有针对公共云 PII 保护的具体指导或其他信息”。

e此控制措施可作为“公共云 PII 保护实施指南和对附件A中控制措施的交叉引用”适用。

表 1 （续）

ISO/IEC 27002:2022 控制标识符	ISO/IEC 27002:2022 控制名称	主题
8.12	防止数据泄露	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.13	信息备份	特定于公共云服务提供商提供了实施指导。 b
8.14	信息处理设施的冗余	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.15	日志记录	特定于公共云服务提供商提供了实施指南，以及对附件A中控制措施的交叉引用。e
8.16	监控活动	没有针对公共云服务提供商的额外实施指南d 或提供其他信息。
8.17	时钟同步	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.18	使用特权实用程序	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.19	在操作系统上安装软件	没有提供针对特定公共云服务提供商的额外实施指南或其他信息。 d
8.20	网络安全	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.21	网络服务安全	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.22	网络隔离	没有针对公共云服务提供商的额外实施指南d 或提供其他信息。
8.23网页过滤		没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.24	密码学的使用	特定于公共云服务提供商提供了实施指导。 b
8.25	安全开发生命周期	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.26	应用程序安全要求	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d

ISO/IEC 27002:2022 中引入了新的控制措施。

b本控制措施可作为“公共云 PII 保护实施指南”适用。

c本控制措施作为“公共云 PII 保护实施指南及公共云 PII 保护的其他信息”适用。

d此控制适用于“没有针对公共云 PII 保护的具体指导或其他信息”。

e此控制措施可作为“公共云 PII 保护实施指南和对附件A中控制措施的交叉引用”适用。

表 1 （续）

ISO/IEC 27002:2022 控制标识符	ISO/IEC 27002:2022 控制名称	主题
8.27	安全系统架构与工程原理	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
上午8点28分	安全编码	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.29	开发和验收中的安全测试未提供针对特定公共云服务提供商的额外实施指南或其他信息。	d
8.30	外包开发	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.31	开发、测试和生产环境的分离	特定于公共云服务提供商 提供了实施指导。 b
8.32	变更管理	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.33	测试信息	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d
8.34	审计测试期间的信息系统保护	没有提供针对公共云服务提供商的额外实施指南或其他信息。 d

ISO/IEC 27002:2022 中引入了新的控制措施。

b本控制措施可作为“公共云 PII 保护实施指南”适用。

c本控制措施适用为“公共云 PII 保护实施指南及公共云 PII 保护的其他信息”。

d此控制适用于“没有针对公共云 PII 保护的具体指导或其他信息”。

e此控制措施可作为“公共云 PII 保护实施指南和对附件A中控制措施的交叉引用”适用。

4.2 控制布局

根据 ISO/IEC 27002:2022 标准，整套控制措施按上表 1中的 4 个主题进行分类。每个控制措施包含以下要素：

a) 控件标题：控件的简称；

b) 属性表：表格显示给定控件的每个属性的值；

c) 控制：控制是什么；

d) 目的：为什么要实施控制；

e) 指导：如何实施控制；

f) 其他信息：解释性文字或对其他相关文件的引用。

一些控制措施的指导文本会使用副标题，以便在指南篇幅较长且涉及多个主题时提高可读性。并非所有指导文本都会使用此类标题。

g) 公共云 PII 保护指南

这提供了更详细的信息,以支持控制措施的实施并实现控制目标。该指南并非在所有情况下都完全适用或充分,因此无法满足组织的特定控制要求。因此,替代或附加控制措施,或其他形式的风险处理（例如,规避、转移或接受风险)可能是合适的。

h) 公共云 PII 保护的其他信息

这提供了预计将被考虑的进一步信息,例如法律考虑和
参考其他标准。

5 组织控制

5.1 信息安全政策

ISO/IEC 27002:2022, 5.1 中的指南适用。此外,以下针对公共云服务提供商的指南及相关信息也适用。

a) 公共云 PII 保护实施指南

合同协议应根据所涉及的云服务类型（例如,云计算参考架构中的基础设施即服务 (IaaS)、平台即服务 (PaaS) 或软件即服务 (SaaS) 类别)在公共云 PII 处理者、其分包商和云服务客户之间分配责任。例如,应用层控制的责任分配可能有所不同,具体取决于公共云 PII 处理者提供的是 SaaS 服务,还是 PaaS 或 IaaS 服务（云服务客户可在其上构建或分层自己的应用程序）。

b) 公共云 PII 保护的其他信息

在某些司法管辖区,公共云 PII 处理者直接受 PII 保护法规的约束。在其他司法管辖区,PII 保护法规仅适用于 PII 控制者。

云服务客户与公共云 PII 处理者之间的合同必须包含一种机制,以确保公共云 PII 处理者支持并管理双方合同的合规性。合同可以要求进行独立合规性审计,并由云服务客户接受,例如通过实施本文档和 ISO/IEC 27002 中的相关控制措施。

5.2 信息安全角色和职责

ISO/IEC 27002:2022, 5.2 中的指南适用。此外,以下针对公共云服务提供商的指南也适用。

a) 公共云 PII 保护实施指南

公共云 PII 处理器应该有一名 PII 专家,为云服务客户提供有关如何正确处理 PII 信息的建议。

5.3 职责分离

ISO/IEC 27002:2022, 5.3 中的指导适用。

5.4 管理职责

ISO/IEC 27002:2022, 5.4 中的指导适用。

5.5 与当局联系

ISO/IEC 27002:2022, 5.5 中的指导适用。

5.6 与特殊利益集团的联系

ISO/IEC 27002:2022, 5.6 中的指导适用。

5.7 威胁情报

注:ISO/IEC 27002:2022 中引入了新的控制措施。

ISO/IEC 27002:2022, 5.7 中的指导适用。

5.8 项目管理中的信息安全

ISO/IEC 27002:2022, 5.8 中的指导适用。

5.9 信息及其他相关资产清单

ISO/IEC 27002:2022, 5.9 中的指导适用。

5.10 信息和其他相关资产的可接受使用

ISO/IEC 27002:2022, 5.10 中的指导适用。

5.11 资产返还

ISO/IEC 27002:2022, 5.11 中的指导适用。

5.12 信息分类

ISO/IEC 27002:2022, 5.12 中的指导适用。

5.13 信息标签

ISO/IEC 27002:2022, 5.13 中的指导适用。

5.14 信息传输

ISO/IEC 27002:2022, 5.14 中的指南适用。此外,以下针对公共云服务提供商的指南也适用。

a) 公共云 PII 保护实施指南

每当使用物理介质进行信息传输时,都应建立系统来记录包含 PII 的传入和传出物理介质,包括物理介质的类型、授权发送者/接收者、日期和时间以及物理介质的数量。在适当的情况下,云服务客户应实施额外措施（例如加密）,以降低在到达预定目的地之前发生未经授权访问的可能性,而公共云 PII 处理者也应支持应用这些措施的技术能力。在这种情况下,双方可以自行采取此类措施。

措施。

5.15 访问控制

ISO/IEC 27002:2022, 5.15 中的指导适用。

5.16 身份管理

ISO/IEC 27002:2022, 5.16 中的指南适用。此外，以下针对公共云服务提供商的指南及相关信息也适用。

a) 公共云 PII 保护实施指南

在云计算参考架构的服务类别背景下，云服务客户可以负责其控制下的云服务用户的部分或全部访问管理。在适当的情况下，公共云 PII 处理者应使云服务客户能够管理其控制下的云服务用户的访问。

用户注册和注销程序应解决用户访问控制受到损害的情况，例如密码或其他用户注册数据的损坏或泄露（例如由于无意泄露）。

注：各个司法管辖区可以对未使用身份验证凭证的检查频率提出具体要求。在这些司法管辖区运营的组织有责任确保遵守这些要求。

5.17 认证信息

ISO/IEC 27002:2022, 5.17 中的指导适用。

5.18 访问权限

ISO/IEC 27002:2022, 5.18 中的指导适用。

5.19 供应商关系中的信息安全

ISO/IEC 27002:2022, 5.19 中的指导适用。

5.20 解决供应商协议中的信息安全问题

ISO/IEC 27002:2022, 5.20 中的指导适用。

5.21 管理ICT供应链中的信息安全

ISO/IEC 27002:2022, 5.21 中的指导适用。

5.22 供应商服务的监控、审查和变更管理

ISO/IEC 27002:2022, 5.22 中的指导适用。

5.23 使用云服务的信息安全

注：ISO/IEC 27002:2022 中引入了新的控制措施。

ISO/IEC 27002:2022, 5.23 中的指导适用。

5.24 信息安全事件管理规划和准备

ISO/IEC 27002:2022, 5.24 中的指导适用。

5.25 信息安全事件评估与决策

ISO/IEC 27002:2022, 5.25 中的指导适用。

5.26 信息安全事件响应

ISO/IEC 27002:2022, 5.26 中的指导适用。

a) 公共云 PII 保护实施指南

信息安全事件应触发公共云 PII 处理器的审查,作为其信息安全事件管理流程的一部分,以确定是否发生了涉及 PII 的数据泄露（参见 A.10.1）。

并非所有信息安全事件都必然触发此类审查。信息安全事件可能不会导致对 PII 或任何公共云 PII 处理者存储 PII 的设备或设施的实际或重大未经授权的访问,并且可能包括但不限于对防火墙或边缘服务器的 ping 和其他诊断探测。

5.27 从信息安全事件中学习

ISO/IEC 27002:2022, 5.27 中的指导适用。

5.28 证据收集

ISO/IEC 27002:2022, 5.28 中的指导适用。

5.29 中断期间的信息安全

ISO/IEC 27002:2022, 5.29 中的指导适用。

5.30 ICT 业务连续性准备

注:ISO/IEC 27002:2022 中引入了新的控制措施。

ISO/IEC 27002:2022, 5.30 中的指导适用。

5.31 法律、法规、监管和合同要求

ISO/IEC 27002:2022, 5.31 中的指导适用。

5.32 知识产权

ISO/IEC 27002:2022, 5.32 中的指导适用。

5.33 记录保护

ISO/IEC 27002:2022, 5.33 中的指导适用。

5.34 隐私和 PII 保护

ISO/IEC 27002:2022, 5.34 中的指导适用。

5.35 信息安全独立审查

ISO/IEC 27002:2022, 5.35 中的指南适用。此外,以下针对公共云服务提供商的指南也适用。

a) 公共云 PII 保护实施指南

如果对单个云服务客户进行审计不切实际或可能增加安全风险,公共云 PII 处理者应在签订合同之前以及合同有效期内向潜在的云服务客户提供独立证据,证明信息安全已得到实施,并且

根据公共云 PII 处理者的政策和程序进行操作。在提供足够透明度的前提下，由公共云 PII 处理者选择的相关独立审计通常应是满足云服务客户审查公共云 PII 处理者处理操作利益的可接受方法。

5.36 遵守信息安全政策、规则和标准

ISO/IEC 27002:2022, 5.36 中的指导适用。

5.37 文件化的操作程序

ISO/IEC 27002:2022, 5.37 中的指导适用。

6人控制

6.1 筛选

ISO/IEC 27002:2022, 6.1 中的指导适用。

6.2 雇佣条款和条件

ISO/IEC 27002:2022, 6.2 中的指导适用。

6.3 信息安全意识、教育和培训

ISO/IEC 27002:2022, 6.3 中的指南适用。此外，以下针对公共云服务提供商的指南及相关信息也适用。

a) 公共云 PII 保护实施指南

应采取措施，让相关工作人员意识到违反隐私或安全规则和程序（尤其是那些涉及 PII 处理的规则和程序）可能对公共云 PII 处理者造成的后果（例如业务和品牌损失或声誉损害）、对工作人员造成的后果（例如纪律处分后果）以及对 PII 主体造成的后果（例如身体、物质和情感后果）。

b) 公共云 PII 保护的其他信息

在某些司法管辖区，公共云 PII 处理器可能受到法律制裁，包括直接来自当地 PII 保护机构的巨额罚款。

6.4 纪律处分程序

ISO/IEC 27002:2022, 6.4 中的指导适用。

6.5 终止或变更雇佣关系后的责任

ISO/IEC 27002:2022, 6.5 中的指导适用。

6.6 保密或不披露协议

注：与保密或不披露协议相关的附加控制和指导可在A.10.1中找到。

ISO/IEC 27002:2022, 6.6 中的指导适用。

6.7 远程工作

ISO/IEC 27002:2022, 6.7 中的指导适用。

6.8 信息安全事件报告

ISO/IEC 27002:2022, 6.8 中的指导适用。

7 物理控制

7.1 物理安全边界

ISO/IEC 27002:2022, 7.1 中的指导适用。

7.2 实体入口

ISO/IEC 27002:2022, 7.2 中的指导适用。

7.3 确保办公室、房间和设施的安全

ISO/IEC 27002:2022, 7.3 中的指导适用。

7.4 物理安全监控

注:ISO/IEC 27002:2022 中引入了新的控制措施。

ISO/IEC 27002:2022, 7.4 中的指导适用。

7.5 防范物理和环境威胁

ISO/IEC 27002:2022, 7.5 中的指导适用。

7.6 在安全区域工作

ISO/IEC 27002:2022, 7.6 中的指导适用。

7.7 清理桌面和屏幕

ISO/IEC 27002:2022, 7.7 中的指导适用。

7.8 设备选址和保护

ISO/IEC 27002:2022, 7.8 中的指导适用。

7.9 场外资产安全

ISO/IEC 27002:2022, 7.9 中的指导适用。

7.10 存储介质

ISO/IEC 27002:2022, 7.10 中的指导适用。

7.11 支持实用程序

ISO/IEC 27002:2022, 7.11 中的指导适用。

7.12 布线安全

ISO/IEC 27002:2022, 7.12 中的指导适用。

7.13 设备维护

ISO/IEC 27002:2022, 7.13 中的指导适用。

7.14 设备的安全处置或再利用

ISO/IEC 27002:2022 7.14 中的指南适用。以下针对特定公共云服务提供商的指南同样适用。

a) 公共云 PII 保护实施指南

为了安全处置或重新使用，包含可能包含 PII 的存储介质的设备应被视为包含 PII。

注：与设备安全处置或再利用相关的附加控制和指导可在A.11.7 中找到。

8 技术控制

8.1 用户端点设备

ISO/IEC 27002:2022, 8.1 中的指导适用。

8.2 特权访问权限

ISO/IEC 27002:2022, 8.2 中的指导适用。

8.3 信息访问限制

ISO/IEC 27002:2022, 8.3 中的指导适用。

8.4 访问源代码

ISO/IEC 27002:2022, 8.4 中的指导适用。

8.5 安全认证

ISO/IEC 27002:2022, 8.5 中的指南适用。以下针对公共云服务提供商的指南同样适用。

a) 公共云 PII 保护实施指南

如有需要，公共云 PII 处理器应为云服务客户为其控制下的云服务用户请求的任何帐户提供安全登录程序。

8.6 容量管理

ISO/IEC 27002:2022, 8.6 中的指导适用。

8.7 防范恶意软件

ISO/IEC 27002:2022, 8.7 中的指导适用。

8.8 技术漏洞管理

ISO/IEC 27002:2022, 8.8 中的指导适用。

8.9 配置管理

注:ISO/IEC 27002:2022 中引入了新的控制措施。

ISO/IEC 27002:2022, 8.9 中的指导适用。

8.10 信息删除

注:ISO/IEC 27002:2022 中引入了新的控制措施。

ISO/IEC 27002:2022, 8.10 中的指导适用。

8.11 数据屏蔽

注:ISO/IEC 27002:2022 中引入了新的控制措施。

ISO/IEC 27002:2022, 8.11 中的指导适用。

8.12 数据泄露防护

注:ISO/IEC 27002:2022 中引入了新的控制措施。

ISO/IEC 27002:2022, 8.12 中的指导适用。

8.13 信息备份

ISO/IEC 27002:2022, 8.13 中的指南适用。以下针对公共云服务提供商的指南同样适用。

a) 公共云 PII 保护实施指南

基于云计算模型的信息处理系统引入了异地备份的额外或替代机制,以防止数据丢失,确保数据处理操作的连续性,并提供在中断事件后恢复数据处理操作的能力。为了备份或恢复,或两者兼而有之,应在物理或逻辑上不同的位置（可以是信息处理系统本身）创建或维护多个数据副本。

在这方面,PII 的具体责任可能由云服务客户承担。如果公共云 PII 处理者明确向云服务客户提供备份和恢复服务,则公共云 PII 处理者应向云服务客户提供有关云服务在备份和恢复云服务客户数据方面的能力的信息。

应制定程序,以便在中断事件发生后指定的、记录的时间内恢复数据处理操作。

应按照指定的、记录的频率审查备份和恢复程序。

注:某些司法管辖区可能对备份和恢复程序的审查频率提出具体要求。在这些司法管辖区运营的组织有责任确保遵守这些要求。

使用分包商存储正在处理的数据的复制或备份副本,受本文件中适用于分包 PII 处理的控制措施A.8.1和A.11.12的约束。如果发生物理介质传输,则也受本文件中控制措施5.14和A.11.5的约束。

公共云 PII 处理器应制定一项政策,以满足信息备份的要求以及为备份目的而持有的信息中包含的 PII 的擦除的任何进一步要求（例如合同要求）。

8.14 信息处理设施的冗余

ISO/IEC 27002:2022, 8.14 中的指导适用。

8.15 日志记录

ISO/IEC 27002:2022, 8.15 中的指南适用。以下针对特定公共云服务提供商的指南同样适用。

a) 公共云 PII 保护实施指南

应建立一个流程，以指定的、记录的周期审查事件日志，以识别异常情况并提出补救措施。

事件日志应尽可能记录 PII 是否因事件而发生变化（例如，添加、修改或删除），以及由谁更改。如果涉及多个服务提供商提供云计算参考架构中不同服务类别的服务，则在实施本指南时，可以有多种角色或共享角色。

公共云 PII 处理者应定义是否、何时以及如何向云服务客户提供或使用日志信息的标准。这些程序应向云服务客户提供。

当云服务客户被允许访问公共云 PII 处理者控制的日志记录时，公共云 PII 处理者应确保云服务客户只能访问与该云服务客户活动相关的记录，而不能访问与其他云服务客户活动相关的任何日志记录。

为安全监控和操作诊断等目的而记录的日志信息可能包含 PII。应采取访问控制等措施，确保记录的信息仅用于其预期用途。

应制定一个程序（最好是自动的），以确保在指定和记录的期限内删除记录的信息。

8.16 监测活动

注：ISO/IEC 27002:2022 中引入了新的控制措施。

ISO/IEC 27002:2022, 8.16 中的指导适用。

8.17 时钟同步

ISO/IEC 27002:2022, 8.17 中的指导适用。

8.18 特权实用程序的使用

ISO/IEC 27002:2022, 8.18 中的指导适用。

8.19 在操作系统上安装软件

ISO/IEC 27002:2022, 8.19 中的指导适用。

8.20 网络安全

ISO/IEC 27002:2022, 8.20 中的指导适用。

8.21 网络服务安全

ISO/IEC 27002:2022, 8.21 中的指导适用。

8.22 网络隔离

ISO/IEC 27002:2022, 8.22 中的指导适用。

8.23 网页过滤

注:ISO/IEC 27002:2022 中引入了新的控制措施。

ISO/IEC 27002:2022, 8.23 中的指导适用。

8.24 密码学的使用

ISO/IEC 27002:2022, 8.24 中的指南适用。以下针对特定公共云服务提供商的指南同样适用。

a) 公共云 PII 保护实施指南

公共云 PII 处理器还应向云服务客户提供有关其提供的任何功能的信息,这些功能可以帮助云服务客户应用和管理自己的加密保护和流程,例如管理保险库中的密钥或秘密的各种方法、密钥管理系统 (KMS)、硬件安全模块 (HSM) 支持的服务、云 HSM 等。

注意:在某些司法管辖区,可能需要应用加密技术来保护特定类型的 PII,例如有关 PII 主体的健康数据、居民登记号码、护照号码和驾驶执照号码。

8.25 安全开发生命周期

ISO/IEC 27002:2022, 8.25 中的指导适用。

8.26 应用安全要求

ISO/IEC 27002:2022, 8.26 中的指导适用。

8.27 安全系统架构和工程原理

ISO/IEC 27002:2022, 8.27 中的指导适用。

8.28 安全编码

注:ISO/IEC 27002:2022 中引入了新的控制措施。

ISO/IEC 27002:2022, 8.28 中的指导适用。

8.29 开发和验收中的安全测试

ISO/IEC 27002:2022, 8.29 中的指导适用。

8.30 外包开发

ISO/IEC 27002:2022, 8.30 中的指导适用。

8.31 开发、测试和生产环境的分离

ISO/IEC 27002:2022, 8.31 中的指南适用。以下针对特定公共云服务提供商的指南同样适用。

a) 公共云 PII 保护实施指南

如果无法避免使用 PII 进行测试目的,则应进行风险评估。
应实施技术和组织措施,以尽量减少已发现的风险。

8.32 变更管理

ISO/IEC 27002:2022, 8.32 中的指导适用。

8.33 测试信息

ISO/IEC 27002:2022, 8.33 中的指导适用。

8.34 审计测试期间的信息系统保护

ISO/IEC 27002:2022, 8.34 中的指导适用。

附件A
（信息性）

公共云 PII 处理器扩展控制集,用于 PII 保护

A.1 总则

本附件规定了新的控制措施和相关实施指南,这些控制措施和指南与 ISO/IEC 27002（见第 5至8 条)中的控制措施和指南相结合,构成了扩展的控制集,以满足适用于作为 PII 处理者的公共云服务提供商的 PII 保护要求。

这些附加控制措施根据 ISO/IEC 29100 的 11 项隐私原则进行分类。在许多情况下,这些控制措施可以根据多项隐私原则进行分类。在这种情况下,它们将根据最相关的原则进行分类。

A.2 同意和选择

A.2.1 有关 PII 主体权利的合作义务

a) 控制

公共云 PII 处理器应为云服务客户提供手段,以促进 PII 主体行使访问、更正和删除与其相关的 PII 的权利,从而使云服务客户能够履行其义务。

b) 公共云 PII 保护实施指南

PII 控制者在这方面的义务可以通过法律、法规或合同来定义。这些义务可以包括云服务客户使用公共云 PII 处理者服务进行实施的事项。例如,这可以包括及时更正或删除 PII。

PII控制者依赖公共云PII处理者提供信息或技术措施以便利PII主体权利行使的,应当在合同中约定相关信息或技术措施。

A.3 目的合法性和规范

A.3.1 公共云 PII 处理器的目的

a) 控制

根据合同处理的 PII 不应为了任何独立于云服务客户指示的目的而进行处理。

b) 公共云 PII 保护实施指南

公共云 PII 处理器和云服务客户之间的合同中可以包含指令,例如服务要实现的目标和时间框架。

为了实现云服务客户的目的,出于技术原因,公共云 PII 处理者可以自行决定 PII 处理方法,该处理方法应符合云服务客户的一般指示,而无需云服务客户的明确指示。例如,为了有效利用网络或处理能力,可能需要分配特定的

根据 PII 主体的某些特征,处理资源。在公共云 PII 处理者确定处理方法涉及 PII 收集和使用的情况下,公共云 PII 处理者应遵守 ISO/IEC 29100 中规定的相关隐私原则和“隐私设计”原则（参见参考文献[64]和[65]）。

公共云 PII 处理者应及时向云服务客户提供所有相关信息,以便云服务客户确保公共云 PII 处理者遵守目的规范和限制原则,并确保公共云不会处理任何 PII

PII 处理器或其任何分包商,用于独立于云指令的其他目的
服务客戶。

A.3.2 公有云PII处理者的商业用途

a) 控制

未经明确同意,公共云 PII 处理者不得将根据合同处理的 PII 用于营销和广告目的。此类同意不应成为接受服务的条件。

注:此控制是对A.3.1中更通用的控制的补充,并不替代或取代它。

A.4 收集限制

没有任何额外的控制与此隐私原则相关。

A.5 数据最小化

A.5.1 安全删除临时文件

a) 控制

临时文件和文档应在规定的、记录的期限内删除或销毁。

b) 公共云 PII 保护实施指南

A.10.3中提供了有关 PII 擦除的实施指导。

信息系统在正常运行过程中可能会创建临时文件。此类文件特定于系统或应用程序,但可能包括文件系统回滚日志以及与数据库更新和其他应用软件运行相关的临时文件。相关信息处理任务完成后,将不再需要临时文件,除非特殊情况要求不删除,否则应在完成后将其删除。这些文件持续使用的时间并非总是确定的,但“垃圾收集”程序应识别相关文件并确定自上次使用以来的时间。

PII 处理信息系统应定期检查,确保超过指定期限的未使用的临时文件被删除。

A.6 使用、保留和披露限制

A.6.1 PII 披露通知

a) 控制

预计公共云 PII 处理器与云服务客户之间的合同要求公共云 PII 处理器根据任何程序通知云服务客户,并且

合同中约定的时间段，任何具有法律约束力的执法机构要求披露 PII 的请求，除非此类披露被禁止。

b) 公共云 PII 保护实施指南

公共云 PII 处理器应提供合同保证，以确保：

拒绝任何不具有法律约束力的 PII 披露请求；

在法律允许的情况下，在进行任何 PII 之前咨询相应的云服务客户
披露；以及

接受相应云服务客户授权的任何合同约定的 PII 披露请求。

示例：可能的披露禁令是刑法禁止维护执法调查的机密性。

A.6.2 PII 披露记录

a) 控制

应记录向第三方披露 PII 的情况，包括披露了哪些 PII、披露 PII 的原因、向谁披露以及何时披露。

b) 公共云 PII 保护实施指南

PII 可以在正常运营过程中披露。这些披露应予以记录。任何向第三方的额外披露，例如因合法调查或外部审计而产生的披露，也应予以记录。记录应包括披露来源、披露原因以及披露授权来源。

A.7 准确性和质量

没有任何额外的控制与此隐私原则相关。

A.8 公开、透明和通知

A.8.1 分包 PII 处理的披露

a) 控制

如果公共云 PII 处理器打算使用分包商来处理 PII，则应向
提前联系相关云服务客户。

b) 公共云 PII 保护实施指南

公共云 PII 处理者与云服务客户之间的合同中，应明确规定使用分包商处理 PII 的条款。合同应明确规定，只有在获得云服务客户同意的情况下才能委托分包商，而云服务客户通常可以在服务开始时给予同意。公共云 PII 处理者应及时告知云服务客户任何此类变更，以便云服务客户能够反对此类变更或终止合同。

披露的信息应涵盖使用分包的事实以及相关分包商的名称，但不包含任何具体业务细节。披露的信息还应包括分包商可以在哪些国家/地区处理数据（参见A.12.1），以及分包商有义务满足或超过公共云 PII 处理者的义务的方式（参见A.11.12）。

如果评估认为公开披露分包商信息会导致安全风险增加,则应根据保密协议和/或云服务客户的要求进行披露。云服务客户应知晓该信息可供获取。

A.9 个人参与和访问

没有任何额外的控制与此隐私原则相关。

A.10问责制

A.10.1 涉及 PII 的数据泄露通知

a) 控制

公共云PII处理者在发生任何未经授权访问PII或未经授权访问处理设备或设施,导致PII丢失、泄露或变更时,应当及时通知相关云服务客户。

b) 公共云 PII 保护实施指南

涉及 PII 的数据泄露通知条款应构成公共云 PII 处理者与云服务客户之间合同的一部分。合同应明确公共云 PII 处理者将如何提供云服务客户履行其通知相关部门义务所需的信息。此通知义务不适用于由云服务客户或 PII 主体造成的数据泄露,或由其负责的系统组件造成的数据泄露。

合同还应规定涉及 PII 的数据泄露通知的最大延迟时间。

如果发生涉及 PII 的数据泄露,则应保留记录,其中包含事件描述、时间段、事件后果、报告人姓名、事件报告对象、解决事件所采取的步骤（包括负责人和恢复的数据)以及事件导致 PII 丢失、泄露或更改的事实。

如果发生涉及 PII 的数据泄露,记录还应包含已知泄露数据的描述。如果已发出通知,记录应包含通知云服务客户或监管机构（或两者兼而有之)的步骤。

在某些司法管辖区,相关法律或法规可以要求公共云 PII 处理者直接通知适当的监管机构（例如 PII 保护机构)涉及 PII 的数据泄露。

注意:可能存在其他需要通知但本文未涵盖的违规行为,例如未经同意或其他授权的收集、用于未经授权的目的等。

A.10.2 管理安全政策和指南的保留期限

a) 控制

已更新的安全政策和操作程序的现有副本应保留一段指定的、有记录的替换期。

b) 公共云 PII 保护实施指南

可能需要审查当前和历史政策及程序,例如在客户争议解决和个人身份信息保护机构调查的情况下。在没有具体合同要求或其他适用要求的情况下,建议最低保留期限为五年。

A.10.3 PII 的返回、转移和处置

a) 控制

公共云 PII 处理器应该制定有关这些活动的政策，并应将该政策提供给云服务客户。

b) 公共云 PII 保护实施指南

在某个时间点，PII 预计会以某种方式被处置。这可能包括将 PII 返还给云服务客户、将其转移至另一个公有云 PII 处理者或 PII 控制者（例如，由于合并）、安全删除或以其他方式销毁、匿名化或归档。

公共云 PII 处理者应提供必要信息，以便云服务客户确保根据合同处理的 PII 在其存储位置（包括出于备份和业务连续性目的）不再需要用于云服务客户的特定目的时，立即被（由公共云 PII 处理者及其任何分包商）从其存储位置删除。处置机制的性质（解除链接、覆盖、消磁、销毁或其他形式的擦除）和/或适用的商业标准应在合同中规定。

公共云 PII 处理者应制定并实施有关 PII 处置的政策，并应将该政策提供给云服务客户。

该政策应涵盖合同终止后 PII 销毁之前的保留期限，以保护云服务客户不会因合同意外失效而丢失 PII。

注：本控制和指南也与“使用、保留和披露限制”原则的保留要素相关（见A.6）。

A.11信息安全

A.11.1 保密或不披露协议

a) 控制

公共云 PII 处理器控制下且有权访问 PII 的个人应承担保密义务。

b) 公共云 PII 保护实施指南

公共云 PII 处理者与其员工和代理人之间签订的保密协议，无论形式如何，都应确保员工和代理人不得出于云服务客户指示以外的目的披露 PII（参见A.3.1）。保密协议的义务在任何相关合同终止后仍然有效。

A.11.2 限制制作硬拷贝材料

a) 控制

应限制创建显示 PII 的硬拷贝材料。

b) 公共云 PII 保护实施指南

硬拷贝材料包括通过印刷创建的材料。

A.11.3 数据恢复的控制和记录

a) 控制

应该有一个数据恢复工作的程序和日志。

b) 公共云 PII 保护实施指南

数据恢复工作的日志应包含：负责人、恢复的数据描述以及手动恢复的数据。

A.11.4 保护离开场所的存储介质上的数据

a) 控制

离开组织场所的媒体上的 PII 应经过授权程序，并且除授权人员外，任何人都不能访问（例如，通过加密相关数据）。

A.11.5 使用未加密的便携式存储介质和设备

a) 控制

除非不可避免的情况，否则不应使用不允许加密的便携式物理媒体和便携式设备，并且应记录任何此类便携式媒体和设备的使用情况。

A.11.6 通过公共数据传输网络传输的 PII 的加密

a) 控制

通过公共数据传输网络传输的 PII 应在传输前进行加密。

b) 公共云 PII 保护实施指南

在某些情况下，例如电子邮件交换，公共数据传输网络系统的固有特性可能要求暴露一些标头或流量数据以实现有效传输。

当有多个服务提供商参与提供云计算参考架构的不同服务类别的服务时，在实施本指南时可以有多种或共享的角色。

A.11.7 安全处置硬拷贝材料

a) 控制

销毁硬拷贝材料时，应采用交叉切割、粉碎、焚烧、制浆等方式安全销毁。

A.11.8 用户 ID 的唯一用途

a) 控制

如果多个个人有权访问存储的 PII，那么他们每个人都应该有一个不同的用户 ID，以便进行识别、身份验证和授权。

A.11.9 用户ID管理

a) 控制

已停用或过期的用户 ID 不应授予其他个人。

b) 公共云 PII 保护实施指南

在整个云计算参考架构的背景下，云服务客户可以负责其控制下的云服务用户的部分或全部用户身份管理工作。

A.11.10 授权用户的记录

a) 控制

已授权访问信息系统的用户或用户资料的最新记录
应予以维持。

b) 公共云 PII 保护实施指南

应为所有获得公共云 PII 处理器授权访问的用户维护用户配置文件。
用户的个人资料包含有关该用户的一组数据，包括用户 ID，这些数据对于实施提供对信息系统的授权访问的技术控制是必需的。

A.11.11 合同措施

a) 控制

云服务客户与公共云 PII 处理者之间的合同应明确最低限度的技术和组织措施，以确保合同规定的安全措施到位，并确保数据不会出于任何独立于控制者指示的目的进行处理。公共云 PII 处理者不应单方面削减此类措施。

b) 公共云 PII 保护实施指南

与公共云 PII 处理者相关的信息安全和 PII 保护义务可直接源于适用法律。若非适用法律，则与公共云 PII 处理者相关的 PII 保护义务应在合同中约定。

本文件中的控制措施以及 ISO/IEC 27002 中的控制措施旨在作为协助签订 PII 信息处理合同的参考措施目录。公共云 PII 处理者应在签订合同之前告知潜在的云服务客户为保护 PII 而实施的信息安全和隐私控制措施。

公共云 PII 处理者在签订合同的过程中应对其能力保持透明。然而，确保公共云 PII 处理者实施的措施符合其义务最终是云服务客户的责任。

A.11.12 分包 PII 处理

a) 控制

公共云 PII 处理者与任何处理 PII 的分包商之间的合同应明确规定满足公共云 PII 处理者信息安全和 PII 保护义务的最低技术和组织措施。此类措施不应受到分包商单方面削减。

b) 公共云 PII 保护实施指南

本控制涵盖使用分包商存储备份副本的情况（参见A.8.1）。

A.11.13 访问预先使用的数据存储空间上的数据

a) 控制

公共云 PII 处理器应确保每当将数据存储空间分配给云服务客户时，该存储空间上先前驻留的任何数据对于该云服务客户都是不可见的。

b) 公共云 PII 保护实施指南

当云服务用户删除信息系统中的数据时，由于性能问题，直接擦除这些数据可能不切实际。这会导致其他用户读取数据的风险。应采取特定的技术措施来避免此类风险。

在实施此控制时，没有特别适合处理所有情况的具体指导。
然而，举例来说，如果云服务用户尝试读取尚未被该用户自己的数据覆盖的存储空间，某些云基础设施、平台或应用程序将返回零或随机数。

A.12隐私合规性

A.12.1 PII 的地理位置

a) 控制

公共云 PII 处理器应指定并记录可能存储 PII 的国家/地区。

b) 公共云 PII 保护实施指南

可能存储 PII 的国家/地区的身份信息应向云服务客户提供。使用分包 PII 处理所产生的国家/地区的身份信息也应包含在内。如果国际数据传输适用特定合同协议，例如示范合同条款、具有约束力的公司规则或跨境隐私规则，则还应明确该协议以及适用此类协议的国家/地区或情况。公共云 PII 处理者应及时将任何此类变更告知云服务客户，以便云服务客户能够反对此类变更或终止合同。

A.12.2 PII 的预期目的地

a) 控制

使用数据传输网络传输的 PII 应受到适当的控制，以确保数据到达预定目的地。

附件B
（信息性）

本文档与第一版的对应关系

ISO/IEC 27018:2019

本附件的目的是为当前使用本文件第一版（ISO/IEC 27018:2019)并希望过渡到此版本的组织提供与该版本（ISO/IEC 27018:2019）的向后兼容性。

表 B.1提供了第 5至8条中规定的控制与 ISO/IEC 27018:2019 中的控制的对应关系。

表 B.1　本文档中的控制措施与 ISO/IEC 27018:2019 中的控制措施之间的对应关系

ISO/IEC 27018:2025 控制标识符	ISO/IEC 27018:2019 控制标识符	控件名称
5.1	05.1.1, 05.1.2	信息安全政策
5.2	06.1.1	信息安全角色和职责
5.3	06.1.2	职责分离
5.4	07.2.1	管理职责
5.5	06.1.3	与当局联系
5.6	06.1.4	与特殊利益团体的联系
5.7	新的	威胁情报
5.8	06.1.5, 14.1.1	项目管理中的信息安全
5.9	08.1.1, 08.1.2	信息和其他相关资产的清单
5.10	08.1.3, 08.2.3	信息和其他相关资产的可接受使用
5.11	08.1.4	资产返还
5.12	08.2.1	信息分类
5.13	08.2.2	信息标签
5.14	13.2.1、13.2.2、13.2.3	信息传递
5.15	09.1.1、09.1.2	访问控制
5.16	09.2.1	身份管理
5.17	09.2.4, 09.3.1, 09.4.3	身份验证信息
5.18	09.2.2, 09.2.5, 09.2.6	访问权限
5.19	15.1.1	供应商关系中的信息安全
5.20	15.1.2	解决供应商协议中的信息安全问题
5.21	15.1.3	管理ICT供应链中的信息安全
5.22	15.2.1, 15.2.2	供应商服务的监控、审查和变更管理
5.23	新的	使用云服务的信息安全
5.24	16.1.1	信息安全事件管理规划和准备
5.25	16.1.4	信息安全事件评估与决策
5.26	16.1.5	信息安全事件响应

表 B.1 （续）

ISO/IEC 27018:2025 控制标识符	ISO/IEC 27018:2019 控制标识符	控件名称
5.27	16.1.6	从信息安全事件中吸取教训
5.28	16.1.7	证据收集
5.29	17.1.1、17.1.2、17.1.3 中断期间的信息安全	
5.30	新的	ICT 为业务连续性做好了准备
5.31	18.1.1, 18.1.5	法律、法规、监管和合同要求
5.32	18.1.2	知识产权
5.33	18.1.3	记录保护
5.34	18.1.4	隐私和 PII 保护
5.35	18.2.1	信息安全独立审查
5.36	18.2.2, 18.2.3	遵守信息安全政策、规则和标准
5.37	12.1.1	记录的操作程序
6.1	07.1.1	筛查
6.2	07.1.2	雇佣条款和条件
6.3	07.2.2	信息安全意识、教育和培训
6.4	07.2.3	纪律处分程序
6.5	07.3.1	终止或变更雇佣关系后的责任
6.6	13.2.4	保密或不披露协议
6.7	06.2.2	远程工作
6.8	16.1.2, 16.1.3	信息安全事件报告
7.1	11.1.1	物理安全边界
7.2	11.1.2, 11.1.6	实体入口
7.3	11.1.3	确保办公室、房间和设施的安全
7.4	新的	物理安全监控
7.5	11.1.4	防范物理和环境威胁
7.6	11.1.5	在安全区域工作
7.7	11.2.9	清理桌面和屏幕
7.8	11.2.1	设备选址和保护
7.9	11.2.6	场外资产安全
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	存储介质
7.11	11.2.2	支持实用程序
7.12	11.2.3	布线安全
7.13	11.2.4	设备维护
7.14	11.2.7	安全处置或再利用设备
8.1	06.2.1, 11.2.8	用户端点设备
8.2	09.2.3	特权访问权限
8.3	09.4.1	信息访问限制
8.4	09.4.5	访问源代码
8.5	09.4.2	安全身份验证
8.6	12.1.3	容量管理
8.7	12.2.1	防范恶意软件
8.8	12.6.1, 18.2.3	技术漏洞管理

表 B.1 （续）

ISO/IEC 27018:2025 控制 标识符	ISO/IEC 27018:2019 控制 标识符	控件名称
8.9	新的	配置管理
8.10	新的	信息删除
8.11	新的	数据屏蔽
8.12	新的	防止数据泄露
8.13	12.3.1	信息备份
8.14	17.2.1	信息处理设施的冗余
8.15	12.4.1、12.4.2、12.4.3	日志记录
8.16	新的	监控活动
8.17	12.4.4	时钟同步
8.18	09.4.4	使用特权实用程序
8.19	12.5.1, 12.6.2	在操作系统上安装软件
8.20	13.1.1	网络安全
8.21	13.1.2	网络服务安全
8.22	13.1.3	网络隔离
8.23	新的	Web 过滤
8.24	10.1.1、10.1.2	密码学的使用
8.25	14.2.1	安全开发生命周期
8.26	14.1.2, 14.1.3	应用程序安全要求
8.27	14.2.5	安全系统架构与工程原理
8.28	新的	安全编码
8.29	14.2.8, 14.2.9	开发和验收中的安全测试
8.30	14.2.7	外包开发
8.31	12.1.4, 14.2.6	开发、测试和生产环境的分离
8.32	12.1.2、14.2.2、14.2.3, 14.2.4	变更管理
8.33	14.3.1	测试信息
8.34	12.7.1	审计测试期间的信息系统保护

参考书目

[1] ISO 9000,质量管理体系 基础和词汇

[2] ISO 55001,资产管理 - 资产管理体系 - 要求

[3] ISO/IEC 11770（所有部分）,信息安全 密钥管理

[4] ISO/IEC 15408（所有部分）,信息安全、网络安全和隐私保护 IT安全评估标准

[5] ISO 15489（所有部分）,信息和文档 记录管理

[6] ISO/IEC 22123-1,信息技术 - 云计算 - 第 1 部分:词汇

[7] ISO/IEC 22123-2,信息技术 - 云计算 - 第 2 部分:概念

[8] ISO/IEC 22123-3,信息技术 云计算 第 3 部分:参考架构

[9] ISO/IEC 19086（所有部分）,云计算 服务水平协议（SLA)框架

[10] ISO/IEC 19770（所有部分）,信息技术 - IT资产管理

[11] ISO/IEC 19941,信息技术 - 云计算 - 互操作性和可移植性

[12] ISO/IEC 20889,隐私增强数据去识别术语和技术分类

[13] ISO 21500,项目、项目群和项目组合管理 背景和概念

[14] ISO 21502,项目、项目群和项目组合管理 项目管理指南

[15] ISO 22301,安全性和弹性 业务连续性管理系统 要求

[16] ISO 22313,安全性和弹性 业务连续性管理系统 使用指南
ISO 22301

[17] ISO/TS 22317,安全性和弹性 业务连续性管理系统 指南
业务影响分析

[18] ISO 22396,安全性和恢复力 社区恢复力 信息交换指南
组织之间

[19] ISO/IEC/TS 23167,信息技术 - 云计算 - 通用技术和技巧

[20] ISO/IEC 23751,信息技术 - 云计算和分布式平台 - 数据共享协议（DSA)框架

[21] ISO/IEC 24760（所有部分）， IT 安全和隐私 身份管理框架

[22] ISO/IEC 27001:2022,信息安全、网络安全和隐私保护 信息安全管理体系 要求

[23] ISO/IEC 27002:2013,信息技术安全技术信息安全实践准则
安全控制1)

[24] ISO/IEC 27005,信息安全、网络安全和隐私保护 信息安全风险管理指南

[25] ISO/IEC 27007,信息安全、网络安全和隐私保护 信息安全管理系统审计指南

1) 取消并由 ISO/IEC 27002:2022 取代。

[26] ISO/IEC/TS 27008,信息技术-安全技术-信息安全控制评估指南

[27] ISO/IEC 27011,信息安全、网络安全和隐私保护　信息安全
基于 ISO/IEC 27002 的电信组织控制

[28] ISO/IEC/TR 27016,信息技术-安全技术-信息安全管理
组织经济学

[29] ISO/IEC 27017,信息技术安全技术信息安全实践准则
基于 ISO/IEC 27002 的云服务安全控制

[30] ISO/IEC 27018,信息技术 - 安全技术 - 作为 PII 处理器的公共云中个人身份信息 (PII) 保护实践准则

[31] ISO/IEC 27019,信息安全、网络安全和隐私保护　能源公用事业行业的信息安全控制

[32] ISO/IEC 27031,网络安全　信息和通信技术为企业做好准备
连续性

[33] ISO/IEC 27033（所有部分）， --信息技术-网络安全

[34] ISO/IEC 27034（所有部分）,信息技术-应用安全

[35] ISO/IEC 27035-1,信息技术　信息安全事件管理　第 1 部分：
原则和流程

[36] ISO/IEC 27035-2,信息技术　信息安全事件管理　第 2 部分：
计划和准备事件响应的指南

[37] ISO/IEC 27036（所有部分）,网络安全　供应商关系

[38] ISO/IEC 27037,信息技术　安全技术　数字证据识别、收集、获取和保存指南

[39] ISO/IEC 27040,信息技术安全技术存储安全

[40] ISO/IEC 27050（所有部分）,信息技术 - 电子发现

[41] ISO/IEC/TS 27110,信息技术、网络安全和隐私保护　网络安全
框架开发指南

[42] ISO/IEC 27701,安全技术　ISO/IEC 27001 和 ISO/IEC 27002 隐私保护的扩展
信息管理　要求和指南

[43] ISO 27799,卫生信息学　采用 ISO/IEC 27002 进行卫生信息安全管理

[44] ISO/IEC 29100,信息技术安全技术隐私框架

[45] ISO/IEC 29115,信息技术安全技术实体认证保证
框架

[46] ISO/IEC 29134,信息技术 - 安全技术 - 隐私影响指南
评估

[47] ISO/IEC 29146,信息技术安全技术访问管理框架

[48] ISO/IEC 29147,信息技术安全技术漏洞披露

[49] ISO 30000,船舶和航海技术　船舶回收管理系统　安全和环境无害化船舶回收设施管理系统规范

[50] ISO/IEC 30111,信息技术安全技术漏洞处理流程

[51] ISO 31000:2018,风险管理　指南

[52] IEC 31010,风险管理-风险评估技术

[53] ISO/IEC 22123（所有部分）,信息技术 - 云计算

[54] ISO/IEC 27555,信息安全、网络安全和隐私保护　个人信息保护指南
可识别信息删除

[55] 信息安全论坛（ISF）。ISF信息安全良好实践标准2020，
请访问： https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-信息安全/

[56] ITIL® Foundation,ITIL 4 版,AXELOS,2019 年 2 月,ISBN:9780113316076

[57] 美国国家标准与技术研究院 (NIST),SP 800-37,《信息系统和组织风险管理框架:安全与隐私的系统生命周期方法》,修订版 2。2018 年 12 月[查看日期 2023 年 8 月 9 日]。网址： https://doi.org/10.6028/NIST.SP.800-37r2

[58] 开放 Web 应用安全项目 (OWASP)。OWASP Top Ten - 2021,十大最关键的 Web 应用安全风险， 2021 年 [查看日期:2023 年 8 月 9 日]。网址： https://owasp.org/Top10/

[59] 开放 Web 应用安全项目 (OWASP)。OWASP开发者指南， [在线] [浏览日期:2023-08-09]。网址： https://owasp.org/www-project-developer-guide/

[60] 开放 Web 应用安全项目 (OWASP)。OWASP十大 API 安全风险 – 2023 年， [在线] [查看日期:2023 年 8 月 9 日]。网址： https://owasp.org/API-Security/editions/2023/en/0x11-t10/

[61] 美国国家标准与技术研究院 (NIST),SP 800-63B， 《数字身份指南;身份验证和生命周期管理》 。2020 年 2 月 [查看日期:2023 年 8 月 9 日]。网址： https://doi.org/10.6028/NIST.SP.800-63b

[62] OASIS， 《结构化威胁信息表达》。网址:https: //www.oasis-open.org/standards#stix2.0

[63] OASIS， 《可信自动指标信息交换》。网址： https://www.oasis-open.org/标准#taxii2.0

[64] ISO 31700-1:2023,消费者保护　消费品和服务的隐私设计　第 1 部分：
高层要求

[65] ISO/TR 31700-2:2023,消费者保护　消费品和服务的隐私设计
第 2 部分:用例

ICS 35.030
价格基于 35 页

iso.org

International Standard

ISO/IEC 27018

Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors

Sécurité de l'information, cybersécurité et protection de la vie privée — Lignes directrices en matière de protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

Third edition
2025-08

Reference number
ISO/IEC 27018:2025(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27018:2019), which has been technically revised.

The main changes are as follows:

— the text has been aligned with ISO/IEC 27002:2022;

— Annex B has been added.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

0.1 Background and context

Cloud service providers who process personally identifiable information (PII) under contract to their customers are expected to operate their services in ways that allow both parties to meet the requirements of applicable legislation and regulations covering the protection of PII. The requirements and the way in which the requirements are divided between the cloud service provider and its customers vary according to legal jurisdiction, and according to the terms of the contract between the cloud service provider and the customer. Legislation which governs how PII is allowed to be processed (i.e. collected, used, transferred and disposed of) is sometimes referred to as data protection legislation; PII is sometimes referred to as personal data or personal information. The obligations falling on a PII processor vary from jurisdiction to jurisdiction, which makes it challenging for businesses providing cloud computing services to operate in a multinational environment.

A public cloud service provider is a "PII processor" when it processes PII for and according to the instructions of a cloud service customer. The cloud service customer, who has the contractual relationship with the public cloud PII processor, can range from a natural person (i.e. a "PII principal", processing his or her own PII in the cloud) to an organization (i.e. a "PII controller", processing PII relating to many PII principals). The cloud service customer can authorize one or more cloud service users associated with it to use the services made available to the customer under its contract with the public cloud PII processor. The cloud service customer has authority over the processing and use of the data. A cloud service customer who is also a PII controller can be subject to a wider set of obligations governing the protection of PII than the public cloud PII processor. Maintaining the distinction between PII controller and PII processor relies on the public cloud PII processor having no data processing objectives other than those set by the cloud service customer with respect to the PII it processes and the operations necessary to achieve the cloud service customer's objectives.

NOTE 1 Where the public cloud PII processor is processing cloud service customer account data, it can be acting as a PII controller for this purpose. This document does not cover such activity.

The intention of this document, when used in conjunction with the information security objectives and controls in ISO/IEC 27002, is to create a common set of security categories and controls that can be implemented by a public cloud computing service provider acting as a PII processor. This document has the following objectives:

— to enable the public cloud PII processor to be transparent in relevant matters so that cloud service customers can select well-governed cloud-based PII processing services;

— to assist the cloud service customer and the public cloud PII processor in entering into a contractual agreement;

— to provide cloud service customers with a mechanism for exercising audit and compliance rights and responsibilities in cases where the individual cloud service customer data, which are hosted in a multi-party, virtualized server (cloud) environment, can be technically impractical to audit and can potentially increase risks to those physical and logical network security controls in place.

NOTE 2 It is expected that public cloud service providers comply with applicable obligations when acting as a PII processor.

This document can assist by providing a common compliance framework for public cloud service providers, in particular those that operate in a multinational market.

0.2 PII protection controls for public cloud computing services

This document is designed for organizations to use as a reference for selecting PII protection controls within the process of implementing a cloud computing information security management system based on ISO/IEC 27001, or as a guidance document for implementing commonly accepted PII protection controls for organizations acting as public cloud PII processors. In particular, this document has been based on ISO/IEC 27002, taking into consideration the specific risk environment(s) arising from those PII protection requirements which can apply to public cloud computing service providers acting as PII processors.

In the context of PII protection requirements for a public cloud service provider acting as a PII processor, the organization is protecting the information assets entrusted to it by its customers. Implementation of the controls of ISO/IEC 27002 by the public cloud PII processor is both suitable for this purpose and necessary. This document extends the ISO/IEC 27002 controls to accommodate the distributed nature of the risk and the existence of a contractual relationship between the cloud service customer and the public cloud PII processor. This document extends ISO/IEC 27002 in two ways, by providing:

— implementation guidance applicable to public cloud PII protection for some of the existing ISO/IEC 27002 controls, and

— a set of additional controls and associated guidance in Annex A intended to address public cloud PII protection requirements not addressed by the existing ISO/IEC 27002 control set, organized in line with the privacy principles of ISO/IEC 29100.

Most of the controls and guidelines in this document also apply to a PII controller. However, the PII controller is, in most cases, subject to additional obligations not specified here.

0.3 PII protection requirements

It is essential that an organization identifies its requirements for the protection of PII. There are three main sources of requirement, as given below.

a) Legal and contractual requirements: One source is the legal and contractual requirements to which an organization, its trading partners, contractors and service providers are bound, as well as responsibilities concerning their socio-cultural and operating environment. It should be noted that legislation, regulations and contractual commitments made by the PII processor can mandate the selection of particular controls and can also necessitate specific criteria for implementing those controls. These requirements can vary from one jurisdiction to another.

b) Risks: Another source is derived from assessing risks to the organization associated with PII, taking into account the organization's overall business strategy and objectives. Through a risk assessment, risks are identified, their consequence and likelihood are assessed and risks are evaluated. ISO/IEC 27005 provides information security risk management guidance, including advice on risk assessment, risk acceptance, risk communication, risk monitoring and risk review. ISO/IEC 29134 provides guidelines on privacy impact assessment.

c) Corporate policies: While many aspects covered by a corporate policy are derived from legal and socio-cultural requirements, an organization can also choose voluntarily to go beyond the criteria that are derived from the requirements of a).

0.4 Selecting and implementing controls in a cloud computing environment

Controls can be selected from this document (which includes by reference the controls from ISO/IEC 27002, creating a combined reference control set for the sector or application defined by the relevant sector). If required, controls can also be selected from other control sets, or new controls can be designed to meet specific needs as appropriate.

NOTE A PII processing service provided by a public cloud PII processor can be considered as an application of cloud computing rather than as a sector in itself. Nevertheless, the term "public cloud service provider-specific" is used in this document, as this is the conventional term used within other Information Security Management systems standards developed by ISO/IEC JTC 1/SC 27.

The selection of controls is dependent on organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization and, through contractual agreements, its customers and suppliers. It is also subject to relevant national and international legislation. Where organizations/public cloud providers do not select the controls specified in this document, a justification should be provided.

Further, the selection and implementation of controls is dependent on the public cloud provider's actual role in the context of the whole cloud computing reference architecture (see ISO/IEC 22123-3). Many different organizations can be involved in providing infrastructure and application services in a cloud computing environment. In some circumstances, selected controls can be unique to a particular service category of

the cloud computing reference architecture. In other instances, there can be shared roles in implementing security controls. Contractual agreements are expected to specify the PII protection responsibilities of all organizations involved in providing or using the cloud services, including the public cloud PII processor, its sub-contractors and the cloud service customer.

The controls in this document can be considered as guiding principles and applicable for most organizations. They are explained in more detail in this document along with implementation guidance. Implementation can be made simpler if requirements for the protection of PII have been considered in the design of the public cloud PII processor's information system, services and operations. Such consideration is an element of the concept that is often called "privacy by design" (see References [64] and [65]).

0.5 Developing additional guidelines

This document can be regarded as a starting point for developing PII protection guidelines. It is possible that not all of the controls and guidance in this code of practice are applicable. Furthermore, additional controls and guidelines not included in this document can be required. When documents are developed containing additional guidelines or controls, it can be useful to include cross-references to clauses in this document where applicable to facilitate compliance checking by auditors and business partners.

0.6 Lifecycle considerations

PII has a natural lifecycle, from creation and origination, through to storage, processing, use and transmission, to its eventual destruction or disuse. The risks to PII can vary during its lifetime but protection of PII remains important at all stages.

PII protection requirements are expected to be taken into account as existing and new information systems are managed through their lifecycle.

Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors

1 Scope

This document establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect personally identifiable information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

In particular, this document specifies guidelines based on ISO/IEC 27002:2022, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations.

The guidelines in this document can also be relevant to organizations acting as PII controllers.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

ISO/IEC 22123-1, *Information technology — Cloud computing — Part 1: Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22123-1, ISO/IEC 27000, ISO/IEC 27002 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
data breach
compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected data transmitted, stored or otherwise processed

[SOURCE: ISO/IEC 27040:2024, 3.5.2]

3.2
personally identifiable information
PII
information that a) can be used to establish a link between the information and the natural person to whom such information relates, or b) is or can be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the *PII principal* (3.4). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

Note 2 to entry: This definition is included to define the term PII as used in this document. A public cloud *PII processor* (3.5) is typically not in a position to know explicitly whether information it processes falls into any specified category unless this is made transparent by the cloud service customer.

[SOURCE: ISO/IEC 29100:2024, 3.7, modified — Note 2 to entry has been added.]

3.3
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.2) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others [e.g. *PII processors* (3.5)] to process PII on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100:2024, 3.8]

3.4
PII principal
natural person to whom the *personally identifiable information (PII)* (3.2) relates

Note 1 to entry: Depending on the jurisdiction and the particular PII protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2024, 3.9, modified — Note 1 to entry has been added.]

3.5
PII processor
privacy stakeholder that processes *personally identifiable information (PII)* (3.2) on behalf of and in accordance with the instructions of a *PII controller* (3.3)

[SOURCE: ISO/IEC 29100:2024, 3.10]

3.6
PII processing
processing of PII
operation or set of operations performed on *personally identifiable information (PII)* (3.2)

Note 1 to entry: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.

[SOURCE: ISO/IEC 29100:2024, 3.21, modified — "PII processing" has been added as the preferred term.]

3.7
public cloud service provider
party which makes cloud services available according to the public cloud model

4 Overview

4.1 Structure of this document

This document follows the structure used in ISO/IEC 27002:2022 for the description of controls. In this aspect, the same strategy that was adopted in the earlier version of this document (ISO/IEC 27018:2019), in mirroring the controls in ISO/IEC 27002:2013,[1] has been repeated here.

Annex B provides a comparison of the two control layouts in this document and the previous edition (ISO/IEC 27018:2019).

Specifically, the following rules have been used in mirroring the controls in ISO/IEC 27002:2022 in this document. In cases where the various elements of the control layout (described in 4.2) for a control are identical, only a reference is provided to the corresponding control in ISO/IEC 27002:2022. For those controls that require additional guidance and related information in the context of public cloud PII protection, additional guidance is provided under the headings "Public cloud PII protection implementation guidance" and "Other information for public cloud PII protection" respectively. This type of guidance is also referred to using the term "Public cloud service provider-specific implementation guidance". Besides these, additional controls and associated implementation guidance applicable to PII protection for cloud computing service providers are described in Annex A. Finally, the clause numbers in this document are aligned with the corresponding clause numbers in ISO/IEC 27002:2022.

The controls in Table 1 are organized into four themes, which correspond to the controls listed in Clauses 5 to 8 as follows:

— the theme "Public cloud service provider-specific implementation guidance is provided" corresponds to the control "Public cloud PII protection implementation guidance";

— the theme "Public cloud service provider-specific implementation guidance and other information is provided" corresponds to the control "Public cloud PII protection implementation guidance and other information for Public cloud PII protection";

— the theme "No additional public cloud service provider-specific implementation guidance or other informationisprovided"correspondstothecontrol"nospecificGuidanceorotherinformationforPublic cloud PII protection";

— the theme "Public cloud service provider-specific implementation guidance is provided, together with a cross-reference to control(s) in Annex A" corresponds to the control "Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A".

Table 1 — Location of public cloud service provider-specific guidance and other information for implementing controls in ISO/IEC 27002:2022

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
Clause 5 – Organizational controls		
5.1	Policies for information security	Public cloud service provider-specific implementation guidance and other information is provided.[c]
5.2	Information security roles and responsibilities	Public cloud service provider-specific implementation guidance is provided.[b]
5.3	Segregation of duties	No additional public cloud service provider-specific implementation guidance or other information is provided.[d]
5.4	Management responsibilities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.5	Contact with authorities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.6	Contact with special interest groups	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.7 [a]	Threat intelligence	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.8	Information security in project management	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.9	Inventory of information and other associated assets	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.10	Acceptable use of information and other associated assets	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.11	Return of assets	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.12	Classification of information	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.13	Labelling of information	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as "Public cloud PII protection implementation guidance".

[c] This control is applicable as "Public cloud PII protection implementation guidance and other information for public cloud PII protection".

[d] This control is applicable as "no specific Guidance or other information for Public cloud PII protection".

[e] This control is applicable as "Public cloud PII protection implementation guidance and cross-reference to control(s) in ". Annex A

Table 1 *(continued)*

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
5.14	Information transfer	Public cloud service provider-specific implementation guidance is provided. [b]
5.15	Access control	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.16	Identity management	Public cloud service provider-specific implementation guidance is provided. [b]
5.17	Authentication information	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.18	Access rights	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.19	Information security in supplier relationships	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.20	Addressing information security within supplier agreements	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.21	Managing information security in the ICT supply chain	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.22	Monitoring, review and change management of supplier services	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.23 [a]	Information security for use of cloud services	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.24	Information security incident management planning and preparation	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.25	Assessment and decision on information security events	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.26	Response to information security incidents	Public cloud service provider-specific implementation guidance is provided, together with a cross-reference to control(s) in Annex A. [e]
5.27	Learning from information security incidents	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.28	Collection of evidence	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as "Public cloud PII protection implementation guidance".

[c] This control is applicable as "Public cloud PII protection implementation guidance and other information for public cloud PII protection".

[d] This control is applicable as "no specific Guidance or other information for Public cloud PII protection".

[e] This control is applicable as "Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A".

Table 1 *(continued)*

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
5.29	Information security during disruption	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.30 [a]	ICT readiness for business continuity	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.31	Legal, statutory, regulatory and contractual requirements	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.32	Intellectual property rights	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.33	Protection of records	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.34	Privacy and protection of PII	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.35	Independent review of information security	Public cloud service provider-specific implementation guidance is provided. [b]
5.36	Compliance with policies, rules and standards for information security	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
5.37	Documented operating procedures	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
Clause 6 – People controls		
6.1	Screening	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
6.2	Terms and conditions of employment	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
6.3	Information security awareness, education and training	Public cloud service provider-specific implementation guidance and other information is provided.[c]
6.4	Disciplinary process	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
6.5	Responsibilities after termination or change of employment	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as "Public cloud PII protection implementation guidance".

[c] This control is applicable as "Public cloud PII protection implementation guidance and other information for public cloud PII protection".

[d] This control is applicable as "no specific Guidance or other information for Public cloud PII protection".

[e] This control is applicable as "Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A".

Table 1 *(continued)*

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
6.6	Confidentiality or non-disclosure agreements	Public cloud service provider-specific implementation guidance is provided, together with a cross-reference to control(s) in Annex A. [e]
6.7	Remote working	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
6.8	Information security event reporting	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
Clause 7 – Physical controls		
7.1	Physical security perimeters	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.2	Physical entry	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.3	Securing offices, rooms and facilities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.4 [a]	Physical security monitoring	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.5	Protecting against physical and environmental threats	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.6	Working in secure areas	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.7	Clear desk and clear screen	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.8	Equipment siting and protection	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.9	Security of assets off-premises	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.10	Storage media	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.11	Supporting utilities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as "Public cloud PII protection implementation guidance".

[c] This control is applicable as "Public cloud PII protection implementation guidance and other information for public cloud PII protection".

[d] This control is applicable as "no specific Guidance or other information for Public cloud PII protection".

[e] This control is applicable as "Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A".

Table 1 *(continued)*

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
7.12	Cabling security	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.13	Equipment maintenance	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
7.14	Secure disposal or re-use of equipment	Public cloud service provider-specific implementation guidance is provided, together with a cross-reference to control(s) in Annex A. [e]
Clause 8 – Technological controls		
8.1	User endpoint devices	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.2	Privileged access rights	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.3	Information access restriction	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.4	Access to source code	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.5	Secure authentication	Public cloud service provider-specific implementation guidance is provided. [b]
8.6	Capacity management	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.7	Protection against malware	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.8	Management of technical vulnerabilities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.9 [a]	Configuration management	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.10 [a]	Information deletion	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.11 [a]	Data masking	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as "Public cloud PII protection implementation guidance".

[c] This control is applicable as "Public cloud PII protection implementation guidance and other information for public cloud PII protection".

[d] This control is applicable as "no specific Guidance or other information for Public cloud PII protection".

[e] This control is applicable as "Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A".

Table 1 *(continued)*

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
8.12 [a]	Data leakage prevention	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.13	Information backup	Public cloud service provider-specific implementation guidance is provided. [b]
8.14	Redundancy of information processing facilities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.15	Logging	Public cloud service provider-specific implementation guidance is provided, together with a cross-reference to control(s) in Annex A. [e]
8.16 [a]	Monitoring activities	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.17	Clock synchronization	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.18	Use of privileged utility programs	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.19	Installation of software on operational systems	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.20	Networks security	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.21	Security of network services	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.22	Segregation of networks	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.23 [a]	Web filtering	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.24	Use of cryptography	Public cloud service provider-specific implementation guidance is provided. [b]
8.25	Secure development lifecycle	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.26	Application security requirements	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as "Public cloud PII protection implementation guidance".

[c] This control is applicable as "Public cloud PII protection implementation guidance and other information for public cloud PII protection".

[d] This control is applicable as "no specific Guidance or other information for Public cloud PII protection".

[e] This control is applicable as "Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A".

Table 1 *(continued)*

ISO/IEC 27002:2022 Control identifier	ISO/IEC 27002:2022 Control name	Theme
8.27	Secure system architecture and engineering principles	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.28 [a]	Secure coding	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.29	Security testing in development and acceptance	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.30	Outsourced development	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.31	Separation of development, test and production environments	Public cloud service provider-specific implementation guidance is provided. [b]
8.32	Change management	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.33	Test information	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]
8.34	Protection of information systems during audit testing	No additional public cloud service provider-specific implementation guidance or other information is provided. [d]

[a] New control introduced in ISO/IEC 27002:2022.

[b] This control is applicable as "Public cloud PII protection implementation guidance".

[c] This control is applicable as "Public cloud PII protection implementation guidance and other information for public cloud PII protection".

[d] This control is applicable as "no specific Guidance or other information for Public cloud PII protection".

[e] This control is applicable as "Public cloud PII protection implementation guidance and cross-reference to control(s) in Annex A".

4.2 Control layout

In line with ISO/IEC 27002:2022, the entire set of controls are categorized under the 4 themes found in Table 1 above. Each control has the following elements:

a) Control title: short name of the control;

b) Attribute table: a table shows the value(s) of each attribute for the given control;

c) Control: what the control is;

d) Purpose: why the control should be implemented;

e) Guidance: how the control should be implemented;

f) Other information: explanatory text or references to other related documents.

Subheadings are used in the guidance text for some controls to aid readability where guidance is lengthy and addresses multiple topics. Such headings are not necessarily used in all guidance text.

g) Public cloud PII protection guidance

This provides more detailed information to support the implementation of the control and to meet the control objectives. The guidance should not be considered as entirely suitable or sufficient in all situations and hence will not fulfil the organization's specific control requirements. Alternative or additional controls, or other forms of risk treatment (e.g. avoiding, transferring, or accepting risks), can therefore be appropriate.

h) Other information for public cloud PII protection

This provides further information that is expected to be considered, such as legal considerations and references to other standards.

5 Organizational controls

5.1 Policies for information security

The guidance in ISO/IEC 27002:2022, 5.1 applies. In addition, the following public cloud service provider-specific guidance and associated information also apply.

a) Public cloud PII protection implementation guidance

Contractual agreements should allocate responsibilities between the public cloud PII processor, its sub-contractors and the cloud service customer, taking into account the type of cloud service in question [e.g. a service of an Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) category of the cloud computing reference architecture]. For example, the allocation of responsibility for application layer controls can differ depending on whether the public cloud PII processor is providing a SaaS service or rather is providing a PaaS or IaaS service on which the cloud service customer can build or layer its own applications.

b) Other information for public cloud PII protection

In some jurisdictions, the public cloud PII processor is directly subject to PII protection legislation. In others, PII protection legislation can apply to the PII controller only.

It is necessary that the contract between the cloud service customer and the public cloud PII processor includes a mechanism to ensure the public cloud PII processor supports and manages compliance with the contract between the cloud service customer and the public cloud PII processor. The contract can call for independently audited compliance, acceptable to the cloud service customer, e.g. via the implementation of the relevant controls in this document and in ISO/IEC 27002.

5.2 Information security roles and responsibilities

The guidance in ISO/IEC 27002:2022, 5.2 applies. In addition, the following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

The public cloud PII processor should have a PII specialist who advises the cloud service customers on the proper handling of PII information.

5.3 Segregation of duties

The guidance in ISO/IEC 27002:2022, 5.3 applies.

5.4 Management responsibilities

The guidance in ISO/IEC 27002:2022, 5.4 applies.

5.5 Contact with authorities

The guidance in ISO/IEC 27002:2022, 5.5 applies.

5.6 Contact with special interest groups

The guidance in ISO/IEC 27002:2022, 5.6 applies.

5.7 Threat intelligence

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 5.7 applies.

5.8 Information security in project management

The guidance in ISO/IEC 27002:2022, 5.8 applies.

5.9 Inventory of information and other associated assets

The guidance in ISO/IEC 27002:2022, 5.9 applies.

5.10 Acceptable use of information and other associated assets

The guidance in ISO/IEC 27002:2022, 5.10 applies.

5.11 Return of assets

The guidance in ISO/IEC 27002:2022, 5.11 applies.

5.12 Classification of information

The guidance in ISO/IEC 27002:2022, 5.12 applies.

5.13 Labelling of information

The guidance in ISO/IEC 27002:2022, 5.13 applies.

5.14 Information transfer

The guidance in ISO/IEC 27002:2022, 5.14 applies. In addition, the following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

Whenever physical media are used for information transfer, a system should be put in place to record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/recipients, the date and time, and the number of physical media. Where appropriate, cloud service customers should implement, and public cloud PII processors should support technical capacity to apply, additional measures (such as encryption) to reduce the likelihood that unauthorized access could occur en route, prior to arrival at the intended destination. In these cases, both parties can apply their own such measures.

5.15 Access control

The guidance in ISO/IEC 27002:2022, 5.15 applies.

5.16 Identity management

The guidance in ISO/IEC 27002:2022, 5.16 applies. In addition, the following public cloud service provider-specific guidance and associated information also apply.

a) Public cloud PII protection implementation guidance

In the context of the service categories of the cloud computing reference architecture, the cloud service customer can be responsible for some or all aspects of access management for cloud service users under its control. Where appropriate, the public cloud PII processor should enable the cloud service customer to manage the access of cloud service users under the cloud service customer's control.

Procedures for user registration and de-registration should address the situation where user access control is compromised, such as the corruption or compromise of passwords or other user registration data (e.g. as a result of inadvertent disclosure).

NOTE Individual jurisdictions can impose specific requirements regarding the frequency of checks for unused authentication credentials. It is the responsibility of organizations operating in these jurisdictions to ensure that they comply with these requirements.

5.17 Authentication information

The guidance in ISO/IEC 27002:2022, 5.17 applies.

5.18 Access rights

The guidance in ISO/IEC 27002:2022, 5.18 applies.

5.19 Information security in supplier relationships

The guidance in ISO/IEC 27002:2022, 5.19 applies.

5.20 Addressing information security within supplier agreements

The guidance in ISO/IEC 27002:2022, 5.20 applies.

5.21 Managing information security in the ICT supply chain

The guidance in ISO/IEC 27002:2022, 5.21 applies.

5.22 Monitoring, review and change management of supplier services

The guidance in ISO/IEC 27002:2022, 5.22 applies.

5.23 Information security for use of cloud services

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 5.23 applies.

5.24 Information security incident management planning and preparation

The guidance in ISO/IEC 27002:2022, 5.24 applies.

5.25 Assessment and decision on information security events

The guidance in ISO/IEC 27002:2022, 5.25 applies.

5.26 Response to information security incidents

The guidance in ISO/IEC 27002:2022, 5.26 applies.

a) Public cloud PII protection implementation guidance

An information security incident should trigger a review by the public cloud PII processor, as part of its information security incident management process, to determine if a data breach involving PII has taken place (see A.10.1).

Not all information security events should necessarily trigger such a review. It is possible that an information security event does not result in actual, or the significant probability of, unauthorized access to PII or to any of the public cloud PII processor's equipment or facilities storing PII, and can include, without limitation, pings and other diagnostic probes to firewalls or edge servers.

5.27 Learning from information security incidents

The guidance in ISO/IEC 27002:2022, 5.27 applies.

5.28 Collection of evidence

The guidance in ISO/IEC 27002:2022, 5.28 applies.

5.29 Information security during disruption

The guidance in ISO/IEC 27002:2022, 5.29 applies.

5.30 ICT readiness for business continuity

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 5.30 applies.

5.31 Legal, statutory, regulatory and contractual requirements

The guidance in ISO/IEC 27002:2022, 5.31 applies.

5.32 Intellectual property rights

The guidance in ISO/IEC 27002:2022, 5.32 applies.

5.33 Protection of records

The guidance in ISO/IEC 27002:2022, 5.33 applies.

5.34 Privacy and protection of PII

The guidance in ISO/IEC 27002:2022, 5.34 applies.

5.35 Independent review of information security

The guidance in ISO/IEC 27002:2022, 5.35 applies. In addition, the following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

In cases where individual cloud service customer audits are impractical or can increase risks to security, the public cloud PII processor should make available to prospective cloud service customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and

operated according to the public cloud PII processor's policies and procedures. A relevant independent audit as selected by the public cloud PII processor should normally be an acceptable method for fulfilling the cloud service customer's interest in reviewing the public cloud PII processor's processing operations, provided sufficient transparency is provided.

5.36 Compliance with policies, rules and standards for information security

The guidance in ISO/IEC 27002:2022, 5.36 applies.

5.37 Documented operating procedures

The guidance in ISO/IEC 27002:2022, 5.37 applies.

6 People controls

6.1 Screening

The guidance in ISO/IEC 27002:2022, 6.1 applies.

6.2 Terms and conditions of employment

The guidance in ISO/IEC 27002:2022, 6.2 applies.

6.3 Information security awareness, education and training

The guidance in ISO/IEC 27002:2022, 6.3 applies. In addition, the following public cloud service provider-specific guidance and associated information also apply.

a) Public cloud PII protection implementation guidance

Measures should be put in place to make relevant staff aware of the possible consequences on the public cloud PII processor (e.g. loss of business and brand or reputational damage), on the staff member (e.g. disciplinary consequences) and on the PII principal (e.g. physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the handling of PII.

b) Other information for public cloud PII protection

In some jurisdictions, the public cloud PII processor can be subject to legal sanctions, including substantial fines directly from the local PII protection authority.

6.4 Disciplinary process

The guidance in ISO/IEC 27002:2022, 6.4 applies.

6.5 Responsibilities after termination or change of employment

The guidance in ISO/IEC 27002:2022, 6.5 applies.

6.6 Confidentiality or non-disclosure agreements

NOTE Additional controls and guidance relevant to confidentiality or non-disclosure agreements can be found in A.10.1.

The guidance in ISO/IEC 27002:2022, 6.6 applies.

6.7 Remote working

The guidance in ISO/IEC 27002:2022, 6.7 applies.

6.8 Information security event reporting

The guidance in ISO/IEC 27002:2022, 6.8 applies.

7 Physical controls

7.1 Physical security perimeters

The guidance in ISO/IEC 27002:2022, 7.1 applies.

7.2 Physical entry

The guidance in ISO/IEC 27002:2022, 7.2 applies.

7.3 Securing offices, rooms and facilities

The guidance in ISO/IEC 27002:2022, 7.3 applies.

7.4 Physical security monitoring

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 7.4 applies.

7.5 Protecting against physical and environmental threats

The guidance in ISO/IEC 27002:2022, 7.5 applies.

7.6 Working in secure areas

The guidance in ISO/IEC 27002:2022, 7.6 applies.

7.7 Clear desk and clear screen

The guidance in ISO/IEC 27002:2022, 7.7 applies.

7.8 Equipment siting and protection

The guidance in ISO/IEC 27002:2022, 7.8 applies.

7.9 Security of assets off-premises

The guidance in ISO/IEC 27002:2022, 7.9 applies.

7.10 Storage media

The guidance in ISO/IEC 27002:2022, 7.10 applies.

7.11 Supporting utilities

The guidance in ISO/IEC 27002:2022, 7.11 applies.

7.12 Cabling security

The guidance in ISO/IEC 27002:2022, 7.12 applies.

7.13 Equipment maintenance

The guidance in ISO/IEC 27002:2022, 7.13 applies.

7.14 Secure disposal or re-use of equipment

The guidance in ISO/IEC 27002:2022, 7.14 applies. The following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

For the purposes of secure disposal or re-use, equipment containing storage media that can possibly contain PII should be treated as though it does.

NOTE Additional controls and guidance relevant to secure disposal or re-use of equipment can be found in A.11.7.

8 Technological controls

8.1 User endpoint devices

The guidance in ISO/IEC 27002:2022, 8.1 applies.

8.2 Privileged access rights

The guidance in ISO/IEC 27002:2022, 8.2 applies.

8.3 Information access restriction

The guidance in ISO/IEC 27002:2022, 8.3 applies.

8.4 Access to source code

The guidance in ISO/IEC 27002:2022, 8.4 applies.

8.5 Secure authentication

The guidance in ISO/IEC 27002:2022, 8.5 applies. The following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

Where required, the public cloud PII processor should provide secure log-on procedures for any accounts requested by the cloud service customer for cloud service users under its control.

8.6 Capacity management

The guidance in ISO/IEC 27002:2022, 8.6 applies.

8.7 Protection against malware

The guidance in ISO/IEC 27002:2022, 8.7 applies.

8.8 Management of technical vulnerabilities

The guidance in ISO/IEC 27002:2022, 8.8 applies.

8.9 Configuration management

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.9 applies.

8.10 Information deletion

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.10 applies.

8.11 Data masking

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.11 applies.

8.12 Data leakage prevention

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.12 applies.

8.13 Information backup

The guidance in ISO/IEC 27002:2022, 8.13 applies. The following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

Information processing systems based on the cloud computing model introduce additional or alternative mechanisms to off-site backups for protecting against loss of data, ensuring continuity of data processing operations, and providing the ability to restore data processing operations after a disruptive event. Multiple copies of data in either physically or logically diverse locations or both (which can be within the information processing system itself) should be created or maintained for the purposes of either backup or recovery or both.

PII-specific responsibilities in this respect can lie with the cloud service customer. Where the public cloud PII processor explicitly provides backup and restore services to the cloud service customer, the public cloud PII processor should provide information to the cloud service customer about the capabilities of the cloud service with respect to backup and restoration of the cloud service customer data.

Procedures should be put in place to allow for restoration of data processing operations within a specified, documented period after a disruptive event.

The back-up and recovery procedures should be reviewed at a specified, documented frequency.

NOTE Some jurisdictions can impose specific requirements regarding the frequency of reviews of backup and recovery procedures. It is the responsibility of organizations operating in these jurisdictions to ensure that they comply with these requirements.

The use of sub-contractors to store replicated or backup copies of data being processed is covered by the controls A.8.1 and A.11.12 in this document applying to sub-contracted PII processing. Where physical media transfers take place this is also covered by controls 5.14 and A.11.5 in this document.

The public cloud PII processor should have a policy which addresses the requirements for the backup of information and any further requirements (e.g. contractual requirements) for the erasure of PII contained in information held for backup purposes.

8.14 Redundancy of information processing facilities

The guidance in ISO/IEC 27002:2022, 8.14 applies.

8.15 Logging

The guidance in ISO/IEC 27002:2022, 8.15 applies. The following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

A process should be put in place to review event logs with a specified, documented periodicity, to identify irregularities and propose remediation efforts.

Where possible, event logs should record whether or not PII has been changed (e.g. added, modified or deleted) as a result of an event and by whom. Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there can be varied or shared roles in implementing this guidance.

The public cloud PII processor should define criteria regarding if, when and how log information can be made available to or usable by the cloud service customer. These procedures should be made available to the cloud service customer.

Where a cloud service customer is permitted to access log records controlled by the public cloud PII processor, the public cloud PII processor should ensure that the cloud service customer can only access records that relate to that cloud service customer's activities, and cannot access any log records which relate to the activities of other cloud service customers.

Log information recorded for purposes such as security monitoring and operational diagnostics can contain PII. Measures, such as controlling access, should be put in place to ensure that logged information is only used for its intended purposes.

A procedure, preferably automatic, should be put in place to ensure that logged information is deleted within a specified and documented period.

8.16 Monitoring activities

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.16 applies.

8.17 Clock synchronization

The guidance in ISO/IEC 27002:2022, 8.17 applies.

8.18 Use of privileged utility programs

The guidance in ISO/IEC 27002:2022, 8.18 applies.

8.19 Installation of software on operational systems

The guidance in ISO/IEC 27002:2022, 8.19 applies.

8.20 Networks security

The guidance in ISO/IEC 27002:2022, 8.20 applies.

8.21 Security of network services

The guidance in ISO/IEC 27002:2022, 8.21 applies.

8.22 Segregation of networks

The guidance in ISO/IEC 27002:2022, 8.22 applies.

8.23 Web filtering

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.23 applies.

8.24 Use of cryptography

The guidance in ISO/IEC 27002:2022, 8.24 applies. The following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

The public cloud PII processor should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying and managing its own cryptographic protection and processes such as various methods to manage keys or secrets in a vault, key management system (KMS), hardware security module (HSM) backed service, cloud HSM, etc.

NOTE In some jurisdictions, it can be required to apply cryptography to protect particular kinds of PII, such as health data concerning a PII principal, resident registration numbers, passport numbers and driver's licence numbers.

8.25 Secure development lifecycle

The guidance in ISO/IEC 27002:2022, 8.25 applies.

8.26 Application security requirements

The guidance in ISO/IEC 27002:2022, 8.26 applies.

8.27 Secure system architecture and engineering principles

The guidance in ISO/IEC 27002:2022, 8.27 applies.

8.28 Secure coding

NOTE New control introduced in ISO/IEC 27002:2022.

The guidance in ISO/IEC 27002:2022, 8.28 applies.

8.29 Security testing in development and acceptance

The guidance in ISO/IEC 27002:2022, 8.29 applies.

8.30 Outsourced development

The guidance in ISO/IEC 27002:2022, 8.30 applies.

8.31 Separation of development, test and production environments

The guidance in ISO/IEC 27002:2022, 8.31 applies. The following public cloud service provider-specific guidance also applies.

a) Public cloud PII protection implementation guidance

Where the use of PII for testing purposes cannot be avoided, a risk assessment should be undertaken. Technical and organizational measures should be implemented to minimize the risks identified.

8.32 Change management

The guidance in ISO/IEC 27002:2022, 8.32 applies.

8.33 Test information

The guidance in ISO/IEC 27002:2022, 8.33 applies.

8.34 Protection of information systems during audit testing

The guidance in ISO/IEC 27002:2022, 8.34 applies.

Annex A
(informative)

Public cloud PII processor extended control set for PII protection

A.1 General

This annex specifies new controls and associated implementation guidance which, in combination with the controls and guidance in ISO/IEC 27002 (see Clauses 5 to 8), make up an extended control set to meet the requirements for PII protection which apply to public cloud service providers acting as PII processors.

These additional controls are classified according to the 11 privacy principles of ISO/IEC 29100. In many cases, the controls can be classified under more than one of the privacy principles. In such cases, they are classified under the most relevant principle.

A.2 Consent and choice

A.2.1 Obligation to co-operate regarding PII principals' rights

a) Control

The public cloud PII processor should enable the cloud service customer to fulfil their obligations, by providing them with the means to facilitate the exercise of the PII principals' rights to access, correct and erase PII pertaining to them.

b) Public cloud PII protection implementation guidance

The PII controller's obligations in this respect can be defined by law, by regulations or by contract. These obligations can include matters where the cloud service customer uses the services of the public cloud PII processor for implementation. For example, this can include the correction or deletion of PII in a timely fashion.

Where the PII controller depends on the public cloud PII processor for information or technical measures to facilitate the exercise of PII principals' rights, the relevant information or technical measures should be specified in the contract.

A.3 Purpose legitimacy and specification

A.3.1 Public cloud PII processor's purpose

a) Control

PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer.

b) Public cloud PII protection implementation guidance

Instructions can be contained in the contract between the public cloud PII processor and the cloud service customer including, e.g. the objective and time frame to be achieved by the service.

In order to achieve the cloud service customer's purpose, there can be technical reasons why it is appropriate for a public cloud PII processor to determine the method for PII processing, consistent with the general instructions of the cloud service customer but without the cloud service customer's express instruction. For example, in order to efficiently utilize network or processing capacity it can be necessary to allocate specific

processing resources depending on certain characteristics of the PII principal. In circumstances where the public cloud PII processor's determination of the processing method involves the collection and use of PII, the public cloud PII processor should adhere to the relevant privacy principles set forth in ISO/IEC 29100 and the principles of "privacy by design" (see References [64] and [65]).

The public cloud PII processor should provide the cloud service customer with all relevant information, in a timely fashion, to allow the cloud service customer to ensure the public cloud PII processor's compliance with purpose specification and limitation principles and ensure that no PII is processed by the public cloud PII processor or any of its sub-contractors for further purposes independent of the instructions of the cloud service customer.

A.3.2 Public cloud PII processor's commercial use

a) Control

PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.

NOTE This control is an addition to the more general control in A.3.1 and does not replace or otherwise supersede it.

A.4 Collection limitation

No additional controls are relevant to this privacy principle.

A.5 Data minimization

A.5.1 Secure erasure of temporary files

a) Control

Temporary files and documents should be erased or destroyed within a specified, documented period.

b) Public cloud PII protection implementation guidance

Implementation guidance on PII erasure is provided in A.10.3.

Information systems can create temporary files in the normal course of their operation. Such files are specific to the system or application, but can include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed and should be deleted after completion unless the particular circumstances require that they should not be deleted. The length of time for which these files remain in use is not always deterministic but a "garbage collection" procedure should identify the relevant files and determine how long it has been since they were last used.

PII processing information systems should implement a periodic check that unused temporary files above a specified age are deleted.

A.6 Use, retention and disclosure limitation

A.6.1 PII disclosure notification

a) Control

It is expected that the contract between the public cloud PII processor and the cloud service customer requires the public cloud PII processor to notify the cloud service customer, according to any procedure and

time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.

b) Public cloud PII protection implementation guidance

The public cloud PII processor should provide contractual guarantees that it will:

— reject any requests for PII disclosure that are not legally binding;

— consult the corresponding cloud service customer, where legally permissible, before making any PII disclosure; and

— accept any contractually agreed requests for PII disclosures that are authorized by the corresponding cloud service customer.

EXAMPLE A possible prohibition on disclosure would be a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

A.6.2 Recording of PII disclosures

a) Control

Disclosure of PII to third parties should be recorded, including what PII has been disclosed, the reason for disclosing the PII, to whom and at what time.

b) Public cloud PII protection implementation guidance

PII can be disclosed during the course of normal operations. These disclosures should be recorded. Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure, reason for disclosure and the source of the authority to make the disclosure.

A.7 Accuracy and quality

No additional controls are relevant to this privacy principle.

A.8 Openness, transparency and notice

A.8.1 Disclosure of sub-contracted PII processing

a) Control

If public cloud PII processors intend to use sub-contractors to process PII, this should be disclosed to the relevant cloud service customers in advance.

b) Public cloud PII protection implementation guidance

Provisions for the use of sub-contractors to process PII should be transparent in the contract between the public cloud PII processor and the cloud service customer. The contract should specify that sub-contractors can only be commissioned on the basis of a consent that can generally be given by the cloud service customer at the beginning of the service. The public cloud PII processor should inform the cloud service customer in a timely fashion of any intended changes in this regard so that the cloud service customer has the ability to object to such changes or to terminate the contract.

Information disclosed should cover the fact that sub-contracting is used and the names of relevant sub-contractors, but not any business-specific details. The information disclosed should also include the countries in which sub-contractors can process data (see A.12.1) and the means by which sub-contractors are obliged to meet or exceed the obligations of the public cloud PII processor (see A.11.12).

Where public disclosure of sub-contractor information is assessed as leading to security risk increase, disclosure should be made under a non-disclosure agreement and/or on the request of the cloud service customer. The cloud service customer should be made aware that the information is available.

A.9 Individual participation and access

No additional controls are relevant to this privacy principle.

A.10Accountability

A.10.1 Notification of a data breach involving PII

a) Control

The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII.

b) Public cloud PII protection implementation guidance

Provisions covering the notification of a data breach involving PII should form part of the contract between the public cloud PII processor and the cloud service customer. The contract should specify how the public cloud PII processor will provide the information necessary for the cloud service customer to fulfil his obligation to notify relevant authorities. This notification obligation does not extend to a data breach caused by the cloud service customer or PII principal, or within system components for which they are responsible. The contract should also define the maximum delay in notification of a data breach involving PII.

In the event that a data breach involving PII has occurred, a record should be maintained with a description of the incident, the time period, the consequences of the incident, the name of the reporter, to whom the incident was reported, the steps taken to resolve the incident (including the person in charge and the data recovered) and the fact that the incident resulted in loss, disclosure or alteration of PII.

In the event that a data breach involving PII has occurred, the record should also include a description of the data compromised, if known. If notifications were performed, the record should include the steps taken to notify either the cloud service customer or regulatory authorities or both.

In some jurisdictions, relevant legislation or regulations can require the public cloud PII processor to directly notify appropriate regulatory authorities (e.g. a PII protection authority) of a data breach involving PII.

NOTE There can be other breaches requiring notification that are not covered here, e.g. collection without consent or other authorization, use for unauthorized purposes, etc.

A.10.2 Retention period for administrative security policies and guidelines

a) Control

The existing copies of security policies and operating procedures that are updated should be retained for a specified, documented period of replacement.

b) Public cloud PII protection implementation guidance

Review of current and historical policies and procedures can be required, e.g. in the cases of customer dispute resolution and investigation by a PII protection authority. A minimum retention period of five years is recommended in the absence of a specific contractual requirement or other requirements as applicable.

A.10.3 PII return, transfer and disposal

a) Control

The public cloud PII processor should have a policy in respect of these activities and should make this policy available to the cloud service customer.

b) Public cloud PII protection implementation guidance

At some point in time, PII are expected to be disposed of in some manner. This can involve returning the PII to the cloud service customer, transferring it to another public cloud PII processor or to a PII controller (e.g. as a result of a merger), securely deleting or otherwise destroying it, anonymizing it or archiving it.

The public cloud PII processor should provide the information necessary to allow the cloud service customer to ensure that PII processed under a contract is erased (by the public cloud PII processor and any of its sub-contractors) from wherever they are stored, including for the purposes of backup and business continuity, as soon as they are no longer necessary for the specific purposes of the cloud service customer. The nature of the disposition mechanisms (de-linking, overwriting, demagnetization, destruction or other forms of erasure) and/or the applicable commercial standards should be provided for contractually.

The public cloud PII processor should develop and implement a policy in respect of the disposition of PII and should make this policy available to the cloud service customer.

The policy should cover the retention period for PII before its destruction after termination of a contract, to protect the cloud service customer from losing PII through an accidental lapse of the contract.

NOTE This control and guidance is also relevant under the retention element of the "Use, retention and disclosure limitation" principle (see A.6).

A.11Information security

A.11.1 Confidentiality or non-disclosure agreements

a) Control

Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation.

b) Public cloud PII protection implementation guidance

A confidentiality agreement, in whatever form, between the public cloud PII processor, its employees and its agents should ensure that employees and agents do not disclose PII for purposes independent of the instructions of the cloud service customer (see A.3.1). The obligations of the confidentiality agreement should survive termination of any relevant contract.

A.11.2 Restriction of the creation of hardcopy material

a) Control

The creation of hardcopy material displaying PII should be restricted.

b) Public cloud PII protection implementation guidance

Hardcopy material includes material created by printing.

A.11.3 Control and logging of data restoration

a) Control

There should be a procedure for, and a log of, data restoration efforts.

b) Public cloud PII protection implementation guidance

The log of data restoration efforts should contain: the person responsible, a description of the restored data, and the data that were restored manually.

A.11.4 Protecting data on storage media leaving the premises

a) Control

PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).

A.11.5 Use of unencrypted portable storage media and devices

a) Control

Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.

A.11.6 Encryption of PII transmitted over public data-transmission networks

a) Control

PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.

b) Public cloud PII protection implementation guidance

In some cases, e.g. the exchange of e-mail, the inherent characteristics of public data-transmission network systems can require that some header or traffic data be exposed for effective transmission.

Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there can be varied or shared roles in implementing this guidance.

A.11.7 Secure disposal of hardcopy materials

a) Control

Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.

A.11.8 Unique use of user IDs

a) Control

If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.

A.11.9 User ID management

a) Control

De-activated or expired user IDs should not be granted to other individuals.

b) Public cloud PII protection implementation guidance

In the context of the whole cloud computing reference architecture, the cloud service customer can be responsible for some or all aspects of user ID management for cloud service users under its control.

A.11.10 Records of authorized users

a) Control

An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.

b) Public cloud PII protection implementation guidance

A user profile should be maintained for all users whose access is authorized by the public cloud PII processor. The profile of a user comprises the set of data about that user, including user ID, which is necessary to implement the technical controls providing authorized access to the information system.

A.11.11 Contract measures

a) Control

Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor.

b) Public cloud PII protection implementation guidance

Information security and PII protection obligations relevant to the public cloud PII processor can arise directly from applicable law. Where this is not the case, PII protection obligations relevant to the public cloud PII processor are expected to be covered in the contract.

The controls in this document, together with the controls in ISO/IEC 27002, are intended as a reference catalogue of measures to assist in entering into an information processing contract in respect of PII. The public cloud PII processor should inform a prospective cloud service customer, before entering into a contract, about the information security and privacy controls implemented for the protection of PII.

The public cloud PII processor should be transparent about its capabilities during the process of entering into a contract. However, it is ultimately the cloud service customer's responsibility to ensure that the measures implemented by the public cloud PII processor meet its obligations.

A.11.12 Sub-contracted PII processing

a) Control

Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.

b) Public cloud PII protection implementation guidance

The use of sub-contractors to store backup copies is covered by this control (see A.8.1).

A.11.13 Access to data on pre-used data storage space

a) Control

The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.

b) Public cloud PII protection implementation guidance

On deletion by a cloud service user of data held in an information system, performance issues can mean that explicit erasure of those data are impractical. This creates the risk that another user can read the data. Such risk should be avoided by specific technical measures.

No specific guidance is especially appropriate for dealing with all cases in implementing this control. However, as an example, some cloud infrastructure, platforms or applications will return either zeroes or nonces if a cloud service user attempts to read storage space which has not been overwritten by that user's own data.

A.12Privacy compliance

A.12.1 Geographical location of PII

a) Control

The public cloud PII processor should specify and document the countries in which PII can possibly be stored.

b) Public cloud PII protection implementation guidance

The identities of the countries where PII can possibly be stored should be made available to cloud service customers. The identities of the countries arising from the use of sub-contracted PII processing should be included. Where specific contractual agreements apply to the international transfer of data, such as model contract clauses, binding corporate rules or cross border privacy rules, the agreements and the countries or circumstances in which such agreements apply should also be identified. The public cloud PII processor should inform the cloud service customer in a timely fashion of any intended changes in this regard so that the cloud service customer has the ability to object to such changes or to terminate the contract.

A.12.2 Intended destination of PII

a) Control

PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.

Annex B
(informative)

Correspondence between this document and the first edition ISO/IEC 27018:2019

The purpose of this annex is to provide backwards compatibility with the first edition of this document (ISO/IEC 27018:2019) for organizations currently using it and wanting to transition to this edition.

Table B.1 provides the correspondence of the controls specified in Clauses 5 to 8 with those in ISO/IEC 27018:2019.

Table B.1 — Correspondence between controls in this document and controls in ISO/IEC 27018:2019

ISO/IEC 27018:2025 control identifier	ISO/IEC 27018:2019 control identifier	Control name
5.1	05.1.1, 05.1.2	Policies for information security
5.2	06.1.1	Information security roles and responsibilities
5.3	06.1.2	Segregation of duties
5.4	07.2.1	Management responsibilities
5.5	06.1.3	Contact with authorities
5.6	06.1.4	Contact with special interest groups
5.7	New	Threat intelligence
5.8	06.1.5, 14.1.1	Information security in project management
5.9	08.1.1, 08.1.2	Inventory of information and other associated assets
5.10	08.1.3, 08.2.3	Acceptable use of information and other associated assets
5.11	08.1.4	Return of assets
5.12	08.2.1	Classification of information
5.13	08.2.2	Labelling of information
5.14	13.2.1, 13.2.2, 13.2.3	Information transfer
5.15	09.1.1, 09.1.2	Access control
5.16	09.2.1	Identity management
5.17	09.2.4, 09.3.1, 09.4.3	Authentication information
5.18	09.2.2, 09.2.5, 09.2.6	Access rights
5.19	15.1.1	Information security in supplier relationships
5.20	15.1.2	Addressing information security within supplier agreements
5.21	15.1.3	Managing information security in the ICT supply chain
5.22	15.2.1, 15.2.2	Monitoring, review and change management of supplier services
5.23	New	Information security for use of cloud services
5.24	16.1.1	Information security incident management planning and preparation
5.25	16.1.4	Assessment and decision on information security events
5.26	16.1.5	Response to information security incidents

Table B.1 ***(continued)***

ISO/IEC 27018:2025 control identifier	ISO/IEC 27018:2019 control identifier	Control name
5.27	16.1.6	Learning from information security incidents
5.28	16.1.7	Collection of evidence
5.29	17.1.1, 17.1.2, 17.1.3	Information security during disruption
5.30	New	ICT readiness for business continuity
5.31	18.1.1, 18.1.5	Legal, statutory, regulatory and contractual requirements
5.32	18.1.2	Intellectual property rights
5.33	18.1.3	Protection of records
5.34	18.1.4	Privacy and protection of PII
5.35	18.2.1	Independent review of information security
5.36	18.2.2, 18.2.3	Compliance with policies, rules and standards for information security
5.37	12.1.1	Documented operating procedures
6.1	07.1.1	Screening
6.2	07.1.2	Terms and conditions of employment
6.3	07.2.2	Information security awareness, education and training
6.4	07.2.3	Disciplinary process
6.5	07.3.1	Responsibilities after termination or change of employment
6.6	13.2.4	Confidentiality or non-disclosure agreements
6.7	06.2.2	Remote working
6.8	16.1.2, 16.1.3	Information security event reporting
7.1	11.1.1	Physical security perimeters
7.2	11.1.2, 11.1.6	Physical entry
7.3	11.1.3	Securing offices, rooms and facilities
7.4	New	Physical security monitoring
7.5	11.1.4	Protecting against physical and environmental threats
7.6	11.1.5	Working in secure areas
7.7	11.2.9	Clear desk and clear screen
7.8	11.2.1	Equipment siting and protection
7.9	11.2.6	Security of assets off-premises
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Storage media
7.11	11.2.2	Supporting utilities
7.12	11.2.3	Cabling security
7.13	11.2.4	Equipment maintenance
7.14	11.2.7	Secure disposal or re-use of equipment
8.1	06.2.1, 11.2.8	User endpoint devices
8.2	09.2.3	Privileged access rights
8.3	09.4.1	Information access restriction
8.4	09.4.5	Access to source code
8.5	09.4.2	Secure authentication
8.6	12.1.3	Capacity management
8.7	12.2.1	Protection against malware
8.8	12.6.1, 18.2.3	Management of technical vulnerabilities

Table B.1 ***(continued)***

ISO/IEC 27018:2025 control identifier	ISO/IEC 27018:2019 control identifier	Control name
8.9	New	Configuration management
8.10	New	Information deletion
8.11	New	Data masking
8.12	New	Data leakage prevention
8.13	12.3.1	Information backup
8.14	17.2.1	Redundancy of information processing facilities
8.15	12.4.1, 12.4.2, 12.4.3	Logging
8.16	New	Monitoring activities
8.17	12.4.4	Clock synchronization
8.18	09.4.4	Use of privileged utility programs
8.19	12.5.1, 12.6.2	Installation of software on operational systems
8.20	13.1.1	Networks security
8.21	13.1.2	Security of network services
8.22	13.1.3	Segregation of networks
8.23	New	Web filtering
8.24	10.1.1, 10.1.2	Use of cryptography
8.25	14.2.1	Secure development lifecycle
8.26	14.1.2, 14.1.3	Application security requirements
8.27	14.2.5	Secure system architecture and engineering principles
8.28	New	Secure coding
8.29	14.2.8, 14.2.9	Security testing in development and acceptance
8.30	14.2.7	Outsourced development
8.31	12.1.4, 14.2.6	Separation of development, test and production environments
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Change management
8.33	14.3.1	Test information
8.34	12.7.1	Protection of information systems during audit testing

Bibliography

[1] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

[2] ISO 55001, *Asset management — Asset management system — Requirements*

[3] ISO/IEC 11770 (all parts), *Information security — Key management*

[4] ISO/IEC 15408 (all parts), *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security*

[5] ISO 15489 (all parts), *Information and documentation — Records management*

[6] ISO/IEC 22123-1, *Information technology — Cloud computing — Part 1: Vocabulary*

[7] ISO/IEC 22123-2, *Information technology — Cloud computing — Part 2: Concepts*

[8] ISO/IEC 22123-3, *Information technology — Cloud computing — Part 3: Reference architecture*

[9] ISO/IEC 19086 (all parts), *Cloud computing — Service level agreement (SLA) framework*

[10] ISO/IEC 19770 (all parts), *Information technology — IT asset management*

[11] ISO/IEC 19941, *Information technology — Cloud computing — Interoperability and portability*

[12] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*

[13] ISO 21500, *Project, programme and portfolio management — Context and concepts*

[14] ISO 21502, *Project, programme and portfolio management — Guidance on project management*

[15] ISO 22301, *Security and resilience — Business continuity management systems — Requirements*

[16] ISO 22313, *Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*

[17] ISO/TS 22317, *Security and resilience — Business continuity management systems — Guidelines for business impact analysis*

[18] ISO 22396, *Security and resilience — Community resilience — Guidelines for information exchange between organizations*

[19] ISO/IEC/TS 23167, *Information technology — Cloud computing — Common technologies and techniques*

[20] ISO/IEC 23751, *Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework*

[21] ISO/IEC 24760 (all parts), *IT Security and Privacy — A framework for identity management*

[22] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[23] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*[1)]

[24] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[25] ISO/IEC 27007, *Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*

1) Cancelled and replaced by ISO/IEC 27002:2022.

[26] ISO/IEC/TS 27008, *Information technology — Security techniques — Guidelines for the assessment of information security controls*

[27] ISO/IEC 27011, *Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations*

[28] ISO/IEC/TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*

[29] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[30] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[31] ISO/IEC 27019, *Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry*

[32] ISO/IEC 27031, *Cybersecurity — Information and communication technology readiness for business continuity*

[33] ISO/IEC 27033 (all parts), *— Information technology – Network security*

[34] ISO/IEC 27034 (all parts), *Information technology — Application security*

[35] ISO/IEC 27035-1, *Information technology — Information security incident management — Part 1: Principles and process*

[36] ISO/IEC 27035-2, *Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*

[37] ISO/IEC 27036 (all parts), *Cybersecurity — Supplier relationships*

[38] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

[39] ISO/IEC 27040, *Information technology — Security techniques — Storage security*

[40] ISO/IEC 27050 (all parts), *Information technology — Electronic discovery*

[41] ISO/IEC/TS 27110, *Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines*

[42] ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[43] ISO 27799, *Health informatics — Information security management in health using ISO/IEC 27002*

[44] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[45] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

[46] ISO/IEC 29134, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[47] ISO/IEC 29146, *Information technology — Security techniques — A framework for access management*

[48] ISO/IEC 29147, *Information technology — Security techniques — Vulnerability disclosure*

[49] ISO 30000, *Ships and marine technology — Ship recycling management systems — Specifications for management systems for safe and environmentally sound ship recycling facilities*

[50] ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*

[51] ISO 31000:2018, *Risk management — Guidelines*

[52] IEC 31010, *Risk management — Risk assessment techniques*

[53] ISO/IEC 22123 (all parts), *Information technology — Cloud computing*

[54] ISO/IEC 27555, *Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion*

[55] Information Security Forum (ISF). *The ISF Standard of Good Practice for Information Security2020*. Available at https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security/

[56] ITIL® Foundation, ITIL 4 edition, AXELOS, February 2019, ISBN: 9780113316076

[57] National Institute of Standards and Technology (NIST), SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy, Revision 2. December2018* [viewed 2023-08-09]. Available at https://doi.org/10.6028/NIST.SP.800-37r2

[58] Open Web Application Security Project (OWASP). *OWASP Top Ten - 2021, The Ten Most Critical Web Application Security Risks*, 2021 [viewed 2023-08-09]. Available at https://owasp.org/Top10/

[59] Open Web Application Security Project (OWASP). *OWASP Developer Guide*, [online] [viewed 2023-08-09]. Available at https://owasp.org/www-project-developer-guide/

[60] Open Web Application Security Project (OWASP). *OWASP Top 10 API Security Risks – 2023*, [online] [viewed 2023-08-09]. Available at https://owasp.org/API-Security/editions/2023/en/0x11-t10/

[61] National Institute of Standards and Technology (NIST), SP 800-63B, *Digital Identity Guidelines; Authentication and Lifecycle Management*. February 2020 [viewed 2023-08-09]. Available at https://doi.org/10.6028/NIST.SP.800-63b

[62] OASIS, *Structured Threat Information Expression*. Available at https://www.oasis-open.org/standards#stix2.0

[63] OASIS, *Trusted Automated Exchange of Indicator Information*. Available at https://www.oasis-open .org/standards#taxii2.0

[64] ISO 31700-1:2023, *Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements*

[65] ISO/TR 31700-2:2023, *Consumer protection — Privacy by design for consumer goods and services — Part 2: Use cases*

ICS 35.030

Price based on 35 pages